Conspectus materiae tomi XXX, fasciculi 3

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 geboten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

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
XXX (1976)

Critères d'irréductibilite des polynômes composés à coefficients dans un corps fini

par

SIMON AGOU (Lyon)

Dans ce qui suit, on considère un polynôme irréductible monique $f \in \boldsymbol{F}_q[X]$, où $\boldsymbol{F}_q$ est le corps fini ayant $q = p^s$ éléments, où p est premier. On étudie l'irréductibilité des polynômes composés $f(g(X))$, obtenus en substituant divers polynômes moniques $g(X) \in \boldsymbol{F}_q[X]$ à X dans $f(X)$.

Je remercie M. L. Carlitz pour les suggestions et les indications bibliographiques qu'il m'a communiquées au cours de la rédaction de cet article.

1. Un lemme fondamental.

1.1. LEMME. *Soient f, $g \in \boldsymbol{F}_q[X]$ des polynômes moniques de degrés respectifs $n \geqslant 1$ et $m \geqslant 1$; on suppose f irréductible. Pour que le polynôme $f(g(X))$ soit irréductible dans $\boldsymbol{F}_q[X]$, il faut et il suffit que les coefficients dans $\boldsymbol{F}_q[X]$ du polynôme*

$$h(X, Y) = \prod_{k=0}^{m-1} (Y - X^{q^{kn}}) - g(Y) + g(0) - (-1)^m X^{(q^{mn}-1)/(q^n-1)} \in \boldsymbol{F}_q[X][Y]$$

appartiennent à l'idéal $f(g(X))\,\boldsymbol{F}_q[X]$.

On note $\overline{\boldsymbol{F}}_p$ la clôture algébrique $\bigcup_{r>0} \boldsymbol{F}_{p^r}$ de $\boldsymbol{F}_p$.

Montrons que la condition est nécessaire. Comme f et $f(g(X))$ sont irréductibles, il existe $\theta \in \boldsymbol{F}_{q^n}$ et $\xi \in \boldsymbol{F}_{q^{mn}}$ tels que

$$f(X) = \prod_{j=0}^{n-1} (X - \theta^{q^j}) \quad \text{et} \quad f(g(X)) = \prod_{i=0}^{mn-1} (X - \xi^{q^i}).$$

Puisque ξ est racine de

$$f(g(X)) = \prod_{j=0}^{n-1} (g(X) - \theta^{q^j}),$$

il existe un unique j tel que $0 \leqslant j \leqslant n-1$ et tel que $g(\xi) = \theta^{q^j}$. Les racines de $g(X) - \theta^{q^j}$ sont les $\xi^{q^{kn}}$ $(0 \leqslant k \leqslant m-1)$; on a ainsi

$$g(X) - \theta^{q^j} = \prod_{k=0}^{m-1} (X - \xi^{q^{kn}}), \qquad \theta^{q^j} = g(0) - (-1)^m N_{\boldsymbol{F}_{q^{mn}}/\boldsymbol{F}_{q^n}}(\xi)$$

et

$$g(X) - \theta^{q^j} = g(X) - g(0) + (-1)^m N_{\boldsymbol{F}_{q^{mn}}/\boldsymbol{F}_{q^n}}(\xi).$$

Ceci montre que $h(\xi, Y) = 0$. Les coefficients dans $\boldsymbol{F}_q[X]$ du polynôme h ont donc ξ pour racine et, par suite, sont divisibles dans $\boldsymbol{F}_q[X]$ par le polynôme minimal $f(g(X))$ de ξ sur $\boldsymbol{F}_q$.

La condition est suffisante. Soit $\xi \in \overline{\boldsymbol{F}}_p$ une racine du polynôme $f(g(X))$. On a par hypothèse $h(\xi, Y) = 0$, c'est-à-dire $\prod_{k=0}^{m-1} (X - \xi^{q^{kn}}) = g(X) - \theta$, en posant $\theta = g(0) - (-1)^m \xi^{(q^{mn}-1)/(q^n-1)}$. Les coefficients du polynôme $g(X) - \theta$ appartiennent à $\boldsymbol{F}_q$, à l'exception peut-être du terme constant $g(0) - \theta$. Par suite, pour tout $j \geqslant 0$, on a $g(X) - \theta^{q^j} = \prod_{k=0}^{m-1} (X - \xi^{q^j + kn})$. Comme $f(g(\xi)) = 0$ et $g(\xi) = \theta$, les racines de $f(X)$ dans $\boldsymbol{F}_{q^n}$ sont $\theta, \theta^q, \ldots, \theta^{q^{n-1}}$ et on a ainsi

$$f(g(X)) = \prod_{j=0}^{n-1} (g(X) - \theta^{q^j}) = \prod_{i=0}^{mn-1} (X - \xi^{q^i}).$$

Posons $g(X) = X^m + aX^{m-1} + \ldots$ D'après l'hypothèse, $f(g(X))$ divise le coefficient dominant (dans $\boldsymbol{F}_q[X]$) de $h[X, Y]$, qui est $-(a + \sum_{k=0}^{m-1} X^{q^{kn}})$; les racines de ce dernier polynôme sont simples puisque sa dérivée est -1. Par suite $f(g(X))$ est le polynôme minimal de ξ sur $\boldsymbol{F}_q$. D'où l'assertion.

1.2. Voici deux applications du lemme précédent. Soit $f(X) = X^3 + X + 1 \in \boldsymbol{F}_2[X]$; f est irréductible. Soit $g(X) = X^3 + X \in \boldsymbol{F}_2[X]$. Avec les notations de 1.1, on a

$$f(g(X)) = X^9 + X^7 + X^5 + X + 1$$

et

$$h(X, Y) = (X^{64} + X^8 + X)\, Y^2 + (X^{72} + X^{65} + X^9 + 1)\, Y.$$

Modulo $f(g(X))$, on a $X^9 \equiv X^7 + X^5 + X + 1$; d'où l'on déduit facilement que

$$X^{64} \equiv X^8 + X \quad \text{et} \quad X^{72} \equiv X^{65} + X^9 + 1$$

et, par suite, que

$$X^{64} + X^8 + X \equiv 0 \quad \text{et} \quad X^{72} + X^{65} + X^9 + 1 \equiv 0.$$

Donc, $X^9 + X^7 + X^5 + X + 1$ est irréductible sur $\boldsymbol{F}_2$.

Soient maintenant $f(X) = X^2 + 1 \in \boldsymbol{F}_3[X]$ et $g(X) = X^2 + X \in \boldsymbol{F}_3[X]$. Avec les notations de 1.1, on a

$$f(g(X)) = X^4 + 2X^3 + X^2 + 1 \quad \text{et} \quad h(X, Y) = -Y(X^9 + X + 1).$$

Modulo $f(g(X))$, on a $X^9 \equiv 2X + 2$. D'après le lemme 1.1, $X^4 + 2X^3 + X^2 + 1$ est irréductible sur $\boldsymbol{F}_3$.

1.3. Théorème. *Soit $u \in \boldsymbol{F}_q[X]$ un polynôme monique et irréductible et soit m un diviseur > 0 de $\deg(u)$. Pour qu'il existe des polynômes moniques $f, g \in \boldsymbol{F}_q[X]$ tels que $u(X) = f(g(X))$ et $\deg(g) = m$, il faut et il suffit que dans $\boldsymbol{F}_q[X]$,*

$$-(-1)^m X^{(q^{\deg(u)}-1)/(q^{\deg(u)/m}-1)}$$

soit congru modulo $u(X)$ à un polynôme monique de degré m de $\boldsymbol{F}_q[X]$, ayant 0 pour racine.

La condition est nécessaire. Avec les notations de l'énoncé, soit $u = f(g(X))$ cet irréductible et soit $n = \deg(f)$. On a $\deg(u) = mn$. D'après le lemme 1.1, le polynôme $-g(X) + g(0) - (-1)^m X^{(q^{mn}-1)/(q^n-1)}$ appartient à l'idéal $u(X)\, \boldsymbol{F}_q[X]$.

La condition est suffisante. Soit $n = \deg(u)/m$ et soit $g \in \boldsymbol{F}_q[X]$ un polynôme monique de degré m tel que

$$g(X) - g(0) \equiv -(-1)^m X^{(q^{mn}-1)/(q^n-1)} \bmod u(X).$$

Soit ξ une racine de u dans $\boldsymbol{F}_{q^{mn}}$, on a $g(\xi) \in \boldsymbol{F}_{q^n}$. Le polynôme

$$f(X) = \prod_{j=0}^{n-1} \left(X - (g(\xi))^{q^j}\right)$$

appartient à $\boldsymbol{F}_q[X]$. $f(g(X))$ est un polynôme monique, de degré mn, de $\boldsymbol{F}_q[X]$, dont ξ est une racine. Donc $f(g(X))$ est divisible dans $\boldsymbol{F}_q[X]$ par le polynôme minimal $u(X)$ de cette racine. Donc $u = f(g(X))$.

1.4. Voici une application de ce résultat (cf. *infra* 3.1).
Soit

$$u(X) = X^6 + X^5 + X^3 + X^2 + 1 \in \boldsymbol{F}_2[X];$$

ce polynôme est irréductible sur $\boldsymbol{F}_2$. Avec les notations de 1.3, prenons $m = 2$. On a

$$X^{(2^6-1)/(2^3-1)} = X^9.$$

Mais, modulo $u(X)$, on a:

$$X^6 \equiv X^5 + X^3 + X^2 + 1;$$

on en déduit que

$$X^8 \equiv X + 1,$$

donc que

$$X^9 \equiv X^2+X.$$

Il existe par conséquent un polynôme irréductible $f(X) \in \boldsymbol{F}_2[X]$ de degré 3 et $a \in \boldsymbol{F}_2$ tels que:

$$u(X) = f(X^2+X+a).$$

En posant $f(X) = X^3+aX^2+\beta X+\gamma$, $f_1(X) = X^2+\beta$, $f_2(X) = X+a$ et $f_3(X) = 1$ on a:

$$u(X) = f(a)+(X^2+X)f_1(a)+(X^2+X)^2f_2(a)+(X^2+X)^3f_3(a).$$

Par identification, on voit que

$$u(X) = (X^2+X)^3+(X^2+X)^2+1 = (X^2+X+1)^3+(X^2+X+1)+1.$$

(On observera que la congruence $X^8+X+1 \equiv 0 \bmod u(X)$ redonne, dans ce cas particulier, du même coup, l'irréductibilité de $u(X)$ sur $\boldsymbol{F}_2$.)

Dans les paragraphes suivants, nous allons donner d'autres applications de 1.1, retrouvant là et améliorant des résultats contenus dans [2], [3], [4] et [6].

2. Irréductibilité des polynômes $f(X^m)$ (cf. [3], § 34).

2.1. Lemme. *Soient $f \in \boldsymbol{F}_q[X]$ un polynôme de degré n tel que $f(X) \neq X$ et m un entier > 0 divisant q^n-1.*

(a) *Les conditions suivantes sont équivalentes:*

(i) *Les coefficients dans $\boldsymbol{F}_q[X]$ de*

$$\prod_{k=0}^{m-1}(Y-X^{q^{kn}})-Y^m-(-1)^m X^{(q^{mn}-1)/(q^n-1)} \in \boldsymbol{F}_q[X, Y]$$

appartiennent à l'idéal $f(X^m)\,\boldsymbol{F}_q[X]$;

(ii) *Les coefficients dans $\boldsymbol{F}_q[X]$ de*

$$u(X, Y) = \prod_{k=0}^{m-1}(Y-X^{q^{kn}-1})-Y^m-(-1)^m X^{(q^{mn}-1)/(q^n-1)-m}$$

appartiennent à $f(X^m)\,\boldsymbol{F}_q[X]$;

(iii) *Les coefficients de*

$$v(X, Y) = \prod_{k=0}^{m-1}(Y-X^{(q^{kn}-1)/m})-Y^m-(-1)^m X^{((q^{mn}-1)/(q^n-1)-m)/m}$$

appartiennent à $f(X)\,\boldsymbol{F}_q[X]$.

(b) *De plus, si l'on suppose f irréductible sur $\boldsymbol{F}_q$ et si $\xi \in \overline{\boldsymbol{F}}_p$ est une racine de $f(X^m)$, ces conditions sont équivalentes à*

(iv) $u(\xi, Y) = 0$.

(a) Comme $f(X) \neq X$, (i) et (ii) sont équivalentes. D'autre part, si u, v et $w \in \boldsymbol{F}_q[X]$ et si w n'est pas constant, il est clair que, pour que u divise v, il faut et il suffit que $u(w(X))$ divise $v(w(X))$. Cette remarque montre que (ii) et (iii) sont équivalentes.

(b) Il est clair que (ii) entraine (iv). Inversement, supposons (iv) vérifiée. Les coefficients dans $\boldsymbol{F}_q[X]$ de $v(X, Y)$ ont pour racine ξ^m, qui est racine du polynôme irréductible $f(X)$. D'où (iii).

2.2. Théorème. *Soit $f \in \boldsymbol{F}_q[X]$ un polynôme monique, irréductible, de degré n et d'exposant e[1] et soit m un entier > 0 divisant q^n-1 et tel que $\left(m, \dfrac{q^n-1}{e}\right) = 1$. Alors $f(X^m)$ est irréductible sur $\boldsymbol{F}_q$.*

On va montrer que f vérifie la condition (iv) de 2.1. S'il en est ainsi, f vérifie la condition (i) c'est-à-dire le lemme 1.1, où l'on fait $g(X) = X^m$, ce qui entraine alors le théorème.

Soient $d = \dfrac{q^n-1}{e}$, $\xi \in \overline{\boldsymbol{F}}_p$ une racine de $f(X^m)$ et γ un générateur de $\boldsymbol{F}_{q^n}^{\times}$. Comme $\xi^m \in \boldsymbol{F}_{q^n}^*$, on a $\xi^m = \gamma^{ad}$ et on a $(a, m) = 1$. Donc $\eta = \gamma^{ad(q^n-1)/m}$ est une racine m-ème de 1 dans $\boldsymbol{F}_{q^n}$, d'ordre m.

Comme $\xi^{q^{kn}-1} = \eta^k$, on a

$$\prod_{k=0}^{m-1}(Y-\xi^{q^{kn}-1}) = \prod_{k=0}^{m-1}(Y-\eta^k) = Y^m-1.$$

De plus, si $a = \xi^{(q^{mn}-1)/(q^n-1)-m}$ on a

$$a = -(-1)^m.$$

Mais alors, avec les notations de 2.1, on a $u(\xi, Y) = -1-(-1)^m a = 0$. ■

3. Irréductibilité des polynômes $f(X^p-X-b)$.

On rappelle que l'on a posé $q = p^s$.

3.1. Théorème. *Soit $f(X) = X^n+aX^{n-1}+\ldots+a_n$ un polynôme irréductible de $\boldsymbol{F}_q[X]$ et soit $b \in \boldsymbol{F}_q$. Pour que le polynôme $f(X^p-X-b)$ soit irréductible, il faut et il suffit que*

$$\mathrm{Tr}_{\boldsymbol{F}_q/\boldsymbol{F}_p}(a) \neq n\,\mathrm{Tr}_{\boldsymbol{F}_q/\boldsymbol{F}_p}(b).$$

Pour abréger, posons, pour $x \in \boldsymbol{F}_q$,

$$\mathrm{Tr}(x) = \mathrm{Tr}_{\boldsymbol{F}_q/\boldsymbol{F}_p}(x) = x+x^p+\ldots+x^{p^{s-1}}.$$

---

[1] e est, par définition, le plus petit entier > 0 tel que $f(X)$ divise X^e-1 dans $\boldsymbol{F}_q[X]$.

(a) Dans $\boldsymbol{F}_q[X, Y]$, on a

$$\prod_{k=0}^{p-1}\big(Y-X-k\mathrm{Tr}(nb-a)\big)=(Y-X)\prod_{k=1}^{p-1}\big(Y-X-k\mathrm{Tr}(nb-a)\big)$$
$$=Y^p-X^p-(Y-X)\big(\mathrm{Tr}(nb-a)\big)^{p-1}.$$

(b) Posons $T(X)=X+X^q+\ldots+X^{q^{n-1}}$ et, pour $k>0$,

$$\Psi_k(X)=\sum_{i=0}^{kns-1}X^{p^i}.$$

On a

$$\Psi_k(X)=\sum_{l=0}^{s-1}\big(T(X)^{p^l}+\ldots+T(X)^{p^{(k-1)ns+l}}\big).$$

Puisque $f(X)$ est irréductible, on sait que $a+T(X)\equiv 0 \bmod f(X)$. Donc

$$\Psi_k(X)\equiv -k\mathrm{Tr}(a) \bmod f(X).$$

Pour $k>0$, on a

$$X^{p^{kns}}=\Big(\sum_{i=0}^{kns-1}(X^p-X-b)^{p^i}\Big)+X+\mathrm{Tr}_{\boldsymbol{F}_{q^{kn}}/\boldsymbol{F}_p}(b)$$
$$=\Psi_k(X^p-X-b)+X+kn\,\mathrm{Tr}(b).$$

Par suite, pour $k\geqslant 0$, on a

$$X^{p^{kns}}\equiv X+k\mathrm{Tr}(nb-a) \bmod f(X^p-X-b).$$

(c) D'après 1.1, pour que $f(X^p-X-b)$ soit irréductible, il faut et il suffit que les coefficients dans $\boldsymbol{F}_q[X]$ du polynôme

$$\prod_{k=0}^{p-1}(Y-X^{q^{kn}})-(Y^p-Y)-(-1)^pX^{1+q^n+\ldots+q^{(p-1)n}}$$
$$=\prod_{k=0}^{p-1}(Y-X^{p^{kns}})-(Y^p-Y)-(-1)^p\prod_{k=0}^{p-1}X^{p^{kns}}$$

soient congrus à 0 modulo $f(X^p-X-b)$. D'après (a), cette condition est équivalente à la suivante:

$f(X^p-X-b)$ divise $1-\big(\mathrm{Tr}(nb-a)\big)^{p-1}$, ou encore $\big(\mathrm{Tr}(nb-a)\big)^{p-1}=1$, c'est-à-dire $\mathrm{Tr}(nb)\neq\mathrm{Tr}(a)$.

3.2. Le théorème 3.1 permet de retrouver divers résultats de L. E. Dickson.

En prenant $f(X)=X$, le théorème 3.1 redonne le résultat cité dans [3], p. 29.

En prenant $b=0$, on retrouve celui donné dans [3], p. 34.

Enfin, soient $f=X^n+aX^{n-1}+\ldots\in\boldsymbol{F}_q[X]$ un polynôme irréductible et $b\in\boldsymbol{F}_q$. La méthode utilisée pour démontrer 3.1 permet de démontrer facilement les résultats suivants.

Pour que $f(X^q-X-b)$ soit irréductible, il faut et il suffit que $q=p$ et que $a\neq nb$; cf. [3], p. 30.

Pour que $f(X^{q^n}-X-b)$ soit irréductible, il faut et il suffit que $n=1$, $q=p$ et $a\neq b$, par suite que $f(X^{q^n}-X-b)=X^p-X-b+a$.

Ce dernier résultat peut se déduire d'un théorème dû à A. F. Long ([4], p. 307); on notera que la condition $a\neq b$ est indispensable dans ce résultat. Nous allons développer ces dernières remarques.

4. Irréductibilité des polynômes $f(X^{p^r}-X)$. On pose toujours $q=p^s$.

4.1. Lemme. *Soit $f\in\boldsymbol{F}_q[X]$ un polynôme irréductible, de degré n. Soient r un entier >0 et $\mu=\mathrm{ppcm}(r, ns)$. Alors on a*

$$X^{p^{\mu p}}-X\equiv 0 \bmod f(X^{p^r}-X).$$

$f(X)$ divise $X^{p^{ns}}-X$ dans $\boldsymbol{F}_q[X]$. Par suite, $f(X^{p^r}-X)$ divise $(X^{p^r}-X)^{p^{ns}}-(X^{p^r}-X)$ et donc $(X^{p^{ns}}-X)^{p^r}-(X^{p^{ns}}-X)$.

Les congruences suivantes sont écrites dans $\boldsymbol{F}_q[X]$ modulo $f(X^{p^r}-X)$. Par récurrence sur $k\geqslant 0$, ce qui précède montre que

$$(X^{p^{ns}}-X)^{p^{kr}}\equiv X^{p^{ns}}-X.$$

D'où, en faisant $k=\mu/r$,

$$(X^{p^{ns}}-X)^{p^\mu}\equiv X^{p^{ns}}-X$$

et, pour tout $h\geqslant 0$:

$$X^{p^{hns+\mu}}\equiv X^{p^{hns}}+X^{p^\mu}-X.$$

En faisant $h=r/(r, sn)$, on a donc

$$X^{p^{2\mu}}\equiv 2(X^{p^\mu}-X)+X.$$

D'où, par récurrence sur $k\geqslant 0$:

$$X^{p^{k\mu}}-X\equiv k(X^{p^\mu}-X). \tag{4.1.1}$$

D'où le lemme, en faisant $k=p$.

4.2. Lemme. *Soit $f\in\boldsymbol{F}_q[X]$ un polynôme monique irréductible de degré n et r un entier >0. Si $f(X^{p^r}-X)$ est irréductible sur $\boldsymbol{F}_q$, alors $(r, ns)=1$.*

Soit d un diviseur de (r, ns).

(a) On a $X^{p^r}-X=(X^{p^{d(r/d-1)}}+\ldots+X)^{p^d}-(X^{p^{d(r/d-1)}}+\ldots+X)$. Donc $f(X^{p^d}-X)$ est irréductible aussi.

(b) Pour que $f(X^{p^d}-X)$ soit irréductible, il faut et il suffit, d'après 1.1, que la condition suivante soit vérifiée: les coefficients dans $\boldsymbol{F}_q[X]$ de

$$\prod_{k=0}^{p^d-1}(Y-X^{p^{kns}})-(Y^{p^d}-Y)-(-1)^{p^d}X^{(p^{np^d ns}-1)/(p^{ns}-1)}$$

sont dans l'idéal $f(X^{p^d}-X)\,\boldsymbol{F}_q[X]$.

(c) D'après (4.1.1), on a, pour $k \geqslant 0$,

$$X^{p^{kns}} \equiv X + k(X^{p^{ns}}-X) \bmod f(X^{p^d}-X),$$

puisque le ppcm de d et de sn est sn.

D'autre part, dans $\boldsymbol{F}_p[Y,Z]$, on a (théorème de Gauss–Wilson)

$$\prod_{k=0}^{p^d-1}(Y-kZ) = Y^{p^d}-(Z^{p-1}Y)^{p^d-1}.$$

En substituant $X^{p^{ns}}-X$ à Z, on voit que la condition de (b) s'écrit encore: les coefficients dans $\boldsymbol{F}_q[X]$ de $Y-Y^{p^{d-1}}(X^{p^{ns}}-X)^{(p-1)p^{d-1}}$ sont congrus à 0 modulo $f(X^{p^d}-X)$. Cette dernière condition est équivalente à $d=1$ et $(X^{p^{ns}}-X)^{p-1} \equiv 1 \bmod f(X^p-X)$ ou encore à $d=1$ et $f(X^p-X)$ est irréductible.

D'où $(r, ns)=1$.

4.3. Le lemme 4.1 donne des précisions supplémentaires. En effet, avec les notations de ce lemme, $f(X^{p^r}-X)$ divise $X^{p^{\mu p}}-X$. Comme $p^r n$ divise $\dfrac{\mu p}{s} = \dfrac{npr}{(r, ns)}$, puisque $f(X^{p^r}-X)$ est irréductible, on a $p^{r-1}=r$. Mais alors on a $r=1$ ou bien $p=2$, $r=2$ et ns est impair. D'où le théorème suivant.

4.4. Théorème. *Soit $f \in \boldsymbol{F}_q[X]$ un polynôme monique de degré n et soit r un entier >0.*

On suppose que $f(X^p-X)$ est irréductible sur $\boldsymbol{F}_q$.

Pour que $f(X^{p^r}-X)$ soit irréductible, il faut et il suffit que l'une des deux conditions suivantes soit vérifiée:

(i) $r=1$;

(ii) $p=2$, $r=2$ *et ns est impair.*

Compte tenu de ce qui précède, il reste à prouver que si ns est impair, $f(X^4-X)$ est irréductible sur $\boldsymbol{F}_{2^s}$. Or ceci résulte de 3.1, car $X^4-X = (X^2-X)^2-(X^2-X)$ dans $\boldsymbol{F}_{2^s}[X]$ et le coefficient de X^{2n-1} dans $f(X^2-X)$ est n.

4.5. Comme il m'a été signalé par le rapporteur de cet article, ce résultat se déduit facilement de théorèmes dûs à A. F. Long [5], p. 65, th. 5.1 et 5.2, en procédant de la manière suivante:

Avec les notations de [5], pour que $f(X^{p^r}-X)$ soit irréductible, il est nécessaire que $r'=1$. Mais alors la seule valeur de t est $t=1$ et donc $N(1, p^d)/1 = p^d$; mais $p^d \neq 1$ pour $d \geqslant 1$. Les conditions du théorème 5.1 ne sont donc pas réalisées.

Dans le théorème 5.2, nous devons avoir $l=1$ et par suite $t=1$. Pour établir que $f(X^{p^r}-X)$ est irréductible, nous devons écrire que

$$N(1, p^k d)/p^{k+1} = 1.$$

Alors $p^k d = k+1$ et nous obtenons les deux solutions, en remarquant que $d=(r, sn)$:

(a) $k=0$, $d=1$, $r=1$;

(b) $p=2$, $k=1$, $d=1$ et $r=2$.

Ce qui donne les conditions du théorème 4.4.

5. Irréductibilité des polynômes $f(X^q-aX)$.

5.1. Nous allons maintenant généraliser un résultat de O. Öre ([6], p. 262).

Théorème. *Soient $f \in \boldsymbol{F}_q[X]$ un polynôme monique, irréductible, de degré n et $a \in \boldsymbol{F}_q^{\times}$. Pour que $f(X^q-aX)$ soit irréductible, il faut et il suffi que $s=1$, $a^n=1$ et que $f(X)$ ne divise pas*

$$X^{p^n-1}+aX^{p^n-2}+\ldots+a^{n-1}X.$$

(a) Par hypothèse $f(X)$ divise $X^{q^n}-X$; donc

$$(X^q-aX)^{q^n}-(X^q-aX) \equiv 0 \bmod f(X^q-aX).$$

On en déduit par récurrence sur $k \geqslant 0$ les congruences suivantes modulo $f(X^q-aX)$:

$$X^{q^{kn}} \equiv \begin{cases} \dfrac{a^{kn}-1}{a^n-1}X^{q^n} - \dfrac{a^{kn}-a^n}{a^n-1}X & \text{si} \quad a^n \neq 1, \\ X+k(X^{q^n}-X) & \text{si} \quad a^n=1. \end{cases}$$

(b) Supposons $a^n \neq 1$ (donc $q \neq 2$). Supposons $f(X^q-aX)$ irréductible. Le lemme 1.1 montre alors que

$$\sum_{k=0}^{q-1} X^{q^{kn}} \equiv 0 \bmod f(X^q-aX).$$

D'après (a), modulo $f(X^q-aX)$ on a $\displaystyle\sum_{k=0}^{q-1} X^{q^{kn}} \equiv \frac{X^{q^n}-X}{a^n-1}$; on a donc $X^{q^n}-X \equiv 0$, ce qui est absurde. Donc $a^n=1$.

Plaçons nous dans ce cas. Pour que $f(X^q-aX)$ soit irréductible, il faut et il suffit, d'après (1.1), que les coefficients dans $\boldsymbol{F}_q[X]$ de

$$\prod_{k=0}^{q-1}(Y-X^{q^{kn}})-(Y^q-aY)-(-1)^q X^{(q^{nq}-1)/(q^n-1)}$$

soient congrus à 0 modulo $f(X^q-aX)$.

Compte tenu de (a) et du théorème de Gauss–Wilson, cette condition est équivalente à la suivante: les coefficients dans $\boldsymbol{F}_q[X]$ de $aY-(X^{q^n}-X)^{(p-1)p^{s-1}}Y^{p^{s-1}}$ sont congrus à 0 modulo $f(X^q-aX)$ c'est-à-dire à $s=1$ et

$$(X^{p^n}-X)^{p-1}\equiv a \bmod f(X^p-aX).$$

Posons alors

$$u(X)=X^{p^{n-1}}+aX^{p^{n-2}}+\ldots+a^{n-1}X;$$

on a

$$u(X)^p-au(X)=X^{p^n}-X=u(X^p-aX).$$

La condition précédente s'écrit encore

$$u(X^p-aX)^{p-1}\equiv a \bmod f(X^p-aX),$$

c'est-à-dire

$$u(X)^{p-1}\equiv a \bmod f(X)$$

ou encore $f(X)$ ne divise pas $u(X)$. ■

5.2. Théorème. *On suppose s pair. Soit $f(X)=X^n-aX^{n-1}-\ldots-a_n$ un polynôme irréductible de $\boldsymbol{F}_q[X]$. Pour que $f(X^p+X)$ soit irréductible sur $\boldsymbol{F}_q$, il faut et il suffit que*

$$\sum_{j=1}^{s}(-1)^{j-1}a^{p^{s-j}}\neq 0.$$

(a) On a

$$X^{q^n}=\Big(\sum_{k=0}^{ns-1}(-1)^{ns-k+1}(X^p+X)^{p^k}\Big)+(-1)^{ns}X.$$

Posons

$$u(X)=\sum_{k=0}^{ns-1}(-1)^{ns-k+1}X^{p^k},$$

$$b=\sum_{j=1}^{s}(-1)^{j-1}a^{p^{s-j}} \quad \text{et} \quad T(X)=\sum_{k=0}^{n-1}X^{p^{ks}}.$$

On a

$$u(X)=\sum_{j=1}^{s}(-1)^{j-1}T(X)^{p^{s-j}}.$$

On a donc, modulo $f(X^p+X)$,

$$X^{p^{ns}}\equiv b+X;$$

d'où, pour $k\geqslant 0$

$$X^{p^{kns}}\equiv kb+X.$$

D'autre part, le théorème de Wilson montre que

$$\prod_{k=0}^{p-1}(Y-X^{p^{kns}})\equiv Y^p-X^p-(Y-X)b^{p-1} \bmod f(X^p+X).$$

(b) D'après 1.1, pour que le polynôme $f(X^p+X)$ soit irréductible, il faut et il suffit que les coefficients dans $\boldsymbol{F}_q[X]$ de

$$\prod_{k=0}^{p-1}(Y-X^{q^{kn}})-Y^p-Y-(-1)^p X^{1+\ldots+q^{n(p-1)}}$$

soient congrus à $0 \bmod f(X^p+X)$. D'après (a), cette condition s'écrit $b^{p-1}+1=0$, ce qui équivaut à $b\neq 0$, puisque $b^p+b=0$.

5.3. Les résultats obtenus dans les paragraphes 3, 4 et 5 sont liés à l'observation suivante: le problème essentiel est d'exprimer le reste dans la division euclidienne de $X^{p^{kns}}$ par $f(g(X))$. Ceci est théoriquement possible [1], mais les formules obtenues sont compliquées. Cependant, si $X^{p^{sn}}=u(g(X))+v(X)$ (où $u, v\in \boldsymbol{F}_q[X]$, $u\neq 0$, $v=0$ ou $\deg(v)<\deg(u)$) et si $u(X)\equiv 0 \bmod f(X)$, on a alors $X^{p^{kns}}=v^k(X)$ [2] (modulo $f(g(X))$) pour tout $k>0$; on obtient alors des expressions plus ou moins maniables pour ledit reste, selon que les coefficients dans $\boldsymbol{F}_q[X]$ de $\prod_{k=0}^{m-1}(Y-v^k(X))$ s'expriment plus ou moins facilement modulo $f(g(X))$.

[2] $v^k(X)$ signifie $v(v\ldots(v(X)))$.

Bibliographie

[1] S. Agou, *Formules explicites intervenant dans la division euclidienne des polynômes à coefficients dans un anneau unitaire et applications diverses*, Public. Départ. Math. (Lyon), 8. 1 (1971), p. 107–121.

[2] A. A. Albert, *Fundamental Concepts of Higher Algebra*, London 1956.

[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, New-York 1958.

[4] A. F. Long, *Classification of irreducible factorable polynomials over a finite field*, Acta Arith. 12 (1967), p. 301–313.

[5] — *Factorisation of irreducible polynomials over a finite field with the substitution $X^{p^r}-X$ for X*, Duke Math. Journ. 40 (1) (1973), p. 63–76.

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

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITE DE LYON 1

Reçu le 7. 6. 1974
et dans la forme modifiée le 21. 2. 1975