Canad. Math. Bull. Vol. **23** (2), 1980

IRRÉDUCTIBILITÉ DES POLYNÔMES $f\left(\sum_{i=0}^{m} a_i X^{p^{ri}}\right)$ SUR UN CORPS FINI $\mathbb{F}_{p^s}$.

PAR

S. AGOU

0. **Introduction.** Dans ce qui suit $f(X)$ désigne un polynôme irréductible de degré n de $\mathbb{F}_{p^s}[X]$, et $\sum_{i=0}^{m} a_i X^{p^{ri}}$ un polynôme de $\mathbb{F}_{p^s}[X]$ tel que $a_0 \neq 0$ et r désigne un entier non nul.

On montre dans cet article que les polynômes $f(\sum_{i=0}^{m} a_i X^{p^{ri}})$ ne sont pas irréductibles sur $\mathbb{F}_{p^s}$ pour $m \geq 3$.

Il est loisible de supposer que $a_m = 1$. Ces notations et hypothèses seront utilisées tout au long de ce travail.

Enfin, pour $1 \leq m \leq 2$, cette étude a été faite dans [1], [2], [3], ce qui fait que le problème général de *l'irréductibilité des polynômes* $f(\sum_{i=0}^{m} a_i X^{p^{ri}})$ est complètement résolu.

1. **Lemmes préliminaires.**

1.1. LEMME. *Soient m et r deux entiers, avec $m \geq 8$, et p un nombre premier. On désigne par u l'entier tel que $p^{u-1} < m \leq p^u$. Alors $p^{mr-u-1} > mr$.*

En effet si $m \geq 8$, on a, par récurrence sur l'entier m l'inégalité $2^m \geq 4m^2$. Mais $2^{mr} \geq 2^m \cdot r$ donc $2^{mr} \geq 4m^2 r$. Finalement $p^{mr-2} \geq 2^{mr-2} \geq m^2 r$, et donc $p^{mr} \geq p^2 m^2 r > p^{u+1} mr$. Il résulte de ce lemme que si $p^{mr-u-1} \mid mr$ alors $m < 8$.

1.2. LEMME. *Soient m et r deux entiers, tels que $3 \leq m \leq 7$ et p un nombre premier. Soit u l'entier tel que $p^{u-1} < m \leq p^u$. Pour que p^{mr-u-1} divise mr il faut et il suffit que $m = 3, p = 2, r = 1$ ou $m = 3, p = 3, r = 1$ ou $m = 4, p = 2, r = 1$.*

Pour établir ce lemme fastidieux nous allons examiner les différents cas.

. si $m = 3$ et $p = 2$ alors $u = 2$. Si $2^{3r-3} \mid 3r$, on a $2^{3r-3} = 3r - 2$ ou $2^{3r-3} = 3r$ car $2^{3r-3} \geq 3r - 2$. Par suite on a $2^{3r-3} = 3r - 2$. Si $r > 1$ on a $2^{3(r-1)} \geq 8(r-1) > 3r - 2$, par conséquent la seule solution est $r = 1$.

. si $m = 3$ et $p \geq 3$ alors $u = 1$. Si $p^{3r-2} \mid 3r$ on a $p^{3r-2} = 3r$ et donc $p = 3$. L'égalité $3^{3r-2} = 3r$ fournit alors $r = 1$, car si $r > 1$ on a $3^{3r-3} > 2^{3r-3} \geq 8(r-1) > r$.

Reçu par les rédacteurs le 3 janvier 1979.

. si $m=4$ et $p=2$ alors $u=2$. Si $2^{4r-3} \mid 4r$ on a $r=1$ car $2.2^{4(r-1)} \geq 32(r-1)$ et donc $32(r-1) \leq 4r$.

. si $m=4$ et $p \geq 3$ alors $u \leq 2$. Si $p^{4r-3} \mid 4r$ on a $p^{4r-3}=4r$ et donc $p=2$, ce qui est contradictoire.

. si $m=5$ et $p=2$ alors $u=3$. Si $2^{5r-4} \mid 5r$, $2^{5r-4}=2.2^{5(r-1)} \geq 64(r-1)$ on déduit que $5r \geq 64(r-1)$ et donc $r=1$, ce qui est impossible car $2 \nmid 5$.

. si $m=5$ et $p=3$ alors $u=2$. Si $3^{5r-3} \mid 5r$ on a $9.3^{5(r-1)} > 9.2^5 \cdot (r-1)$ d'où $9.2^5(r-1) \leq 5r$, par suite $r=1$, ce qui est impossible car $3^2 \nmid 5$.

. si $m=5$ et $p \geq 5$ alors $u=1$. Si $p^{5r-2} \mid 5r$ on a $p^3 \cdot p^{5(r-1)} > 8.2^5(r-1)$ ce qui donne $r=1$, ce qui est à rejeter car $p^3 \nmid 5$.

. si $m=6$ et $p=2$ alors $u=3$. Si $2^{6r-4} \mid 6r$ alors $2^8(r-1) \leq 6r$ d'où $r=1$, mais alors $2^2 \nmid 6$.

. si $m=6$ et $3 \leq p \leq 5$ alors $u=2$. Si $p^{6r-3} \mid 6r$ alors $2^9(r-1) < 6r$ et donc $r=1$, mais $p^3 \nmid 6$.

. si $m=6$ et $p>5$ et si $p^{6r-2} \mid 6r$ alors $2^{10}(r-1) < 6r$ d'où $r=1$, mais $p^4 \nmid 6$.

Enfin si $m=7$ et $p=2$ alors $u=3$. Si $2^{7r-4} \mid 7r$ on a $2^{10}(r-1) \leq 7r$ donc $r=1$, mais $2^3 \nmid 7$.

si $m=7$ et $p=3$ ou 5 alors $u=2$. Si $p^{7r-3} \mid 7r$ on a $2^{11}(r-1) < 7r$ d'où $r=1$, mais $p^4 \nmid 7$.

si $m=7$ et $p>5$ alors $u=1$. Si $p^{7r-2} \mid 7r$ on a $2^{12}(r-1) < 7r$ et donc $r=1$, mais $p^5 \nmid 7$.

2. Nous allons dans ce paragraphe donner des précisions sur le degré d'une extension de $\mathbb{F}_{p^s}$ contenant les racines du polynôme $f(\sum_{i=0}^{m} a_i X^{p^{ri}})$.

2.1. Proposition. *Désignons par* $g(X)$ *le polynôme* $\sum_{i=0}^{m} a_i X^{p^{ri}}$, *et par* u *l'entier tel que* $p^{u-1} < m \leq p^u$. *Alors il existe un entier* $\rho > 0$ *tel que* $f(g(X)) \mid X^{q^{p^{u+1}(q^{\rho}-1)}} - X$ *où* $q = p^{[mr,sn]}$.

Pour tout entier j, $1 \leq j \leq m+1$, et tout entier k, $0 \leq k \leq m-1$, il existe des éléments $\alpha_{j,k} \in \mathbb{F}_{p^s}$ tels que:

$$X^{q^j} \equiv \sum_{k=0}^{m-1} \alpha_{j,k} X^{p^{rk}} \mod g(X).$$

Comme $a_0 \neq 0$, en particulier les coefficients $\alpha_{1,k}$ pour $0 \leq k \leq m-1$ ne sont pas simultanément nuls.

Il en résulte que la matrice $M=(\alpha_{j,k})_{\substack{1 \leq j \leq m \\ 0 \leq k \leq m-1}}$ de $\mathfrak{M}_m(\mathbb{F}_{p^s})$ a un rang ≥ 1. Il existe par conséquent, des éléments λ_j, $1 \leq j \leq m+1$, de $\mathbb{F}_{p^s}$, non simultanément nuls tels que:

$$\sum_{j=1}^{m+1} \lambda_j X^{q^j} \equiv 0 \mod g(X).$$

https://doi.org/10.4153/CMB-1980-028-7 Published online by Cambridge University Press

Comme $g(X)$ a des racines simples, il en résulte que:

$$\sum_{j=0}^{m} \lambda_{j+1} X^{q^j} \equiv 0 \mod g(X).$$

Considérons alors le polynôme non nul $\sum_{j=0}^{m} \lambda_{j+1} X^j$ de $\mathbb{F}_{p^s}[X] \subset \mathbb{F}_q[X]$. Il est clair que l'ordre de multiplicité maximal d'une racine de ce polynôme est au plus m. Si on considère le produit des irréductibles de $\mathbb{F}_{p^s}[X]$ divisant le polynôme $\sum_{j=0}^{m} \lambda_{j+1} X^j$, il est clair qu'il existe un corps $\mathbb{F}_{q^\rho}$ contenant toutes les racines de ce polynôme, et la remarque précédente montre que $\sum_{j=0}^{m} \lambda_{j+1} X^j \mid (X^{q^\rho} - X)^{p^u}$. Mais alors, la théorie d'Ore [4] montre que

$$\sum_{j=0}^{m} \lambda_{j+1} X^{q^j} \mid X^{q^{q^\rho p^u}} - X^{q^{p^u}}.$$

A fortiori $g(X)$ divise $X^{q^{q^\rho p^u}} - X^{q^{p^u}}$. Mais $g(X)$ n'a que des racines simples, il en résulte que:

$$g(X) \mid X^{q^{p^u(q^\rho - 1)}} - X.$$

Par hypothèse $f(X)$ est irréductible sur $\mathbb{F}_{p^s}$, par suite $f(X) \mid X^q - X$. Ainsi $f(g(X)) \mid (g(X))^q - g(X) = g(X^q - X)$, et donc

$$f(g(X)) \mid (X^q - X)^{q^{p^u(q^\rho - 1)}} - (X^q - X) = (X^{q^{p^u(q^\rho - 1)}} - X)^q - (X^{q^{p^u(q^\rho - 1)}} - X).$$

Il en découle aisément que

$$X^{q^{p^{u+1}(q^\rho - 1)}} - X \equiv 0 \mod f(g(X)) \quad c.q.f.d.$$

Observons que pour une valeur donnée de m, il est possible de mieux préciser l'entier ρ et éventuellement de réduire l'exposant de p dans l'entier $p^{u+1}(q^\rho - 1)$, suivant les valeurs de p.

3. Nous allons supposer dans ce paragraphe le polynôme $f(g(X))$ irréductible sur $\mathbb{F}_{p^s}$, avec toujours $g(X) = \sum_{i=0}^{m} a_i X^{p^{ri}}$ et $m \geq 3$. Si θ désigne une racine de $f(X)$, cela équivaut à l'irréductibilité de $g(X) - \theta$ sur $\mathbb{F}_{p^{sm}}$. La proposition 2.1 fournit alors la condition nécessaire: $p^{mr} \mid mrp^{u+1}$ soit $p^{mr-u-1} \mid mr$, avec u tel que $p^{u-1} < m \leq p^u$. Les cas $m = 1$ et $m = 2$ ayant été réglés dans [1], [2], [3], le lemme 1.2 montre qu'il suffit d'examiner les cas $m = 3$ et $m = 4$.

3.1. Etude du cas $m = 3$.

Soient α, β, γ des éléments de $\bar{\mathbb{F}}_p$ tels que:

$$X^{p^3} - a_2 X^{p^2} - a_1 X^p - a_0 X = (g_\gamma \circ g_\beta \circ g_\alpha)(X)$$

avec $g_\alpha(X) = X^p - \alpha X$, $g_\beta(X) = X^p - \beta X$, $g_\gamma(X) = X^p - \gamma X$. On a alors les relations:

$$(\mathrm{I}) \quad \begin{cases} \alpha^{p^2} + \beta^p + \gamma = a_2 \\ (\alpha\beta)^p + \alpha^p \gamma + \beta\gamma = -a_1 \\ \alpha\beta\gamma = a_0. \end{cases}$$

https://doi.org/10.4153/CMB-1980-028-7 Published online by Cambridge University Press

Ce système est équivalent à:

$$\text{(II)} \quad \begin{cases} \alpha^{p^2+p+1} - a_2\alpha^{p+1} - a_1\alpha - a_0 = 0 \\ \beta^{p+1} + (\alpha^{p^2} - a_2)\beta + a_0\alpha^{-1} = 0 \\ \alpha\beta\gamma = a_0. \end{cases}$$

3.1.1. Etude du cas $m=3$, $p=2$, $r=1$.

Le système II) s'écrit

$$\begin{cases} \alpha^7 - a_2\alpha^3 - a_1\alpha - a_0 = 0 \\ \beta^3 + (\alpha^4 - a_2)\beta + a_0\alpha^{-1} = 0 \\ \alpha\beta\gamma = a_0. \end{cases}$$

Si le polynôme $X^8 - a_2X^4 - a_1X^2 - a_0X - \theta$ est irréductible sur $\mathbb{F}_{2^{sn}}$, ses racines sont dans $\mathbb{F}_{2^{8sn}}$. Soit x une racine de ce polynôme; si y est une racine de $X^8 - a_2X^4 - a_1X^2 - a_0X$ alors $x+y$ est une racine de $g(X) - \theta$ donc $y \in \mathbb{F}_{2^{8sn}}$. Il en résulte que $X^7 - a_2X^4 - a_1X - a_0$ a toutes ses racines dans $\mathbb{F}_{2^{8sn}}$. Ce polynôme a évidemment des racines simples, il en résulte qu'il a nécessairement une racine dans $\mathbb{F}_{2^{sn}}$. On peut donc supposer que $\alpha \in \mathbb{F}_{2^{sn}}$.

Le polynôme $X^3 + (\alpha^4 - a_3)X + a_0\alpha^{-1}$ de $\mathbb{F}_{2^{sn}}[X]$ ne peut avoir de racines dans $\mathbb{F}_{2^{sn}}$, car si c'était le cas on pourrait choisir α, β, γ dans $\mathbb{F}_{2^{sn}}$ et on sait (cf. [1]) qu'alors le polynôme $(g_\gamma \circ g_\beta \circ g_\alpha)(X) - \theta$ ne peut être irréductible sur $\mathbb{F}_{2^{sn}}$. Par conséquent $X^3 + (\alpha^4 - a_2)X + a_0\alpha^{-1}$ est irréductible sur $\mathbb{F}_{2^{sn}}$. On peut donc supposer que α, β, γ sont dans $\mathbb{F}_{2^{3sn}}$.

Mais $X^8 - a_2X^4 - a_1X^2 - a_0X - \theta = (g_\gamma \circ g_\beta \circ g_\alpha)(X) - \theta$ est a fortiori irréductible sur $\mathbb{F}_{2^{3sn}}$ ce qui ne se peut pas ([1]). Ainsi $f(X^8 - a_2X^4 - a_1X^2 - a_0X)$ ne peut être irréductible sur $\mathbb{F}_{2^s}$.

3.1.2. Etude du cas $m=3$, $p=3$, $r=1$.

Le système II) s'écrit:

$$\begin{cases} \alpha^{13} - a_2\alpha^4 - a_1\alpha - a_0 = 0 \\ \beta^4 + (\alpha^9 - a_2)\beta + a_0\alpha^{-1} = 0 \\ \alpha\beta\gamma = a_0. \end{cases}$$

Par hypothèse $X^{27} - a_2X^9 - a_1X^3 - a_0X - \theta$ est irréductible sur $\mathbb{F}_{3^{sn}}$, ses racines sont donc dans $\mathbb{F}_{3^{27sn}}$. Par un raisonnement déjà vu, il en résulte que:

$$X^{27} - a_2X^9 - a_1X^3 - a_0X \mid X^{3^{27sn}} - X.$$

Par conséquent $X^{26} - a_2X^8 - a_1X^2 - a_0$ a une racine dans $\mathbb{F}_{3^{sn}}$. A fortiori $h(X) = X^{13} - a_2X^4 - a_1X^2 - a_0$ a une racine dans $\mathbb{F}_{3^{sn}}$ car $h(X^2) = X^{26} - a_2X^8 - a_1X^2 - a_0$. On peut donc supposer que $\alpha \in \mathbb{F}_{3^{sn}}$: Si $X^4 + (\alpha^9 - a_2)X + a_0\alpha^{-1}$, qui est un polynôme de $\mathbb{F}_{3^{sn}}[X]$, a une racine dans $\mathbb{F}_{3^{sn}}$, alors on peut supposer que $\alpha, \beta, \gamma \in \mathbb{F}_{3^{sn}}$ et $g_\gamma \circ g_\beta \circ g_\alpha(X) - \theta$ ne peut être irréductible sur $\mathbb{F}_{3^{sn}}$([1]). Ainsi $X^4 + (\alpha^9 - a_2)X + a_0\alpha^{-1}$ n'a pas de racines dans

$\mathbb{F}_{3^{sn}}$, il en découle, que ce polynôme a toutes ses racines dans $\mathbb{F}_{3^{4sn}}$. Ainsi on peut supposer que α, β, γ appartiennent à $\mathbb{F}_{3^{4sn}}$. Mais $X^{27}-a_2X^9-a_1X^3-a_0X-\theta$ est irréductible sur $\mathbb{F}_{3^{4sn}}$, d'où une contradiction. (cf [1]). Il résulte de tout ce qui précède que les polynômes $f(X^{p^{3r}}-a_2X^{p^{2r}}-a_1X^{p^r}-a_0X)$ ne sont pas irréductibles sur $\mathbb{F}_{p^s}$.

3.2. Etude du cas $m=4, p=2, r=1$.

Définissons des éléments $\alpha, \beta, \gamma, \delta$ de $\bar{\mathbb{F}}_2$ par l'égalité:

$$g(X)=X^{2^4}-a_3X^{2^3}-a_2X^{2^2}-a_1X^2-a_0X=(g_\delta\circ g_\gamma\circ g_\beta\circ g_\alpha)(X).$$

avec toujours $g_\alpha(X)=X^2-\alpha X$, $g_\beta(X)=X^2-\beta X$, $g_\gamma(X)=X^2-\gamma X$, $g_\delta(X)=X^2-\delta X$.

On a donc le système:

$$\text{(I)}\quad\begin{cases}\alpha^8+\beta^4+\gamma^2+\delta=a_3\\ \alpha^4\beta^4+\alpha^4\gamma^2+\alpha^4\delta+\beta^2\gamma^2+\beta^2\delta+\gamma\delta=-a_2\\ (\alpha\beta\gamma)^2+\delta(\alpha^2\beta^2+\alpha^2\gamma+\beta\gamma)=a_1\\ \alpha\beta\gamma\delta=-a_0.\end{cases}$$

Ce système est équivalent au système:

$$\text{(II)}\quad\begin{cases}\alpha^{15}-a_3\alpha^7-a_2\alpha^3-a_1\alpha-a_0=0,\\ \beta^7-(a_3-\alpha^8)\beta^3-(a_2+a_3\alpha^4+\alpha^{12})\beta+a_0\alpha^{-1}=0,\\ \gamma^3+(\beta^4-a_3+\alpha^8)\gamma-a_0\alpha^{-1}\beta^{-1}=0,\\ \alpha\beta\gamma\delta=-a_0.\end{cases}$$

Par hypothèse le polynôme $X^{16}-a_3X^8-a_2X^4-a_1X^2-a_0X-\theta$ est irréductible sur $\mathbb{F}_{2^{sn}}$, donc a ses racines dans $\mathbb{F}_{2^{16sn}}$, il en résulte que $X^{16}-a_3X^8-a_2X^4-a_1X^2-a_0X$ a ses racines dans $\mathbb{F}_{2^{16sn}}$. Par suite les irréductibles de $\mathbb{F}_{2^{sn}}[X]$ divisant $X^{15}-a_3X^7-a_2X^3-a_1X-a_0$ ont des degrés divisant 16. Ils ne peuvent donc pas être tous pairs. Donc ce polynôme a une racine dans $\mathbb{F}_{2^{sn}}$. On peut donc supposer que $\alpha\in\mathbb{F}_{2^{sn}}$. Le polynôme $g_\delta\circ g_\gamma\circ g_\beta(X)-\theta$ de $\mathbb{F}_{2^{sn}}[X]$ est irréductible sur $\mathbb{F}_{2^{sn}}$ car $(g_\delta\circ g_\gamma\circ g_\beta)(g_\alpha(X))-\theta$ l'est par hypothèse. Par suite $g_\delta\circ g_\gamma\circ g_\beta(X)-\theta$ a ses racines dans $\mathbb{F}_{2^{8sn}}$, et donc $g_\delta\circ g_\gamma\circ g_\beta(X)$ a ses racines dans $\mathbb{F}_{2^{8sn}}$. Les degrés des irréductibles de $\mathbb{F}_{2^{sn}}[X]$ factorisant $g_\delta\circ g_\gamma\circ g_\beta(X)/X$ ne pouvant être tous pairs il en résulte que le polynôme $X^7-(a_3-\alpha^8)X^3-(a_2+a_3\alpha^4+\alpha^{12})X+a_0\alpha^{-1}$ a une racine dans $\mathbb{F}_{2^{sn}}$. On peut donc supposer que $\beta\in\mathbb{F}_{2^{sn}}$.

Mais $(g_\delta\circ g_\gamma(X))/X=X^3+(\beta^4+a_3+\alpha^8)X+a_0\alpha^{-1}\beta^{-1}$. Par suite $g_\delta\circ g_\gamma(X)-\theta\in\mathbb{F}_{2^{sn}}[X]$; ce polynôme est par conséquent irréductible sur $\mathbb{F}_{2^{sn}}$. Il en résulte que γ et $\delta\in\mathbb{F}_{2^{sn}}$ [(3)] et l'irréductibilité de $g_\delta\circ g_\gamma\circ g_\beta\circ g_\alpha(X)-\theta$ sur $\mathbb{F}_{2^{sn}}$ est impossible ([1]).

https://doi.org/10.4153/CMB-1980-028-7 Published online by Cambridge University Press

4. On peut donc énoncer la

PROPOSITION. *Soient f un irréductible de degré n de $\mathbb{F}_{p^s}[X]$, m un entier ≥ 3, et $r \in \mathbb{N}^*$, et $\sum_{i=0}^{m} a_i X^{p^{ri}}$ un polynôme de $\mathbb{F}_{p^s}[X]$. Alors le polynôme $f(\sum_{i=0}^{m} a_i X^{p^{ri}})$ n'est pas irréductible sur $\mathbb{F}_{p^s}$.*

BIBLIOGRAPHIE

1. S. Agou, *Irréductibilité des polynômes $f(X^{p^r} - aX)$ sur un corps fini $\mathbb{F}_{p^s}$.* Jal. für die reine und angewandt Mathematik. 1977. **292.** pp. 191–195.

2. S. Agou, *Irréductibilité des polynômes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini $\mathbb{F}_{p^s}$.* Jal. of Number theory. Vol. **10,** n° 1 pp. 64–69. (1978).

3. S. Agou, *Irréductibilité des polynômes $f(X^{p^{2r}} - aX^{p^r} - bX)$ sur un corps fini $\mathbb{F}_{p^s}$.* Additif. Jal of Number theory. Vol. **11,** No. 1, 20, 1979.

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

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ DE LYON I
43 Bd DU 11 NOVEMBRE 1918
69621 VILLEURBANNE (FRANCE)