Conspectus materiae tomi XXXIX, fasciculi 2

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-01338-9 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
XXXIX (1981)

Sur une classe de polynômes hyponormaux sur un corps fini

par

S. Agou (Lyon)

Dans ce qui suit on note $\boldsymbol{F}_{p^s}$ le corps fini à p^s éléments, par $\overline{\boldsymbol{F}}_p$ la clôture algébrique de $\boldsymbol{F}_{p^s}$.

0. Introduction. Les polynômes composés $f(g(X))$ où $f(X)$ est un polynôme irréductible de $\boldsymbol{F}_{p^s}[X]$ et où $g(X)$ est un polynôme non nul de $\boldsymbol{F}_{p^t}[X]$, t divisant s, de la forme $g(X) = \sum_{i=0}^{m} a_i X^{p^{ri}}$, que nous appelons un p^r-polynôme de $\boldsymbol{F}_{p^t}[X]$, ont été étudiés il y a fort longtemps avec des conditions restrictives liant les entiers r, s et t. Sans faire un historique détaillé et exhaustif de la question, on peut mentionner certains travaux de Serret, [11], parus en 1873 dans le cas $r = s = t = 1$; puis ceux de Dickson, [5], en 1887 dans le cas $t = 1$, $r = s$. Ensuite Ore, [10], en 1933, avec les conditions $r = s = t$, en introduisant la notion de p^s-polynôme de $\boldsymbol{F}_{p^s}[X]$, a considérablement fait avancer l'étude de ce type de polynômes. En s'appuyant sur la théorie d'Ore, en étendant des résultats de Dickson, [6], A. F. Long, [7], a montré que l'on pouvait expliciter les degrés des irréductibles de $\boldsymbol{F}_{p^s}[X]$, factorisant $f(X^{p^r} - X)$ sur $\boldsymbol{F}_{p^s}$ dans le cas $t = 1$, s divisant r. Généralisant ce précédent travail A. F. Long, [8], a montré que l'on pouvait régler le cas $t = 1$ avec r et s arbitraires, pour les polynômes $f(X^{p^r} - X)$ de $\boldsymbol{F}_{p^s}[X]$. En utilisant la notion d'hyponormalité définie dans cet article, nous avons généralisé, [2], le travail de Long en étudiant le polynôme $f(X^{p^r} - aX)$ de $\boldsymbol{F}_{p^s}[X]$, en n'imposant aucune condition aux entiers r, s, t, hormis bien entendu la condition t divisant s.

En s'appuyant sur la théorie d'Ore, A. F. Long et T. P. Vaughan, [9], ont donné des résultats sur la factorisation des polynômes $f(g(X))$ avec la condition $r \mid t$. Enfin, récemment, Carlitz et A. F. Long, [4], ont obtenu des résultats dans l'étude de certains polynômes à plusieurs indéterminées $X_1, \ldots, X_k$ sur un corps $\boldsymbol{F}_{p^s}$, lorsqu'on substitue à chaque indéterminée X_i, le même p^s-polynôme de $\boldsymbol{F}_{p^s}[X]$.

Par ailleurs, nous avons pu obtenir dans [3] et [3'], des conditions explicites d'irréductibilité des polynômes $f(X^{p^r} - aX)$ et $f(X^{p^{2r}} - aX^{p^r} - bX)$

sur un corps $\boldsymbol{F}_{p^s}$. Si on veut s'affranchir du cadre de la théorie d'Ore, pour atteindre les résultats les plus généraux, on est conduit naturellement *compte tenu des travaux précités*, à la notion de p^r-polynômes de $\boldsymbol{F}_{p^s}[X]$, avec r et s arbitraires, et à celle d'hyponormalité. Cet article a justement pour but de donner des résultats dans cette direction.

N. B. On trouvera dans les références ci-dessus une volumineuse bibliographie concernant ces questions.

1. Définition 1.1. On dit que $u \in \boldsymbol{F}_{p^s}[X]$ est *hyponormal sur* $\boldsymbol{F}_{p^s}$ si l'ensemble des $\boldsymbol{F}_{p^s}(x)$, où $x \in \overline{\boldsymbol{F}}_p$ est une racine de u, possède un plus petit élément (quand on l'ordonne par inclusion).

Soit $u(X) = u_1(X) \ldots u_l(X)$ la factorisation sur $\boldsymbol{F}_{p^s}$, en irréductibles, du polynôme $u(X)$. Il résulte aisément de cette définition que l'on a la propriété suivante.

Pour que le polynôme $u(X)$ soit hyponormal sur $\boldsymbol{F}_{p^s}$ il faut et il suffit qu'il existe un indice i, tel que le degré du polynôme $u_i(X)$ divise le degré du polynôme $u_j(X)$, pour tout entier j tel que $1 \leqslant j \leqslant l$.

Voici des exemples de polynômes hyponormaux. Soit $f \in \boldsymbol{F}_{p^s}[X]$ un polynôme irréductible, les polynômes $f(X^m)$ (cf. [1]), pour $m \in \boldsymbol{N}^*$, et $f(X^{p^r} - aX)$ pour $r \in \boldsymbol{N}^*$ et $a \in \boldsymbol{F}_{p^s}^{\times}$ sont hyponormaux; on reviendra plus loin sur ce dernier exemple.

Lemme 1.2. *Soit $f \in \boldsymbol{F}_{p^s}[X]$ un polynôme irréductible de degré n et soit $g \notin \boldsymbol{F}_{p^s}^*$ et $g \in \boldsymbol{F}_{p^s}[X]$; soit θ une racine de f dans $\boldsymbol{F}_{p^{sn}} = \boldsymbol{F}_{p^s}(\theta)$. Alors, pour que $f(g(X))$ soit hyponormal sur $\boldsymbol{F}_{p^s}$, il faut et il suffit que $g(X) - \theta$ soit hyponormal sur $\boldsymbol{F}_{p^{sn}}$.*

La condition est nécessaire. En effet, supposons $f(g(X))$ hyponormal sur $\boldsymbol{F}_{p^s}$. Il existe $x_0 \in \overline{\boldsymbol{F}}_p$ tel que $f(g(x_0)) = 0$ et que, pour toute racine x de $f(g(X))$, on ait

$$[\boldsymbol{F}_{p^s}(x_0) : \boldsymbol{F}_{p^s}] | [\boldsymbol{F}_{p^s}(x) : \boldsymbol{F}_{p^s}].$$

Le polynôme minimal de x_0 sur $\boldsymbol{F}_{p^s}$ se décompose dans $\boldsymbol{F}_{p^{sn}}[X]$ en produit de polynômes irréductibles de degrés $[\boldsymbol{F}_{p^s}(x_0) : \boldsymbol{F}_{p^s}]/n$.

De même, le polynôme minimal de x sur $\boldsymbol{F}_{p^s}$ se décompose dans $\boldsymbol{F}_{p^{sn}}[X]$ en produit de polynômes irréductibles de degrés $[\boldsymbol{F}_{p^s}(x) : \boldsymbol{F}_{p^s}]/n$. Alors $[\boldsymbol{F}_{p^s}(x_0) : \boldsymbol{F}_{p^s}]/n$ divise $[\boldsymbol{F}_{p^s}(x) : \boldsymbol{F}_{p^s}]/n$.

La condition est suffisante; si $g - \theta$ est hyponormal sur $\boldsymbol{F}_{p^{sn}}$, soit d_0 le degré d'un polynôme irréductible de $\boldsymbol{F}_{p^{sn}}[X]$ divisant $g - \theta$, d_0 divisant le degré de tout polynôme irréductible de $\boldsymbol{F}_{p^{sn}}[X]$, factorisant $g - \theta$. Il existe dans la décomposition de $f(g(X))$ en produit de polynômes irréductibles un facteur de degré $\delta_0 n$ tel que $\delta_0 n/\mathrm{pgcd}(\delta_0 n, n) = d_0$. Soit δn le degré d'un polynôme irréductible de $\boldsymbol{F}_{p^s}[X]$ factorisant $f(g(X))$; ce polynôme se décompose dans $\boldsymbol{F}_{p^{sn}}[X]$ en produit de facteurs irréductibles de degrés $d = \delta n/\mathrm{pgcd}(\delta n, n)$. L'un de ces facteurs divise $g - \theta$. Donc $\delta_0 n$, divise δn puisque d_0 divise d.

Définition 1.3. Soit $r \in \boldsymbol{N}^*$. On appelle *p^r-polynôme* à coefficients dans le corps fini $\boldsymbol{F}_{p^s}$, tout polynôme $g \in \boldsymbol{F}_{p^s}[X]$, non nul, de la forme

$$g(X) = \sum_{i=0}^{m} a_i X^{p^{ri}}.$$

On notera que dans cette définition, les entiers r et s ne sont liés par aucune condition.

2. On se propose, dans cette partie, d'établir le théorème suivant:

Théorème 2.0. *Soit $f(X)$ un polynôme irréductible de degré n de $\boldsymbol{F}_{p^s}[X]$ et soit $g(X)$ un p^r-polynôme de $\boldsymbol{F}_{p^s}[X]$. Alors le polynôme $f(g(X))$ est hyponormal sur $\boldsymbol{F}_{p^s}$.*

Avant d'aborder la démonstration de ce théorème, extrayons de [2] une partie des résultats obtenus dans l'étude des polynômes $f(X^{p^r} - aX)$, où $a \in \boldsymbol{F}_{p^s}^{\times}$.

Rappels 2.1. On a montré que dans la décomposition de $f(X^{p^r} - aX)$ en produit de facteurs irréductibles de $\boldsymbol{F}_{p^s}[X]$, trois cas et trois seulement apparaissaient, ces cas s'excluant d'ailleurs mutuellement.

1er cas. Il y a un unique polynôme irréductible de degré n de $\boldsymbol{F}_{p^s}[X]$, divisant $f(X^{p^r} - aX)$. Il existe un irréductible de $\boldsymbol{F}_{p^s}[X]$ de degré λn ($\lambda > 1$), divisant $f(X^{p^r} - aX)$ et tousles autres irréductibles de $\boldsymbol{F}_{p^s}[X]$ factorisant $f(X^{p^r} - aX)$, qui ne sont pas de degré n, ont des degrés multiples de λn.

2ème cas. Les degrés des polynômes irréductibles de $\boldsymbol{F}_{p^s}[X]$ factorisant $f(X^{p^r} - aX)$ sont les entiers de l'ensemble $\left\{n \dfrac{t}{(t, ns)}\right\}_{t|r}$.

3ème cas. Si k est l'unique entier tel que

$$\mathrm{pgcd}(r, snp^{k+1}) = p^k \mathrm{pgcd}(r, sn),$$

alors les degrés des polynômes irréductibles de $\boldsymbol{F}_{p^s}[X]$ factorisant $f(X^{p^r} - aX)$ sont les entiers de l'ensemble $\left\{np^{k+1} \dfrac{t}{(t, nsp^{k+1})}\right\}_{t|r}$.

Ceci étant on a le

Lemme 2.2. *Soient n et s des entiers > 0 et d un diviseur de sn. Le polynôme $u + vX + wX^{p^d}$ de $\boldsymbol{F}_{p^{sn}}[X]$ est hyponormal sur $\boldsymbol{F}_{p^{sn}}$.*

Preuve. Si $u + vX + wX^{p^d}$ a une racine dans $\boldsymbol{F}_{p^{sn}}$, il est évidemment hyponormal sur $\boldsymbol{F}_{p^{sn}}$. On va donc supposer que ce polynôme n'a pas de racine dans $\boldsymbol{F}_{p^{sn}}$. Les rappels montrent qu'alors on est dans le 3ème cas. $u + vX + wX^{p^d}$ se décompose donc en p^{d-1} facteurs irréductibles de $\boldsymbol{F}_{p^{sn}}[X]$ de degrés p, d'où l'hyponormalité sur $\boldsymbol{F}_{p^{sn}}$.

LEMME 2.3. *Soient $f(X)$ un polynôme irréductible de $F_{p^s}[X]$ de degré n, m un entier et d un diviseur de sn. Soit $g(X) = \sum_{i=0}^{m} a_i X^{p^{di}}$ un p^d-polynôme de $F_{p^s}[X]$. Alors le polynôme $f(g(X))$ est hyponormal sur F_{p^s}.*

Preuve. On raisonne par récurrence sur l'entier m. En vertu du lemme 1.2, il faut et il suffit de montrer que $\sum_{i=0}^{m} a_i X^{p^{di}} - \theta$ est hyponormal sur $F_{p^{sn}}$.

Si $m = 1$, $-\theta + a_0 X + a_1 X^{p^d}$ est hyponormal sur $F_{p^{sn}}$: c'est le lemme 2.2. Supposons donc $m \geqslant 2$ et l'hyponormalité sur $F_{p^{sn}}$ de tout polynôme de la forme $b + \sum_{i=0}^{M} a_i X^{p^{di}}$ de $F_{p^{sn}}[X]$, avec $M < m$. Si $\sum_{i=0}^{m} a_i X^{p^{di}} - \theta$ a une racine dans $F_{p^{sn}}$, l'hyponormalité sur $F_{p^{sn}}$ est immédiate. Supposons le contraire; soit μ_0 le degré d'un polynôme irréductible de $F_{p^{sn}}[X]$ divisant $\sum_{i=0}^{m} a_i X^{p^{di}} - \theta$, et qui soit minimal parmi les degrés μ des autres polynômes irréductibles de $F_{p^{sn}}[X]$ factorisant $\sum_{i=0}^{m} a_i X^{p^{di}} - \theta$.

Si $\sum_{i=0}^{m} a_i X^{p^{di}} - \theta | X^{p^{sn\mu_0}} - X$, alors $\mu | \mu_0$ et, comme $\mu \geqslant \mu_0$, on a $\mu = \mu_0$; d'où l'hyponormalité. De plus, on a $\mu_0 = p^{\alpha_0}$ $(1 \leqslant \alpha_0 \leqslant dm)$. Sinon, soit m' un entier tel que $m'sn \geqslant dm$ et premier à tous les degrés des polynômes irréductibles de $F_{p^{sn}}[X]$ divisant $\sum_{i=0}^{m} a_i X^{p^{di}} - \theta$.

On a dans $F_{p^{sn}}[X]$ la congruence

$$X^{p^{sn\mu_0 m'}} - X \equiv b + \sum_{i=0}^{m-1} b_i X^{p^{di}} \bmod \Big(\sum_{i=0}^{m} a_i X^{p^{di}} - \theta \Big).$$

Si $b + \sum_{i=0}^{m-1} b_i X^{p^{di}} = 0$, alors $\mu | \mu_0$, donc $\mu = \mu_0$, et μ_0 est une puissance de p;

Si $b + \sum_{i=0}^{m-1} b_i X^{p^{di}} \neq 0$, soit $\gamma(X) = \operatorname{pgcd}\big(X^{p^{sn\mu_0 m'}} - X, \sum_{i=0}^{m} a_i X^{p^{di}} - \theta\big)$; il est clair que $\gamma(X) - \gamma(0)$ est un p^d-polynôme de $F_{p^{sn}}[X]$; par hypothèse de récurrence, le polynôme $\gamma(X)$ est hyponormal sur $F_{p^{sn}}$; de plus il n'a pas de racine dans $F_{p^{sn}}$; μ_0 est donc le plus petit des degrés des polynômes irréductibles de $F_{p^{sn}}[X]$ factorisant $\gamma(X)$; μ_0 est donc une puissance de p, non nulle.

De même si $\sum_{i=0}^{m} a_i X^{p^{di}} - \theta | X^{p^{sn\mu}} - X$, alors $\mu_0 | \mu$ et le polynôme est hyponormal.

Sinon si $\sum_{i=0}^{m} a_i X^{p^{di}} - \theta \nmid X^{p^{sn\mu}} - X$, on a comme précédemment dans $F_{p^{sn}}[X]$ la congruence

$$X^{p^{sn\mu m'}} - X \equiv b' + \sum_{i=0}^{m-1} b'_i X^{p^{di}} \bmod \Big(\sum_{i=0}^{m} a_i X^{p^{di}} - \theta \Big).$$

Si $b' + \sum_{i=0}^{m-1} b'_i X^{p^{di}} = 0$, alors $\mu_0 | \mu$ et on a l'hyponormalité. Sinon, $\gamma'(X) = \operatorname{pgcd}\big(X^{p^{sn\mu m'}} - X, \sum_{i=0}^{m} a_i X^{p^{di}} - \theta\big)$, n'a pas de racine dans $F_{p^{sn}}$, mais possède, par hypothèse de récurrence, une racine de degré minimal p^a; on a donc $p^a | \mu$. D'autre part, on a $p^a \geqslant \mu_0$ et on a vu que μ_0 était toujours une puissance de p, non nulle. Il en résulte que $\mu_0 | p^a$ et a fortiori $\mu_0 | \mu$. ∎

On est maintenant en mesure de démontrer le théorème 2.0.

Preuve du théorème 2.0. Si $g(X) = \sum_{i=0}^{m} a_i X^{p^{ri}}$ est un p^r-polynôme de $F_{p^s}[X]$, on peut le considérer, si $d | (r, sn)$, comme un p^d-polynôme de $F_{p^s}[X]$, en écrivant

$$g(X) = \sum_{i=0}^{m} a_i X^{p^{d\left(\frac{r}{d} i\right)}} = \sum_{j=0}^{\frac{r}{d} m} b_j X^{p^{dj}}.$$

Le lemme 2.3 montre alors que $f(g(X))$ est hyponormal sur F_{p^s}. ∎

3. Un exemple de polynôme hyponormal mixte.

PROPOSITION 3.1. *Soient $f(X)$ un polynôme irréductible de $F_{p^s}[X]$, de degré n, r un entier, m un diviseur de $p^r - 1$, et a un élément de $F_{p^s}^{\times}$. Alors le polynôme $f((X^{p^r} - aX)^m)$ est hyponormal sur F_{p^s}.*

Preuve. Si $f(X) = X$ la proposition est évidente. Supposons donc $f(0) \neq 0$. Soit θ une racine de $f(X)$ dans $F_{p^{s \deg(f)}} = F_{p^{s'}} = F_{p^{sn}}$.

Le polynôme $X^m - \theta$ est hyponormal sur $F_{p^{s'}}$. Les degrés des irréductibles qui le factorisent dans $F_{p^{s'}}[X]$ sont de la forme $\nu = \frac{1}{s'}[h\sigma, \varrho, s']$ où ϱ est l'ordre de p dans $\left(\frac{\mathbf{Z}}{d\mathbf{Z}}\right)^{\times}$ avec $d|m$, où h est le plus petit entier tel que $\theta^{(p^{h\sigma}-1)/(m, p^{h\sigma}-1)} = 1$ et où σ est tel que $F_p(\theta) = F_{p^\sigma}$.

Soit maintenant f_ν un irréductible de degré ν factorisant $X^m - \theta$ dans $F_{p^{s'}}[X]$ et f_{ν_0} un irréductible de $F_{p^{s'}}[X]$ divisant $X^m - \theta$, et dont le degré ν_0 divise tous les degrés ν.

Si $a^{(p^{s'\nu_0}-1)/(p^{(r,s'\nu_0)}-1)} \neq 1$ alors $f_{\nu_0}(X^{p^r} - aX)$ possède dans sa factorisation un irréductible de degré ν_0, il en résulte que $(X^{p^r} - aX)^m - \theta$ est hyponormal sur $F_{p^{s'}}$ (cf. [2]).

On observera que dans ce cas l'hypothèse $m | p^r - 1$ n'est pas intervenue. Si $a^{(p^{s'\nu_0}-1)/(p^{(r,s'\nu_0)}-1)} = 1$ alors pour tout ν on a $a^{(p^{s'\nu}-1)/(p^{(r,s'\nu)}-1)} = 1$; La décomposition de $f_{\nu_0}(X^{p^r} - aX)$ ou de $f_\nu(X^{p^r} - aX)$ dépend alors de l'élément $\xi \in F_{p^{s'\nu_0}} \subset F_{p^{s'\nu}}$ tel que $\xi^{p^r - 1} = a$ et des quantités $\varrho_{\delta_{\nu_0}, d_{\nu_0}}(x_0)$ et $\varrho_{\delta_\nu, d_\nu}(x_0 \eta)$ où x_0 est une racine de f_{ν_0} où $\delta_\nu, d_\nu, \delta_{\nu_0}, d_{\nu_0}$ sont des entiers tels que: $d_\nu = (r, s'\nu)$, $\delta_\nu \cdot d_\nu = s'\nu$, et de même pour

$$d_{\nu_0} = (r, s'\nu_0), \qquad \delta_{\nu_0} \cdot d_{\nu_0} = s'\nu_0,$$

en observant que si x_0 est une racine de f_{ν_0} donc de $X^m - \theta$, $x_0\eta$ est une racine de $X^m - \theta$, lorsque η est une racine $m^{\text{ième}}$ de l'unité, et donc $\eta \in F_{p^r}^\times$ puisqu'il a été supposé que $m | p^r - 1$, et où enfin $\varrho_{\delta_\nu, d_\nu}(X)$ est le polynôme $\sum_{j=0}^{\delta_\nu - 1} (\xi^{-p^r} X)^{p^{d_\nu j}}$.

Compte tenu des expressions de ν et de $\nu_0 = \frac{[h\sigma, s']}{s'}$ on a:

$$r\delta_\nu = [r, s'\nu] = [h\sigma, s', r] \quad \text{car} \quad m | p^r - 1.$$

Ainsi δ_ν ne dépend pas de ν.

Comme

$$\varrho_{\delta_\nu, d_\nu}(x_0\eta) = \varrho_{\delta_\nu, r}(x_0\eta) \quad \text{et} \quad \varrho_{\delta_{\nu_0}, d_{\nu_0}}(x_0) = \varrho_{\delta_{\nu_0}, r}(x_0)$$

et que $\varrho_{\delta_\nu, r}(x_0\eta) = \eta \varrho_{\delta_{\nu_0}, r}(x_0)$ puisque $\delta_\nu = \delta_{\nu_0}$, on en déduit que les polynômes $f_\nu(X^{p^r} - aX)$ et $f_{\nu_0}(X^{p^r} - aX)$ ont des décompositions similaires dans $F_{p^{s'}}[X]$ lorsque $a^{(p^{s'\nu_0} - 1)/(p^{(r, s'\nu_0)} - 1)} = 1$.

Si $\varrho_{\delta_{\nu_0}, r}(x_0) = 0$ alors chaque $f_\nu(X^{p^r} - aX)$ comporte un irréductible de degré ν dans sa décomposition, d'où l'hyponormalité.

Si $\varrho_{\delta_{\nu_0}, r}(x_0) \neq 0$, il y a dans la factorisation de $f_\nu(X^{p^r} - aX)$ un irréductible de $F_{p^{s'}}[X]$ de degré $\nu p^{k_\nu + 1}$, divisant les degrés de tous les autres irréductibles factorisant $f_\nu(X^{p^r} - aX)$ où k_ν est l'entier tel que $\frac{r}{(r, s'\nu)} = p^{k_\nu} \cdot \omega_\nu$ avec $(\omega_\nu, p) = 1$.

On a donc

$$[r, s'\nu] = s'\nu p^{k_\nu} \cdot \omega_\nu \quad \text{et} \quad [r, s'\nu_0] = s'\nu_0 p^{k_{\nu_0}} \cdot \omega_{\nu_0}.$$

Comme $[r, s'\nu] = [r, s'\nu_0]$ il en résulte que

$$\nu p^{k_\nu} \cdot \omega_\nu = \nu_0 p^{k_{\nu_0}} \cdot \omega_{\nu_0} \quad \text{et donc} \quad p^{k_{\nu_0}} \,\Big|\, \frac{\nu}{\nu_0} p^{k_\nu}.$$

Par conséquent $\nu_0 p^{k_{\nu_0} + 1}$ divise $\nu p^{k_\nu + 1}$ ce qui établit l'hyponormalité dans ce cas là.

On a donc montré que le polynôme $(X^{p^r} - aX)^m - \theta$ était hyponormal sur $F_{p^{s'}}$, d'où, par le lemme 1.2, il résulte que $f\big((X^{p^r} - aX)^m\big)$ est hyponormal sur F_{p^s}. ■

Remarque. On constate que l'on peut donner une description complète des degrés pour $m = p^{r'} - 1$, où $r' | r$.

Bibliographie

[1] S. Agou, *Factorisation sur un corps fini F_{p^n} des polynômes composés $f(X^s)$ lorsque $f(X)$ est un polynôme irréductible de $F_{p^n}[X]$*, Enseignement Math. (2) 22 (1976), pp. 305–312.

[2] — *Factorisation sur un corps fini F_{p^n} des polynômes composés $f(X^{p^r} - aX)$ lorsque $f(X)$ est un polynôme irréductible de $F_{p^n}[X]$*, Journ. Number Theory 9 (1977), pp. 229–239.

[3] — *Irréductiblité des polynômes $f(X^{p^r} - aX)$ sur un corps fini F_{p^s}*, Journ. Reine Angew. Math. 292 (1977), pp. 191–195.

[3′] — *Irréductiblité des polynômes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini F_{p^s}*, Journ. Number Theory 10 (1976), pp. 64–69.

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

[5] L. E. Dickson, *Higher irreducible congruences*, Bull. Amer. Math. Soc. 3 (1897), pp. 381–389.

[6] — *Linear groups with an exposition of the Galois Field Theory*, Dover, New York 1958.

[7] A. F. Long, *Factorization of irreducible polynomials over a finite field with the substitution $x^{q^r} - x$ for x*, Acta Arith. 25 (1973), pp. 65–80.

[8] — *Factorization of irreducible polynomials over a finite field with the substitution $x^{p^r} - x$ for x*, Duke Math. J. 40 (1973), pp. 63–76.

[9] A. F. Long and T. P. Vaughan, *Factorization of $Q\big(h(T(x))\big)$ over GF(q) where $Q(x)$ is irreducible an $h(T)(x)$ is linear II*, Linear Algebra and its applications 11 (1975), pp. 53–72.

[10] O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. 36 (1934), pp. 243–274.

[11] J. A. Serret, *Détermination des fonctions entières irréductibles suivant un module premier, dans le cas où le degré est égal au module*, Journal de Mathématiques, (2) 18 (1873), p. 301–305.

Reçu le 15.3.1978
et dans la forme modifiée le 10.7.1978 (1054)