PUBLICATIONS DU DÉPARTEMENT DE MATHÉMATIQUES DE LYON

SIMON AGOU

Sur l'irréductibilité de certains polynômes à plusieurs indéterminées et à coefficients dans un corps fini

Publications du Département de Mathématiques de Lyon, 1975, tome 12, fascicule 1 , p. 5-12

<http://www.numdam.org/item?id=PDML_1975__12_1_5_0>

© Université de Lyon, 1975, tous droits réservés.

L'accès aux archives de la série « Publications du Département de mathématiques de Lyon » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Publications du
Département de
Mathématiques
Lyon 1975 t.12-1

SUR L'IRREDUCTIBILITE DE CERTAINS POLYNOMES A PLUSIEURS INDETERMINEES ET A COEFFICIENTS DANS UN CORPS FINI

par Simon AGOU

Cet article se réfère à une publication de L. Carlitz [1] . Comme à l'accoutumée, on désigne par $\mathbb{F}_q$ le corps fini à q éléments.

1. DEFINITION. - *On dit qu'un polynôme* $f(X_1,\ldots,X_k) \in \mathbb{F}_q[X_1,\ldots,X_k]$ *est linéairement factorisable s'il peut se mettre sous la forme*

$$f(X_1,\ldots,X_k) = \prod_{i=0}^{s-1} (\alpha_{i,0} + \alpha_{i,1} X_1 + \ldots + \alpha_{i,k} X_k)$$

où les $\alpha_{i,j}$ *sont des éléments d'une extension* $\mathbb{F}_{q'}$ *de* $\mathbb{F}_q$.

Nous faisons la convention expresse suivante : la notation $f(X_1,\ldots,X_k)$ désigne un polynôme où figurent *effectivement* les k indéterminées $X_1,\ldots,X_k$.

2. MANIPULATIONS SUR LES POLYNOMES LINEAIREMENT FACTORISABLES ET IRREDUCTIBLES.

Soit $f(X_1,\ldots,X_k) \in \mathbb{F}_q[X_1,\ldots,X_k]$ un polynôme linéairement factorisable et irréductible dans $\mathbb{F}_q[X_1,\ldots,X_k]$ et soit s son degré total. On sait [1] que l'on peut écrire

$$f(X_1,\ldots,X_k) = \prod_{j=o}^{s-1} (\alpha_o q^j + \alpha_1 q^j X_1 + \ldots + \alpha_k q^j X_k),$$

où $\alpha_o,\ldots,\alpha_k$ sont des éléments de $\mathbb{F}_{q^s}$ qui sont assujettis à une certaine condition.

Si $f(0,\ldots,0) = 0$, le polynôme $f(X_1,\ldots,X_k)$ est homogène et peut être mis sous la forme

$$f(X_1,\ldots,X_k) = a_1 X_1^s \; g\left(\frac{X_2}{X_1},\ldots,\frac{X_k}{X_1}\right),$$

où $a_1 \in \mathbb{F}_q$ et où $g\left(\frac{X_2}{X_1},\ldots,\frac{X_k}{X_1}\right) = \prod_{j=o}^{s-1} (1+\beta_1 q^j \frac{X_2}{X_1} + \ldots + \beta_k q^j \frac{X_k}{X_1})$ est un polynôme irréductible de $\mathbb{F}_q\left[\frac{X_2}{X_1},\ldots,\frac{X_k}{X_1}\right]$.

Si $f(0,\ldots,0) \neq 0$, on peut écrire

$$f(X_1,\ldots,X_k) = \alpha_o^{(q^s-1)/(q-1)} g(X_1,\ldots,X_k),$$

avec $g(X_1,\ldots,X_k) = \prod_{j=o}^{s-1} (1 + (\frac{\alpha_1}{\alpha_o})^{q^j} X_1 + \ldots + (\frac{\alpha_k}{\alpha_o})^{q^j} X_k)$.

On voit ainsi qu'il est possible d'associer à $f(X_1,\ldots,X_k)$ un certain polynôme linéairement factorisable $g(Y_1,\ldots,Y_{k'}) \in \mathbb{F}_q[Y_1,\ldots,Y_{k'}]$ (avec k' = k-1 ou k), que l'on appelle le *normalisé* de $f(X_1,\ldots,X_k)$.

Ceci étant, on a le résultat suivant.

3. PROPOSITION. - *Soit* $f(X_1,\ldots,X_k) \in \mathbb{F}_q[X_1,\ldots,X_k]$ *un polynôme linéairement factorisable, de degré total* s *et tel que* $f(0,\ldots,0) \neq 0$.
Pour que $f(X_1,\ldots,X_k)$ *soit irréductible dans* $\mathbb{F}_q[X_1,\ldots,X_k]$, *il faut et il suffit que les polynômes* $f(0,\ldots,X_t,0,\ldots,0)$ $(t = 1,\ldots,k)$ *vérifient les conditions suivantes :*

1) leurs degrés sont égaux à s,

2) ils sont, à un coefficient multiplicatif de $\mathbb{F}_q$ *près, des puissances de polynômes irréductibles de chacun des* $\mathbb{F}_q[X_t]$, *dont le p.p.c.m. des degrés est* s.

Remarquons que, par une procédure de recherche de p.g.c.d., il est possible de déterminer si un polynôme de $\mathbb{F}_q[X]$ est ou non une puissance d'un polynôme irréductible, à un coefficient multiplicatif de $\mathbb{F}_q$ près (cf. [2]). S'il l'est, on peut effectivement, en utilisant les résultats de [2] , déterminer de quel polynôme irréductible il s'agit *sans nouveaux calculs.*

En effet, soit f(X) un polynôme monique, puissance d'un polynôme irréductible de $\mathbb{F}_q[X]$; il est clair que l'on peut se restreindre aux cas où $f(0) \neq 0$ et où f(X) n'est par une puissance p-ème d'un polynôme de $\mathbb{F}_q[X]$, p étant le diviseur premier unique de q . Reprenant les notations de [2] , on sait alors qu'il existe un diviseur d•du degré n de f(X), tel que $\Delta_{f,d} \notin \mathbb{F}_q$. Avec les hypothèses faites on a pgcd (d,q) = 1 .

Or $\Delta_{f,d}$ divise $\sigma_{f,d,o} = (-1)^{md} X^{\frac{q^m-1}{q-1} d} - f(o)$; donc $\Delta_{f,d}$ n'a que des racines simples et ainsi $\Delta_{f,d}$ est irréductible sur $\mathbb{F}_q$. Il en résulte que, dans ce cas le polynôme irréductible cherché est $\Delta_{f,d}$.

DEMONSTRATION DE LA PROPOSITION.

Condition nécessaire.

Si f est linéairement factorisable et irréductible, il résulte de [1] qu'il existe $\alpha_o,\ldots,\alpha_k \in \mathbb{F}_{q^s}$ tels que

$$f(X_1,\ldots,X_k) = \prod_{j=o}^{s-1} (\alpha_o{}^{q^j} + \alpha_1{}^{q^j} X_1 + \ldots + \alpha_k{}^{q^j} X_k)$$

et que s soit le p.p.c.m. des degrés des polynômes minimaux de $\alpha_o,\ldots,\alpha_k$ sur $\mathbb{F}_q$.

On a $f(0,\ldots,X_t,0,\ldots,0) = \prod_{j=0}^{s-1} (\alpha_o{}^{q^j} + \alpha_t{}^{q^j} X_t)$.

Pour $1 \leq t \leq k$, les polynômes $f(0,\ldots, X_t, 0,\ldots,0)$ sont évidemment dans $\mathbb{F}_q[X_t]$.

On a $\alpha_o \neq 0$ et $\alpha_t \neq 0$ pour $t = 1,\ldots,k$.

Considérons le polynôme normalisé suivant, qui est bien entendu linéairement factorisable et irréductible :

$$\frac{f(X_1,\ldots,X_k)}{\alpha_o^{\frac{q^s-1}{q-1}}} = \prod_{j=0}^{s-1} (1 + \beta_1{}^{q^j} X_1 + \ldots + \beta_k{}^{q^j} X_k) ,$$

où, d'après [1], le p.p.c.m. des degrés des polynômes minimaux sur $\mathbb{F}_q$ des β_i, qui sont non nuls, est s.

Par suite, on a

$$\frac{f(0,\ldots,X_t,\ 0,\ldots,0)}{\alpha_o^{\frac{q^s-1}{q-1}}} = \prod_{j=0}^{s-1} (1 + \beta_t^{q^j} X_t).$$

Ce polynôme est évidemment de degré s ; et le degré du polynôme minimal de β_t sur $\mathbb{F}_q$ est aussi le degré du polynôme minimal de $-\frac{1}{\beta_t}$ sur $\mathbb{F}_q$.

Il en résulte aisément que $\frac{f(0,\ldots,\ X_t,\ 0,\ldots,0)}{\alpha_o^{\frac{q^s-1}{q-1}}}$, qui est un polynôme de degré s, est, au coefficient $\beta_t^{\frac{q^s-1}{q-1}} \in \mathbb{F}_q$ près, une puissance du polynôme minimal de $-\frac{1}{\beta_t}$ sur F_q.

Condition suffisante.

Par hypothèse, les polynômes $f(0,\ldots,X_t,0,\ldots,0)$ sont de degré s ; il en résulte que $f(X_1,\ldots,X_k)$ est un produit de polynômes irréductibles, linéairement factorisables et deux à deux distincts de $\mathbb{F}_q[X_1,\ldots,X_k]$ dans chacun desquels figurent les k indéterminées. Soit alors $f_1(X_1,\ldots,X_k)$ un tel polynôme irréductible et divisant f. Par [1] , on sait que

$$f_1(X_1,\ldots,X_k) = \prod_{j=0}^{m-1} (\alpha_o^{q^j} + \alpha_1^{q^j} X_1 + \ldots + \alpha_k^{q^j} X_k).$$

$f_1(0,\ldots,X_t,0,\ldots,0) = \prod_{j=0}^{m-1} (\alpha_o^{q^j} + \alpha_t^{q^j} X_t)$ est donc , à un coefficient multiplicatif près, une puissance d'un polynôme irréductible de $\mathbb{F}_q[X_t]$.

Comme $f(0,\ldots,0) \neq 0$, on a $\alpha_o \neq 0$; ainsi on peut considérer le polynôme normalisé

$$\frac{f_1(X_1,\ldots,X_k)}{\alpha_o^{\frac{q^m-1}{q-1}}} = \prod_{j=0}^{m-1} (1 + \xi_1^{q^j} X_1 + \ldots + \xi_k^{q^j} X_k) ,$$

où $\xi_1,\ldots,\xi_k$ sont des éléments de $\mathbb{F}_{q^s}$ tels que le p.p.c.m. des degrés de leurs polynômes minimaux sur $\mathbb{F}_q$ soit s.

Comme $f_1(X_1,\ldots,X_k)$ est irréductible, il en résulte que son degré total est s et, par suite, que f est irréductible dans $\mathbb{F}_q[X_1,\ldots,X_k]$.

c.q.f.d.

4. Pour être complet, il suffit de faire les remarques suivantes.

Soit $f(X_1,\ldots,X_k)$ un polynôme linéairement factorisable de $\mathbb{F}_q[X_1,\ldots,X_k]$. Si $f(0,0,\ldots,0) = 0$, alors $f(X_1,\ldots,X_k)$ est divisible par un polynôme homogène linéairement factorisable de $\mathbb{F}_q[X_1,\ldots,X_k]$. Si $f(X_1,\ldots,X_k)$ n'est pas homogène alors f n'est évidemment pas irréductible dans $\mathbb{F}_q[X_1,\ldots,X_k]$.

Enfin, si $f(X_1,\ldots,X_k)$ est homogène, on a le lemme immédiat suivant :

4.1. LEMME. - *Soit* $f(X_1,\ldots,X_k)$ *un polynôme homogène de* $\mathbb{F}_q[X_1,\ldots,X_k]$. *Pour que* $f(X_1,\ldots,X_k)$ *soit irréductible dans* $\mathbb{F}_q[X_1,\ldots,X_k]$, *il faut et il suffit que* $f(1,\frac{X_2}{X_1},\ldots,\frac{X_k}{X_1}) \in \mathbb{F}_q[\frac{X_2}{X_1},\ldots,\frac{X_k}{X_1}]$ *soit irréductible dans* $\mathbb{F}_q[\frac{X_2}{X_1},\ldots,\frac{X_k}{X_1}]$

La preuve découle du fait que si un polynôme homogène de $\mathbb{F}_q[X_1,\ldots,X_k]$ est un produit de deux polynômes de $\mathbb{F}_q[X_1,\ldots,X_k]$, alors ces deux derniers polynômes sont homogènes .

La proposition 3 et le lemme 4.1 permettent donc d'étudier l'irréductibilité de tout polynôme linéairement factorisable.

4.2. EXEMPLE. - Considérons le polynôme suivant de $\mathbb{F}_2[X_1,X_2]$:

$$f(X_1,X_2) = X_1^6 + X_2^6 + X_1X_2^5 + X_1^2X_2^4 + X_1^4X_2^2 + X_1X_2^4 + X_1^2X_2^3 + X_1^3X_2^2 + X_1^5 + X_1X_2^3 + X_1^2X_2^2 + X_2^4 + X_1^3 + X_1 + 1.$$

On a $f(X_1,0) = X_1^6 + X_1^5 + X_1^3 + X_1 + 1 = (X_1^2 + X_1 + 1)^3$,

$f(0,X_2) = X_2^6 + X_2^4 + 1 = (X_2^3 + X_2^2 + 1)^2$.

Les conditions 1) et 2) données dans la proposition 3 sont évidemment des conditions nécessaires pour qu'un polynôme soit linéairement factorisable et irréductible.

On est donc conduit à utiliser les éléments $j \in \mathbb{F}_{2^2}$ et $\theta \in \mathbb{F}_{2^3}$ respectivement définis par $1 + j + j^2 = 0$ et $1 + \theta + \theta^3 = 0$.

Un calcul relativement facile montre que

$$f(X_1,X_2) = \prod_{k=0}^{5} (1 + j^{2^k}X_1 + \theta^{2^k}X_2) .$$

Ceci montre que $f(X_1,X_2)$ est linéairement factorisable et irréductible dans $\mathbb{F}_2[X_1,X_2]$.

BIBLIOGRAPHIE.

[1] L. CARLITZ, *On factorable polynomials in several indeterminates*, Duke math. journ. 2, n° 4 (1936) p. 660.

[2] S. AGOU, *Polynômes sur un corps fini*, Bull. Sc. Math., 95 (1971), p. 327.

Manuscrit reçu le 20 septembre 1974.

Simon AGOU
Département de mathématiques
Université Claude Bernard, Lyon-1
43, boulevard du 11 novembre 1918
69621-VILLEURBANNE