Pacific Journal of Mathematics

DEGRÉ MINIMUM DES POLYNÔMES $f(\sum_{i=0}^{m} a_i X^{p^{ri}})$ SUR LES CORPS FINIS DE CARACTÉRISTIQUE $p > m$

S. AGOU

Vol. 102, No. 1 January 1982

PACIFIC JOURNAL OF MATHEMATICS
Vol. 102, No. 1, 1982

DEGRE MINIMUM DES POLYNÔMES $f(\sum_{i=0}^{m} a_i X^{p^{ri}})$ SUR LES CORPS FINIS DE CARACTÉRISTIQUE $p > m$

S. AGOU

Let $f(x)$ be an irreducible polynomial over the finite field F_{p^s}. In this paper we give explicitly the minimum degree of the irreducible factors in $F_{p^s}[x]$ of the polynomial $f(\sum_{i=0}^{m} a_i x^{p^{ri}})$ where $p > m$ and $a_i \in F_{p^s}$. We also give some other related results.

0. **Rappels.** Soient $u(X) \in \boldsymbol{F}_{p^s}[X]$ un polynôme et R l'ensemble de ses racines.

0.1. Le polynôme $u(X)$ est dit "*hyponormal sur le corps fini* $\boldsymbol{F}_{p^s}$" s'il existe une racine $x_0 \in R$ telle que pour tout $x \in R$ on ait $\boldsymbol{F}_{p^s}(x_0) \subset \boldsymbol{F}_{p^s}(x)$.

0.2. Si $u(X)$ est hyponormal sur $\boldsymbol{F}_{p^s}$ alors le degré $[\boldsymbol{F}_{p^s}(x_0): \boldsymbol{F}_{p^s}]$ s'appelle "*le degré minimum du polynôme hyponormal* $u(X)$ *sur* $\boldsymbol{F}_{p^s}$". On notera que ce degré divise les entiers $[\boldsymbol{F}_{p^s}(x): \boldsymbol{F}_{p^s}]$ pour chaque $x \in R$.

0.3. Un polynôme non nul de la forme $g_m(X) = \sum_{i=0}^{m} a_i X^{p^{ri}}$ de $\boldsymbol{F}_{p^s}[X]$ où r est un entier arbitraire est appelé un "p^r-*polynôme de* $\boldsymbol{F}_{p^s}[X]$".

0.4. Dans l'ensemble des p^r-polynômes de $\boldsymbol{F}_{p^s}[X]$ on a, à l'aide du "*produit symbolique*" au sens de Ore, [6], pour h entier, la relation

$$(*) \qquad \begin{aligned} X^{p^{hr}} &= \xi(X) + u\Big(\sum_{i=0}^{m} a_i X^{p^{ri}}\Big) \\ &= \xi(X) + u(X) \times g_m(X) \text{ avec } \deg(\xi(X)) < p^{mr}, \end{aligned}$$

$\xi(X)$, $u(X)$ étant des p^r-polynômes lorsqu'ils sont non nuls. Cette relation est équivalente à celle donnée par la division euclidienne usuelle. De plus pour tout $\lambda \in \boldsymbol{F}_{p^{sl}}$ on a $X^{p^{hr}} = \xi(X) + u(\lambda) + u(g_m(X) - \lambda)$. Dans "*l'algorithme d'Euclide*" de recherche du p.g.c.d. de deux p^r-polynômes de $\boldsymbol{F}_{p^s}[X]$, c'est-à-dire par divisions euclidiennes successives, les seuls polynômes qui apparaissent dans les formules sont par conséquent des p^r-polynômes et le polynôme nul.

Par ailleurs, si on considère la relation

$$(**) \qquad X^h = \xi_1(X) + u_1(X) \cdot \Big(\sum_{i=0}^{m} a_i X^i\Big) \quad \text{avec } \deg(\xi_1(X)) < m$$

une difficulté surgit: c'est l'explicitation des polynômes $\xi(X)$ et $u(X)$ de la relation $(*)$ à l'aide des polynômes $\xi_1(X)$ et $u_1(X)$. Nous

envisageons de donner dans un travail ultérieur la solution de ce problème. Ceci étant on a le

1. Résultat fondamental.

PROPOSITION 1.1. *Soient m, n, r, s des entiers strictement positifs. Soit p un entier premier, tel que $p > m$. Soient dans $\boldsymbol{F}_{p^s}[X]$ respectivement un polynôme $f(X)$ irréductible de degré n et $g_m(X) = \sum_{i=0}^{m} a_i X^{p^{ri}}$ un p^r-polynôme tel que $a_0 \neq 0$. Alors le degré minimum du polynôme hyponormal $f(g_m(X))$ sur $\boldsymbol{F}_{p^s}$ est n ou $n\,p^{k+1}$ où k est le plus grand entier tel que $p^k \mid r/(r, sn)$.*

Tout d'abord la proposition a été établie dans des publications antérieures [1, 2, 3] pour $m = 1$, $m = 2$, et en outre on y a donné explicitement entre autres, les conditions d'occurence de chaque éventualité. On désigne par θ une racine dans $\boldsymbol{F}_{p^{sn}}$ du polynôme irréductible $f(X)$ et on pose $q = p^{[mr,sn]}$.

Soit x une racine d'ordre t de $g_m(X) - \theta$. On a donc $g_m(X) - \theta = (X - x)^t H(X)$ avec $H(x) \neq 0$. Par dérivation on obtient $a_0 = t(X - x)^{t-1} H(X) + (X - x)^t H'(X)$. Il en résulte que la condition $a_0 \neq 0$ est équivalente à $t = 1$. Ainsi $g_m(X) - \theta$ n'a que des racines simples. Puisque $p > m$, les racines de $g_m(X) - \theta$ sont contenues dans le corps $\boldsymbol{F}_{q^{p(q^\rho - 1)}}$ où ρ est un entier convenable dont l'explicitation est inutile ici.

Les notations et hypothèses ci-dessus seront utilisées tout au long de ce travail. Toute altération sera expressément mentionnée. La numérotation des formules est interne à chaque paragraphe.

Preuve de la Proposition 1.1. Pour établir cette preuve on va examiner différents cas. On procède par récurrence sur l'entier m, en supposant $m \geqq 2$ et la proposition établie pour tous les polynômes de $\boldsymbol{F}_{p^{sn}}[X]$, de la forme $g_{m'}(X) + \lambda$ pour $1 \leqq m' < m$, où $g_{m'}(X)$ est un p^r-polynôme tel que $g_{m'}(X) + \lambda$ n'ait que des racines simples. On désignera, ci-dessous par (H) cette hypothèse de recurrence.

1° *Cas.* Si $(g_m(X) - \theta, X^q - X) = 1$ alors, comme $g_m(X) - \theta$ est hyponormal sur $\boldsymbol{F}_{p^{sn}}$, son degré minimum sur $F_{p^{sn}}$ est de la forme p^{α_0}. On a les conditions $p^{\alpha_0} \nmid p^{[mr,sn]/sn}$ et $p^{\alpha_0} \mid p^{p[mr,sn]/sn}$. Or $[mr, sn]/sn = p^k \cdot \delta$ avec $(\delta, p) = 1$. Il en résulte que $\alpha_0 = k + 1$.

2° *Cas.* Si $(g_m(X) - \theta, X^q - X) \neq 1$ et si $g_m(X) - \theta \nmid X^q - X$. Le polynôme $(g_m(X) - \theta, X^q - X)$ appartient à $\boldsymbol{F}_{p^{sn}}[X]$. Ce polynôme est par hypothèse non constant. De plus ce polynôme a des racines simples et satisfait à l'hypothèse de récurrence (H). Il en résulte,

puisqu'il a une racine dans $\boldsymbol{F}_q$, que $g_m(X) - \theta$ a une racine dans $\boldsymbol{F}_{p^{sn}}$.

3° *Cas.* Si $g_m(X) - \theta \mid X^q - X$.
Alors il existe un p^r-polynôme $u(X)$ de $\boldsymbol{F}_{p^s}[X]$ tel que l'on ait

$$(1) \qquad X^q - X = u(g_m(X) - \theta) = u(g_m(X)) .$$

De (1) on déduit que

$$\begin{aligned}(X^q - X - g_m(u(X)))(g_m(X)) &= (g_m(X))^q - g_m(X) - g_m(u(g_m(X))) \\ &= (g_m(X))^q - g_m(X) - g_m(X^q - X) .\end{aligned}$$

Comme $g_m(X) \in \boldsymbol{F}_{p^s}[X] \subset \boldsymbol{F}_q[X]$ on en déduit que

$$(X^q - X - g_m(u(X)))(g_m(X)) = 0 .$$

Par suite on a

$$(2) \qquad X^q - X = g_m(u(X)) .$$

On est alors conduit à l'étude suivante.

(a) Si $(g_m(X) - \theta, u(X)) \neq 1$ et si $g_m(X) - \theta \nmid u(X)$, alors le polynôme $(g_m(X) - \theta, u(X)) \notin \boldsymbol{F}_{p^{sn}}$ et satisfait à l'hypothèse (H).

La relation (1) montre alors que $(g_m(X) - \theta, u(X))$ a une racine dans $\boldsymbol{F}_{p^{sn}}$, et par conséquent $g_m(X) - \theta$ aussi.

(b) Si $g_m(X) - \theta \mid u(X)$, alors il existe un p^r-polynôme $u_1(X)$ de $\boldsymbol{F}_{p^s}[X]$ tel que

$$(3) \qquad u(X) = u_1(g_m(X) - \theta) = u_1(g_m(X)) .$$

De (3) on déduit en tenant compte de (1) et de (2) que

$$(u(X) - g_m(u_1(X)))(g_m(X)) = u(g_m(X)) - g_m(u(X)) = 0 .$$

D'où

$$(4) \qquad u(X) = g_m(u_1(X)) .$$

On est amené à examiner les sous-cas suivants.

(b1) Si $(g_m(X) - \theta, u_1(X)) \neq 1$ et si $g_m(X) - \theta \nmid u_1(X)$ alors par un raisonnement déjà vu on en déduit que $g_m(X) - \theta$ a une racine dans $\boldsymbol{F}_{p^{sn}}$.

(b2) Si $g_m(X) - \theta \mid u_1(X)$, alors on a

(5) $u_1(X) = u_2(g_m(X) - \theta) = u_2(g_m(X))$ où $u_2(X)$ est un p^r-polynôme de $\boldsymbol{F}_{p^s}[X]$.

On en déduit que $(u_1(X) - g_m(u_2(X)))(g_m(X)) = u_1(g_m(X)) - g_m(u_1(X)) = 0$, d'où

$$u_1(X) = g_m(u_2(X)) \ . \tag{6}$$

A ce stade l'étude est à refaire à partir du polynôme $u_2(X)$. Supposons donc que pour un indice l, $l \geqq 1$, on ait

$$\begin{aligned} &u_l(X) = u_{l+1}(g_m(X) - \theta) = u_{l+1}(g_m(X)) \\ &\text{et} \\ &g_m(u_l(X)) = u_l(g_m(X)) \ . \end{aligned} \tag{7}$$

D'où

$$u_l(X) = g_m(u_{l+1}(X)) \ . \tag{8}$$

D'où les sous-cas:

(b21) Si (7) se produit pour toutes les valeurs possibles de l'entier l, alors $g_m(X) - \theta$ est un p^r-polynôme de $\boldsymbol{F}_{p^s}[X]$ et donc $\theta = 0$, ainsi $g_m(X) - \theta$ a une racine dans $\boldsymbol{F}_{p^s} \subset \boldsymbol{F}_{p^{sn}}$.

(b22) S'il existe un entier l minimal, tel que $g_m(X) - \theta \nmid u_l(X)$ alors on a deux nouveaux sous-cas.

(b221) Ou bien $(g_m(X) - \theta, u_l(X)) \neq 1$ alors on sait que cela conduit à l'existence d'une racine dans $\boldsymbol{F}_{p^{sn}}$ pour $g_m(X) - \theta$.

(b222) Ou bien $(g_m(X) - \theta, u_l(X)) = 1$.

Provisoirement nous allons laisser de côté cette dernière éventualité. Enfin on doit examiner le sous-cas.

(c) Si $(g_m(X) - \theta, u(X)) = 1$.

On peut écrire

$$\begin{aligned} &u(X) = r_{m-1}(X) + u_1(g_m(X) - \theta) \ , \\ &\text{avec deg } (r_{m-1}(X)) < \text{deg } (g_m(X)) \ , \end{aligned} \tag{9}$$

où $u_1(X) \in \boldsymbol{F}_{p^s}[X]$ est un p^r-polynôme.

Maintenant on doit envisager les possibilités suivantes:

(c1) Si $r_{m-1}(X) \in \boldsymbol{F}_{p^{sn}}^{\times}$ alors à nouveau on a:

$$u(X) = u_1(g_m(X)) \quad \text{et} \quad u_1(\theta) = r_{m-1}(X) \neq 0 \ . \tag{3}$$

d'où

$$u(X) = g_m(u_1(X)) \ . \tag{4}$$

En vertu de (1), $g_m(X) \mid X^q - X$. Par suite on a $u(\theta) = 0$. Par conséquent $u_1(\theta)$ est une racine non nulle, dans $\boldsymbol{F}_{p^{sn}}$, de $g_m(X)$. On peut donc écrire

$$g_m(X) - \theta = \gamma_{m-1}(X^{p^r} - u_1(\theta)^{p^r-1}X) - \theta \ ,$$

où $\gamma_{m-1}(X)$ est un p^r-polynôme de $\boldsymbol{F}_{p^{sn}}[X]$.

Puisque $a_0 \neq 0$, alors $\gamma_{m-1}(X) - \theta$ n'a que des racines simples.

L'hypothèse de récurrence (H) montre que si ce polynôme n'a pas de racine dans $\boldsymbol{F}_{p^{sn}}$, alors dans $\boldsymbol{F}_{p^{sn}}[X]$, il possède un facteur irréductible de degré p^{k+1}, ce qui est absurde, puisque $g_m(X) - \theta \mid X^q - X$. Par conséquent $\gamma_{m-1}(X) - \theta$ possède une racine λ_0 dans $\boldsymbol{F}_{p^{sn}}$. Mais alors le polynôme $X^{p^r} - u_1(\theta)^{p^{r-1}}X - \lambda_0$ qui divise $g_m(X) - \theta$, donc $X^q - X$, a une racine dans $\boldsymbol{F}_{p^{sn}}$. Le degré minimum de $g_m(X) - \theta$ sur $\boldsymbol{F}_{p^{sn}}$ est donc 1.

(c2) Si $r_{m-1}(X) \notin \boldsymbol{F}_{p^{sn}}$, à l'aide de l'algorithme d'Euclide de recherche du p.g.c.d. de $g_m(X) - \theta$ et de $r_{m-1}(X)$ on peut écrire les relations

$$r_{m-l}(X) = r_{m-l-2}(X) + u_{l+2}(r_{m-l-1}(X))$$

où $l \geqq 0$ est un entier, en convenant que $r_m(X) = g_m(X) - \theta$, où $u_{l+2}(X)$ est un p^r-polynôme de $\boldsymbol{F}_{p^{sn}}[X]$ et où enfin, $l \leqq l_0$, l_0 étant le plus petit entier tel que $r_{m-l_0-2}(X) \in \boldsymbol{F}_{p^{sn}}^{\times}$. De plus $u_{l+2}(X)$, pour $0 \leqq l \leqq l_0$ est un p^r-polynôme.

On en déduit qu'il existe un p^r-polynôme $U(X)$ de $\boldsymbol{F}_{p^{sn}}[X]$ tel que

$$g_m(X) - \theta = \lambda + U(V(X)) ,$$

$V(X)$ étant un reste convenable, non constant, et non du premier degré, (ce point sera établi dans la Proposition 2.1), de degré strictement inférieur à celui de $g_m(X)$ et où $\lambda \in \boldsymbol{F}_{p^{sn}}$. Le polynôme $U(X) + \lambda$ satisfait à l'hypothèse (H) et a des racines simples. Son degré minimum sur $\boldsymbol{F}_{p^{sn}}$ ne peut être p^{k+1} sinon $g_m(X) - \theta$ possèderait dans sa factorisation en irréductibles de $\boldsymbol{F}_{p^{sn}}[X]$ un irréductible de degré multiple de p^{k+1} ce qui est impossible puisque $g_m(X) - \theta \mid X^q - X$.

Ainsi $U(X) + \lambda$ a une racine λ_0 dans $\boldsymbol{F}_{p^{sn}}$. On peut donc réappliquer le raisonnement à $V(X) - \lambda_0$ et on en déduit l'existence dans $\boldsymbol{F}_{p^{sn}}$ d'une racine pour $g_m(X) - \theta$.

Nous avons laissé en suspens le cas (b222). Il est clair que ce cas se traite à l'aide des mêmes arguments que le cas (c). C.Q.F.D.

Au cours de la démonstration nous avons affirmé que le polynôme $V(X)$ ne pouvait être du premier degré. Prouvons ce point.

2. Compléments et conséquences. On conserve les notations et hypothèses du §1. Mais *dans ce qui suit on ne suppose plus que* $p > m$. On a alors la

PROPOSITION 2.1.

Si dans l'algorithme d'Euclide de recherche d'un p.g.c.d. des polynômes $X^q - X$ *et* $g_m(X) - \theta$ *il apparaît un reste du premier degré alors c'est à un coefficient près le p.g.c.d. de* $X^q - X$ *et de* $g_m(X) - \theta$.

Preuve. Il est possible de supposer $m>2$. Reprenons l'algorithme d'Euclide de recherche d'un p.g.c.d. de $X^q - X$ et de $g_m(X) - \theta$.

$$(1) \qquad X^q - X = r_{m-1}(X) + u(g_m(X) - \theta)$$

où $u(X)$ est un p^r-polynôme de $\boldsymbol{F}_{p^s}[X]$. L'hypothèse faite montre que $\deg(r_{m-1}(X)) > 0$. On en déduit que

$$\begin{aligned}(X^q - X - g_m(u(X)))(g_m(X)) &= g_m(X^q - X) - g_m(X^q - X - r_{m-1}(X) + u(\theta)) \\ &= g_m(r_{m-1}(X) - u(\theta)) \ .\end{aligned}$$

Il en résulte que $X^q - X - g_m(u(X)) = \rho_{m-1}(X)$ où $\rho_{m-1}(X)$ est un p^r-polynôme de $\boldsymbol{F}_{p^s}[X]$ de même degré que $r_{m-1}(X) - u(\theta)$. On a donc

$$(2) \qquad X^q - X = \rho_{m-1}(X) + g_m(u(X)) \ .$$

Ensuite on a les relations:

$$\begin{aligned} g_m(X) - \theta &= r_{m-2} + u_1(r_{m-1}(X)) \\ \vdots \qquad &\quad \vdots \qquad \vdots \\ r_{m-l+2}(X) &= r_{m-l}(X) + u_{l-1}(r_{m-l+1}(X)) \end{aligned}$$

avec $\deg(r_{m-l}(X)) = 1$. Modulo $r_{m-1}(X)$ on en déduit les congruences:

$$\begin{aligned} g_m(X) - \theta &\equiv r_{m-2}(X) \\ X^q - X &\equiv u(r_{m-2}(X)) \ ; \end{aligned}$$

Par (2) il vient

$$r_{m-2}^q(X) - r_{m-2}(X) = \rho_{m-1}(r_{m-2}(X)) + g_m(u(r_{m-2}(X))) \ ,$$

donc

$$(g_m(X) - \theta)^q - (g_m(X) - \theta) \equiv g_m(u(r_{m-2}(X))) \ ;$$

Mais

$$g_m(X^q - X) = (g_m(X) - \theta)^q - (g_m(X) - \theta) \quad \text{puisque} \quad \theta^q = \theta \ ,$$

par suite

$$g_m(X^q - X) \equiv g_m(u(r_{m-2}(X))) \ ;$$

Par ailleurs

$$g_m(X^q - X) \equiv r_{m-2}^q(X) - r_{m-2}(X)$$

donc on a

$$(3) \qquad \rho_{m-1}(r_{m-2}(X)) \equiv 0 \ .$$

(Observons que si $\deg(r_{m-1}(X)) = 1$ alors $r_{m-2}(X) = 0$ et la conclusion

subsiste.)
Il existe par conséquent un p^r-polynôme $\rho_{m-2}(X)$ tel que

$$\rho_{m-1}(r_{m-2}(X)) = \rho_{m-2}(r_{m-1}(X)) . \tag{4}$$

(On a $\deg(\rho_{m-2}(X)) = \deg(r_{m-2}(X))$.)

En continuant ce processus, c'est à dire pour $t < l$, si on suppose que

$$\rho_{m-t+2}(r_{m-t+1}(X)) = \rho_{m-t+1}(r_{m-t+2}(X))$$

avec

$$r_{m-t+2}(X) \equiv r_{m-t}(X) \mod r_{m-t+1}(X)$$

alors on a

$$\rho_{m-t+1}(r_{m-t}(X)) \equiv 0 \mod r_{m-t+1}(X)$$

d'où

$$\rho_{m-l}(r_{m-l+1}(X)) = \rho_{m-l+1}(r_{m-l}(X)) .$$

Comme $r_{m-l}(X)$ est du premier degré il en résulte que $\rho_{m-l}(X) = \alpha X$, $\alpha \in \boldsymbol{F}_{p^{sn}}^{\times}$. Ainsi $r_{m-l}(X) \mid r_{m-l+1}(X)$, donc $r_{m-l}(X)$ est un p.g.c.d.
C.Q.F.D.

On observera qu'avec cette hypothèse $g_m(X) - \theta$ a une racine unique dans $\boldsymbol{F}_{p^{sn}}$. Cette racine est le zéro de $r_{m-l}(X)$, donc est effectivement calculable.

REMARQUE. Dans la Proposition 1.1. (c2) on a donc bien $\deg(V(X)) > 1$. Car si $\deg(V(X)) = 1$, alors la relation $u(g_m(X) - \theta) = g_m(u(X))$, l'algorithme d'Euclide de recherche du p.g.c.d. de $u(X)$ et de $g_m(X) - \theta$ conduisent à la contradiction $V(X) \mid (g_m(X) - \theta, u(X))$, lorsque dans le raisonnement ci-dessus on fait jouer à $u(X)$ le rôle de $X^q - X$.

On a aussi, avec les notations et hypothèses de la Proposition 1.1. la

PROPOSITION 2.2. *Soit d un diviseur de l'entier $p^r - 1$. On suppose à nouveau $p > m$. Alors le polynôme $f((\sum_{i=0}^{m} a_i X^{p^{ri}})^d)$ est hyponormal sur $\boldsymbol{F}_{p^s}$.*

Preuve. Il suffit de prouver l'hyponormalité sur $\boldsymbol{F}_{p^{sn}}$ du polynôme $(\sum_{i=0}^{m} a_i X^{p^{ri}})^d - \theta$. Soit ν_0 le degré minimum sur $\boldsymbol{F}_{p^{sn}}$ du polynôme hyponormal $X^d - \theta$.

Soit alors $f_0(X)$ un polynôme irréductible de $\boldsymbol{F}_{p^{sn}}[X]$ divisant

$X^d - \theta$ admettant ν_0 pour degré.

Le degré minimum de $f_0(\sum_{i=0}^m a_i X^{p^{ri}})$ sur $\boldsymbol{F}_{p^{sn}}$ est ν_0 ou $\nu_0\, p^{k_{\nu_0}+1}$, d'après la Proposition 1.1, où $p^{k_{\nu_0}}$ est la plus forte puissance de p divisant $r/(r, sn\nu_0)$.

Soit $f_\nu(X)$ un irréductible de degré ν de $\boldsymbol{F}_{p^{sn}}[X]$ factorisant $X^d - \theta$. On sait que $\nu_0 | \nu$ d'une part et que $[r, sn\nu] = [r, sn\nu_0]$. Le même raisonnement montre que le degré minimum de $f_\nu(\sum_{i=0}^m a_i X^{p^{ri}})$ sur $\boldsymbol{F}_{p^{sn}}$ est ν ou $\nu p^{k_\nu+1}$.

Si θ_0 est une racine de $f_0(X)$ alors il existe $\eta \in \boldsymbol{F}_{p^r}^\times$ tel que $\theta_0\eta$ soit une racine de f_ν.

Si le degré minimum de $f_0(\sum_{i=0}^m a_i X^{p^{ri}})$ est ν_0 sur $\boldsymbol{F}_{p^{sn}}$ alors il est clair que l'on a l'hyponormalité sur $\boldsymbol{F}_{p^{sn}}$ de $(\sum_{i=0}^m a_i X^{p^{ri}})^d - \theta$.

Si le degré minimum de $f_0(\sum_{i=0}^m a_i X^{p^{ri}})$ est $\nu_0 p^{k_{\nu_0}+1}$, alors $\sum_{i=0}^m a_i X^{p^{ri}} - \theta_0\eta$ ne peut avoir de racine dans $\boldsymbol{F}_{p^{sn\nu}}$. En effet dans le cas contraire il existerait $\lambda \in \boldsymbol{F}_{p^{sn\nu}}$ tel que $\sum_{i=0}^m a_i \lambda^{p^{ri}} = \theta_0\eta$ or $\lambda/\eta \in \boldsymbol{F}_{p^{[r, sn\nu]}} = \boldsymbol{F}_{p^{[r, sn\nu_0]}}$, par suite $f_0(\sum_{i=0}^m a_i X^{p^{ri}})$ aurait une racine λ/η dans $\boldsymbol{F}_{p^{[r, sn\nu_0]}}$ ce qui n'est pas. Pour conclure il reste à montrer que $\nu_0 p^{k_{\nu_0}+1} | \nu p^{k_\nu+1}$. Or on a $r\nu/(r, sn\nu) = r\nu_0/(r, sn\nu_0) = p^{k_\nu} \cdot \omega_\nu \cdot \nu = p^{k_{\nu_0}} \cdot \omega_{\nu_0} \cdot \nu_0$ avec $(\omega_\nu, p) = (\omega_{\nu_0}, p) = 1$. Il en résulte que $p^{k_{\nu_0}} | p^{k_\nu}\nu/\nu_0$ C.Q.F.D..

Bibliographie

1. S. Agou, *Sur une classe de polynômes hyponormaux sur un corps fini*, Acta Arithmetica, vol. **39**, n° 2, (1981), 105-111.

2. ———, *Sur la factorisation des polynômes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini $\boldsymbol{F}_{p^s}$*, J. Number Theory, **12** (80), 447-459.

3. ———, *Sur le degré minimum des polynômes $f(X^{4^r} - aX^{2^r} - bX)$ sur $\boldsymbol{F}_{2^s}$ et sur quelques conséquences*, (Journées SMF de Théorie des Nombres analytique et élémentaire, Limoges FRANCE 1980).

4. L. Carlitz et A. F. Long, *The factorization of $Q(L(x_1), \cdots, L(x_k))$ over a finite field where $Q(x_1, \cdots, x_k)$ is of first degree and $L(x)$ is linear*, Acta Arithmetica, **32** (1977), 407-420.

5. A. F. Long et T. P. Vaughan, *Factorization of $Q(h(T)(x))$ over $GF(q)$ where $Q(x)$ is irreducible and $h(T)(x)$ is linear I, II*, Linear Algebra and Appl., **13** (1976), 207-221. Ibid., **11** (1975), 53-72.

6. O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc., **36** (1934), 53-92.

Received October 23, 1980 and in revised form July 9, 1981.

Université de lyon I

Adresse personnelle: 89, rue Garibaldi, 69006 LYON, France

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

DONALD BABBITT (Managing Editor)
University of California
Los Angeles, California 90024

HUGO ROSSI
University of Utah
Salt Lake City, UT 84112

C. C. MOORE and ARTHUR AGUS
University of California
Berkeley, CA 94720

J. DUGUNDJI
Department of Mathematics
University of Southern California
Los Angeles, California 90007

R. FINN and J. MILGRAM
Stanford University
Stanford, California 94305

ASSOCIATE EDITORS

R. ARNES E. F. BECKENBACH B. H. NEUMANN F. WOLF K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA
UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA, RENO
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF HAWAII
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

Printed in Japan by International Academic Printing Co,, Ltd., Thkyo Japan

Pacific Journal of Mathematics
Vol. 102, No. 1 January, 1982