PUBLICATIONS DU DÉPARTEMENT DE MATHÉMATIQUES DE LYON

SIMON AGOU

Polynômes irréductibles primitifs à coefficients dans un corps fini

Publications du Département de Mathématiques de Lyon, 1977, tome 14, fascicule 4 , p. 17-20

<http://www.numdam.org/item?id=PDML_1977__14_4_17_0>

Publications du
Département de
Mathématiques
Lyon 1977 t.14-4

POLYNOMES IRREDUCTIBLES PRIMITIFS A COEFFICIENTS DANS UN CORPS FINI

par Simon AGOU

I. INTRODUCTION.

Soit $f \in \mathbb{F}_q[X]$ (où $\mathbb{F}_q$ est le corps fini ayant q éléments) un polynôme irréductible tel que $f(0) \neq 0$; on appelle *exposant* de f l'ordre e(f) d'une racine de f dans $\mathbb{F}_q$ deg(f) (cf. [1]). On va donner une caractérisation des polynômes irréductibles de $\mathbb{F}_q[X]$ d'exposant donné. Pour cela, pour m et k entiers tels que $1 \leq k \leq m$, désignons par $r_{m,k}(X)$ le polynôme $\frac{(X^m) \ \ldots \ (X^m - X^k)}{(X-1) \ \ldots \ (X^k-1)}$ de $\mathbb{F}_q[X]$. Enfin on notera que la caractérisation que nous obtenons ci-dessous fait abstraction de la connaissance des diviseurs premiers de l'exposant.

PROPOSITION. - *Soient* e *un entier* ≥ 1, *premier à* q *et* ν *le plus petit entier tel que* $q^\nu - 1 \in \mathbb{Z}$ e. *Soit* $f \in \mathbb{F}_q[X]$ *un polynôme monique non réduit à* X.

Les propriétés suivantes sont équivalentes :

i) f *est irréductible dans* $\mathbb{F}_q[X]$, $e(f) = e$ *et* $\nu = \deg(f)$;

ii) f *divise les polynômes* $(-1)^e r_{e+1,e} + 1$ *et* $r_{e+1,k}$ *pour* $1 \leq k \leq e-1$ *dans* $\mathbb{F}_q[X]$.

Tout d'abord, pour tout entier $m \geq 2$, on a, dans $\mathbb{F}_q[X,Y]$.

$$(1) \quad \prod_{t=1}^{m-1} (Y - X^t) = Y^{m-1} + \sum_{k=1}^{m-1} (-1)^k r_{m,k}(X) \, Y^{m-1-k}$$, identité que l'on établit aisément par récurrence sur m.

Cela étant, montrons que (i) entraine ii). Soit θ une racine de f dans $\mathbb{F}_{q^\nu}^{\times}$. D'après (1), on a

$$\prod_{t=1}^{e} (Y - \theta^t) = Y^e + \sum_{k=1}^{e-1} (-1)^k r_{e+1,k}(\theta) Y^{e-k} + (-1)^e \theta^{e(e+1)/2} = Y^e - 1, \text{ puisque } \theta^e = 1.$$

(Si e = 1 , on a Y - θ = Y-1 et f = X-1 ; i) et ii) sont alors trivialement équivalentes).

Comme f est irréductible, on a

$$(-1)^e X^{e(e+1)/2} + 1 = (-1)^e r_{e+1,e}(X)+1 \equiv 0 \bmod. f(X).$$

et $r_{e+1,k}(X) \equiv 0 \bmod. f(X)$ pour $1 \leq k \leq e-1$.

Inversement, ii) entraîne i). Soit $\theta \in \bar{F}_q$ une racine de f(X). Comme $f(X) | X^e-1$, on a $\theta \neq 0$. *A fortiori*, on a $f(X) | X^{q^\nu-1}-1$. La formule (1) montre alors que $\prod_{t=1}^{e} (Y-\theta^t) = Y^e-1$.

Mais Y^e-1 a ses racines dans $\mathbb{F}_{q^\nu}^{x}$ et ces racines sont simples ; par suite, e est l'ordre de θ dans $\mathbb{F}_{q^\nu}^{x}$. Si $\nu > 1$, les éléments $\theta, \theta^q, \ldots, \theta^{q^{\nu-1}}$ de $\mathbb{F}_q^\nu$ sont des racines deux à deux distinctes de f(X), car l'égalité $\theta^{q^j-1} = 1$ $(1 \leq j \leq \nu-1)$ conduit à une contradiction ; elle implique en effet que $q^j - 1 \equiv 0 \bmod. e$, donc que $j \equiv 0 \bmod. \nu$.

Par suite, f vérifie la propriété (i).

N.B. On notera que l'on a fait abstraction de la connaissance des diviseurs de l'entier e.

REMARQUE. - Il résulte de la formule (1) que la condition ii) est équivalente à la suivante :

iii) $Y^e-1 - \prod_{t=1}^{e} (Y-X^t) \in (f\, \mathbb{F}_q[X])\, [Y]$.

On a, d'autre part, le corollaire suivant :

COROLLAIRE. - *Le pgcd des coefficients dans* $\mathbb{F}_q[X]$ *du polynôme* $Y^e-1-\prod_{t=1}^{e} (Y-X^t)$ *de* $\mathbb{F}_q[X,Y]$ *est le polynôme cyclotomique* $\Phi_e(X)$.

2. EXEMPLE. (cf. [1], § 52).

Déterminons les polynômes irréductibles primitifs de degré 2 de $\mathbb{F}_3[X]$; on a ici $e = 3^2-1 = 8$. En posant $f = X^2+aX+b$, on doit avoir

$Y^8-1- \prod_{t=1}^{8} (Y-X^t) \in (f\, \mathbb{F}_3[X])\, [Y]$.

Si f vérifie cette condition, f est irréductible dans $\mathbb{F}_3[X]$ et on a donc $(Y-X^3)(Y-X)-f(Y) \in (f\,\mathbb{F}_3[X])\,[Y]$. On a donc, mod.$(f\,\mathbb{F}_3[X])\,[Y]$ les congruences :

$$\prod_{t=1}^{8}(Y-X^t) \equiv (Y-X^3)(Y-X)(Y-X^7)(Y-X^5)(Y-1)(Y-X^4)(Y-X^2)(Y-X^6)\ ,$$

soit

$$\prod_{t=1}^{8}(Y-X^t) \equiv (Y^2+aY+b)(Y^2+abY+b)(Y-1)(Y-b)(Y^2-(b+1)X^2Y+b^2)$$

et, finalement

$$Y^8-1 \equiv (Y^2+aY+b)(Y^2+abY+b)(Y-1)(Y-b)(Y^2-(b+1)X^2Y+b^2).$$

En substituant 0 à Y, on en tire b = 2.

Ainsi $Y^8-1 = (Y^2+aY+2)(Y^2+2aY+2)(Y-1)(Y+1)(Y^2+1)$; on en déduit que $Y^4+1 = \phi_8(Y) = (Y^2+aY+2)(Y^2+2aY+2)$, soit $a^2 = 1$. Les polynômes cherchés sont donc les polynômes X^2+X+2 et X^2-X+2.

3. PROPOSITION . - *Soit* $f \in \mathbb{F}_q[X]$ *un polynôme monique, irréductible de degré* n *et tel que* $f(0) \neq 0$. *Soient* d *un diviseur de* n ,

$m = \dfrac{q^n-1}{q^d-1}$ *et* θ *une racine de* f. *Les propriétés suivantes sont équivalentes :*

i) θ^{q^d-1} *est d'ordre* m *dans* $\mathbb{F}_{q^n}^{\times}$;

ii) $Y^{q^{n-1}} - 1 - \prod_{t=1}^{m}(Y^{q^d-1}-X^{t(q^d-1)}) \in (f\,\mathbb{F}_q[X])\,[Y]$.

Montrons que i) entraine ii). Il est clair que $\{\theta^t\alpha\}_{\alpha \in \mathbb{F}_{q^d}^{\times},\ 1 \leq t \leq m}$ est $\mathbb{F}_{q^n}^{\times}$. On a donc $\prod_{t=1}^{m}\prod_{\alpha \in \mathbb{F}_{q^d}^{\times}}(Y-\theta^t\alpha) = \prod_{t=1}^{m}(Y^{q^d-1}-\theta^{t(q^d-1)}) = Y^{q^n-1}-1$.

Comme, par hypothèse, f est irréductible, on a ii). Inversement, soit δ un entier divisant m et tel que $\theta^{\delta(q^d-1)} = 1$. On a

$$\prod_{t=1}^{m} (Y^{q^d-1} - \theta^{t(q^d-1)}) = Y^{q^n-1} - 1$$
$$= \prod_{t=1}^{\delta} (Y^{q^d-1} - \theta^{t(q^d-1)})^{\frac{m}{\delta}}$$

Comme $Y^{q^n-1}-1$ n'a que des racines simples, on a $\delta = m$.

BIBLIOGRAPHIE. -

[1] L.E. DICKSON, *linear groups with an exposition of the galois field theory*, Dover, New-York (1958).

S. AGOU
Département de Mathématiques
43, bd du 11 novembre 1918
69621 VILLEURBANNE