JOURNAL OF NUMBER THEORY 11, 20 (1979)

Irréductibilité Des Polynômes $f(X^{p^{2r}} - aX^{p^r} - bX)$ Sur un Corps Fini $\mathbb{F}_{p^s}$

SIMON AGOU

Département de Mathématiques, Université Claude Bernard – Lyon 1 43, boulevard du 11 novembre 1918 69621 – Villeurbanne France

Communicated by P. Roquette

Received May 10, 1978

Nous donnons ci-dessous des précisions complémentaires concernant le travail paru dans le tome n° 10 (78) pp. 64–69 du Journal of Number Theory.

Lorsque le polynôme $X^3 - aX - b$ est irréductible sur $\mathbb{F}_{2^s}$, il n'existe pas de polynôme $X^n + BX^{n-1} + \cdots$ de $\mathbb{F}_{2^s}[X]$ satisfaisant à la condition $\sum_{k=0}^{3s-1} (\beta^{-2}B)^{2^k} = 1$, et par conséquent pour tout irréductible f de $\mathbb{F}_{2^s}[X]$ le polynôme $f(X^4 - aX^2 - bX)$ n'est pas irréductible sur $\mathbb{F}_{2^s}$. En effet si $u \in \mathbb{F}_{2^{3s}}^{\times}$ on a la congruence:

$$\sum_{k=0}^{3s-1} (uX)^{2^k} \equiv \sum_{k=0}^{s-1} ((u + u^{2^s} + u^{2^{2s}})X)^{2^k} \mod (X^{2^s} - X).$$

Il en résulte que si $\mathrm{Tr}(u) = u + u^{2^s} + u^{2^{2s}} = 0$ alors le polynôme $\sum_{k=0}^{3s-1} (uX)^{2^k} - 1$ n'a pas de racine dans $\mathbb{F}_{2^s}$. Si $X^3 - aX - b$ est irréductible sur $\mathbb{F}_{2^s}$, alors le polynôme minimal sur $\mathbb{F}_{2^s}$ de β^{-2} est $b^4X^3 + a^2X + 1$, et par conséquent le polynôme $\sum_{k=0}^{3s-1} (\beta^{-2}X)^{2^k} - 1$ n'a pas de racine dans $\mathbb{F}_{2^s}$ puisque $\mathrm{Tr}(\beta^{-2}) = 0$. Par contre si $X^3 - aX - b$ n'est pas irréductible sur $\mathbb{F}_{2^s}$, il existe bien entendu toujours un irréductible de $\mathbb{F}_{2^s}[X]$ de la forme $f(X^4 - aX^2 - bX)$ pourvu que B soit différent de 0. En effet on a l'égalité $\sum_{k=0}^{s-1} (BX^2)^{2^{k+1}} - \sum_{k=0}^{s-1} (BX^2)^{2^k} = B(X^{2^s} - X)^2$. Il en résulte que le polynôme $\sum_{k=0}^{s-1} (BX^2)^{2^k} - 1$ a, pour $B \neq 0$, 2^{s-1} racines dans $\mathbb{F}_{2^s}^{\times}$. Si β^{-1} est l'une de ces racines, le même raisonnement montre que le polynôme $\sum_{k=0}^{s-1} (\beta X^2)^{2^k} - 1$ a également 2^{s-1} racines dans $\mathbb{F}_{2^s}^{\times}$. On peut donc énoncer la:

PROPOSITION. *Soit $f(X) = X^n + BX^{n-1} + \cdots$ un polynôme irréductible de $\mathbb{F}_{p^s}[X]$. Pour que le polynôme $f(X^{p^{2r}} - aX^{p^r} - bX)$ soit irréductible sur $\mathbb{F}_{p^s}$ il faut et il suffit que : $p = 2$, $r = 1$, n impair, $B \neq 0$, et en outre que p.g.c.d. $(X^3 - aX - b, X^{2^s} - X) \neq 1$, $\sum_{k=0}^{s-1} (\beta^{-2}B)^{2^k} = 1$ et $\sum_{k=0}^{s-1} (\alpha^{-2}\beta)^{2^k} = 1$, où α et β sont deux éléments de $\mathbb{F}_{2^s}^{\times}$ tels que $\alpha^2 + \beta = a$ et $\alpha\beta = b$.*

0022-314X/79/010020-01$02.00/0