PUBLICATIONS DU DÉPARTEMENT DE MATHÉMATIQUES DE LYON

SIMON AGOU

Factorisation des polynômes à coefficients dans un corps fini

Publications du Département de Mathématiques de Lyon, 1976, tome 13, fascicule 1 , p. 63-71

<http://www.numdam.org/item?id=PDML_1976__13_1_63_0>

Publications du
Département de
Mathématiques
Lyon 1976 t.13-1

FACTORISATION DES POLYNOMES A COEFFICIENTS DANS UN CORPS FINI

par Simon AGOU

Cet article donne un algorithme permettant de déterminer le produit de tous les polynômes irréductibles, de mêmes degrés, qui divisent un polynôme donné à une indéterminée à coefficients dans un corps fini. Une fois ce produit déterminé, une méthode est indiquée pour expliciter effectivement les polynômes irréductibles qui le composent.

1. NOTATIONS ET CONVENTIONS UTILISEES.

$\mathbf{F}_q$ dénote le corps fini à $q = p^s$ éléments, où p est un entier premier $f(X) = a_n X^n + \ldots + a_o$ désigne un polynôme monique ($a_n=1$) de $\mathbf{F}_q[X]$, de degré n.

Si m est un entier tel que $1 \leq m \leq n$, on définit les polynômes $\sigma_i(X)$ par l'égalité suivante, dans $F_q[X][Y]$:

$$\prod_{i=0}^{m-1} (Y - X^{q^i}) = Y^m - \sigma_1(X)Y^{m-1} - \ldots - \sigma_m(X).$$

Pour tout entier j tel que $0 \leq j \leq m-1$, on considère les polynômes

$$\pi_{f,m,j}(X) = a_j + \sum_{k=m}^{n} a_k \Big(\sum_{r_1+2r_2+\ldots+mr_m = k-j} \frac{(r_1+\ldots+r_m-1)!}{r_1!\ldots r_m!} \Big(\sum_{t=0}^{j} r_{m-t} \Big) \sigma_1^{r_1} \ldots \sigma_m^{r_m} \Big);$$

enfin, on pose

$$\Delta_{f,m} = \underset{0 \leq j \leq m-1}{p\ g\ c\ d} (\pi_{f,m,j}(X)).$$

$I_{f,m}$ désigne l'ensemble des polynômes moniques irréductibles de degrés m de $\mathbb{F}_q[X]$, divisant f.

2. RESULTATS.

THEOREME. - *Si* f(X) *est un polynôme monique sans racines multiples de* $\mathbb{F}_q[X]$, *on a*

$$p\ g\ c\ d\ (\Delta_{f,m}, X^{q^m} - X) = \prod_{f_i \in I_{f,m}} f_i .$$

Si $I_{f,m} = \emptyset$, on fait la convention usuelle sur le produit.

COROLLAIRE. - *Si* f(X) *est un polynôme monique de* $\mathbb{F}_q[X]$ *sans racines multiples, on a*

$$f(X) = \prod_{k=1}^{n} p\ g\ c\ d\ (\Delta_{f,k}, X^{q^k} - X).$$

3. PREUVES.

Nous établissons tout d'abord le lemme suivant :

LEMME 1. - *Avec les notations de* 1 *on a :*

$$f(X) = \sum_{j=0}^{m-1} \pi_{f,m,j}(X)\, X^j .$$

En effet, posons :

$$V_{f,m} = \begin{pmatrix} f(X) \\ f(X^q) \\ \vdots \\ f(X^{q^{m-1}}) \end{pmatrix} \quad \text{et} \quad V_{k,m} = \begin{pmatrix} X^k \\ X^{kq} \\ \vdots \\ X^{kq^{m-1}} \end{pmatrix} \quad \text{pour } k \in \mathbf{N}.$$

On a alors

$$(3.1) \quad V_{f,m} = \sum_{k=0}^{n} a_k V_{k,m} .$$

Pour j entier, $0 \leq j \leq m-1$, on a, en utilisant les propriétés des déterminants :

$$(3.2) \quad \frac{[V_{m-1,m}, V_{f,m}, V_{o,m}]}{[V_{m-1,m}, V_{j,m}, V_{o,m}]} = \sum_{k=0}^{n} a_k \frac{[V_{m-1,m}, \ldots, V_{k,m}, \ldots, V_{o,m}]}{[V_{m-1,m}, \ldots, V_{j,m}, \ldots, V_{o,m}]}$$

$$= a_j + \sum_{k=m}^{n} a_k \frac{[V_{m-1,m}, \ldots, V_{k,m}, \ldots, V_{o,m}]}{[V_{m-1,m}, \ldots, V_{j,m}, \ldots, V_{o,m}]} .$$

Mais, pour $k \geq m$, compte tenu des résultats établis dans I , on a la congruence

$$(3.3) \quad Y^k \equiv \sum_{j=0}^{m-1} \gamma_{k,j}\, Y^j \quad \text{modulo } ((Y-X)(Y-X^q)\ldots(Y-X^{q^{m-1}})),$$

$$\text{avec } \gamma_{k,j} = \sum_{r_1+2r_2+\ldots+mr_m=k-j} \frac{(r_1+\ldots+r_m-1)!}{r_1!\ldots r_m!} \left(\sum_{t=0}^{j} r_{m-t}\right) \sigma_1^{r_1} \ldots \sigma_m^{r_m} .$$

Compte tenu de (3.3) on a, pour $k \geq m$,

$$(3.4)\quad V_{k,m} = \sum_{\ell=0}^{m-1} \gamma_{k,\ell}\, V_{\ell,m}.$$

Par conséquent, pour $0 \leq J \leq m-1$, (3.2) fournit

$$(3.5)\quad \frac{\left[V_{m-1,m},\ldots V_{f,m},\ldots,V_{o,m}\right]}{\left[V_{m-1,m},\ldots,V_{j,m},\ldots,V_{o,m}\right]} = a_j + \sum_{k=m}^{n} a_k\, \gamma_{k,j} = \pi_{f,m,j}(X).$$

Par suite il est clair, par les formules de Cramer, que :

$$(3.6)\quad f(Y) \equiv \sum_{j=0}^{m-1} \pi_{f,m,j}(X) Y^j \text{ modulo } ((Y-X)(Y-X^q)\ldots(Y-X^{q^{m-1}})).$$

Il résulte finalement de (3.6) que :

$$(3.7)\quad f(X) = \sum_{j=0}^{m-1} \pi_{f,m,j}(X).X^j,$$

ce qui établit le lemme 1.

En particulier, (3.7) montre que $\Delta_{f,m}$ divise f.

LEMME 2. - *Si* f(X) *n'a que des racines simples et si* $\Delta_{f,m} \notin \mathbf{F}_q$, *alors* $\Delta_{f,m}$ *est un produit de polynômes moniques, irréductibles sur* $\mathbf{F}_q$, *distincts, de degrés au moins égaux à* m *et divisant* f(X).

Si θ est une racine de $\Delta_{f,m}$ dans la clôture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$, on a par la formule (3.6) :

$$f(Y) \equiv 0 \quad \text{modulo} \quad ((Y-\theta)(Y-\theta^q)\ldots(Y-\theta^{q^{m-1}})).$$

Comme, par hypothèse, f(X) n'a que des racines simples, il en résulte que le polynôme minimal de θ sur $\mathbb{F}_q$ est de degré $\geq$ m et divise f(X), puisqu'il divise $\Delta_{f,m}$.

PREUVE DU THEOREME. - Le lemme 2 et le fait que $X^{q^m} - X$ est le produit de tous les polynômes moniques et irréductibles de $\mathbb{F}_q[X]$ dont les degrés divisent m, montrent que p g c d $(\Delta_{f,m}; X^{q^m} - X)$ divise $\prod_{f_i \in I_{f,m}} f_i$.

Si $I_{f,m} = \emptyset$, alors p g c d $(\Delta_{f,m}; X^{q^m} - X) = \prod_{f_i \notin I_{f,m}} = 1$.

Si $I_{f,m} \neq \emptyset$, soient $f_i \in I_{f,m}$ et ξ une racine de f_i dans $\mathbb{F}_{q^m}$. La relation (3.5) montre que

$\pi_{f,m,j}(\xi) = 0$, puisque $V_{f,m}(\xi) = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ pour $0 \leq j \leq m-1$.

Ainsi $\prod_{f_i \notin I_{f,m}} f_i$ divise p g c d $(\Delta_{f,m}; X^{q^m} - X)$; d'où le théorème puisque ces polynômes sont moniques.

On peut remarquer que

$$\text{Card}(I_{f,m}) = \frac{\deg(\text{p g c d } (\Delta_{f,m} ; X^{q^m} - X))}{m}.$$

PREUVE DU COROLLAIRE. - C'est une conséquence du théorème, puisque les facteurs irréductibles de f ont des degrés $\leq n$.

4. REMARQUES

1/ Si g est un polynôme monique de $\mathbb{F}_q[X]$ tel que $g'(X) \neq 0$, on peut appliquer le théorème et son corollaire au polynôme.

$$f(X) = \frac{g}{p\,g\,c\,d\,(g,g')} ,$$

puis éventuellement poursuivre par la méthode de Lagrange.

Supposons f sans racines multiples,

1'/ Soit g un polynôme monique de degré m ; pour que g divise les $\pi_{f,m,j}$ (pour $j=0,\ldots,m-1$) il faut et il suffit que $g \in I_{f,m}$.

2/ Si $f = X^{q^n} - X$, alors $\Delta_{X^{q^n}-X,n}$ est le produit de tous les polynômes moniques irréductibles de $\mathbb{F}_q[X]$ de degrés n.

L'algorithme proposé fait abstraction *a priori* de la connaissance des diviseurs de l'entier n.

3/ Si f(X) est un polynôme monique de $\mathbb{F}_q[X]$, on a

$$p\,g\,c\,d\,(f,\Delta_{X^{q^n}-X,n}) = \prod_{f_i \in I_{f,n}} f_i .$$

4/ Enfin soit $f(X) = a_n X^n + \ldots + a_o$ un polynôme monique de $\mathbb{F}_q[X]$ de degré n. Supposons qu'il soit le produit de h ($h \geq 1$) polynômes irréductibles distincts de degrés $m \geq 1$.

Soit alors S le système de m équations, aux inconnues $\sigma_1,\ldots,\sigma_m$, à coefficients dans $\mathbb{F}_q$, défini par les m relations :

$$a_j + \sum_{k=m}^{n} a_k \Big(\sum_{r_1+2r_2+\ldots+mr_m=k-j} \frac{(r_1+\ldots+r_m-1)!}{r_1!\ldots r_m!} \Big(\sum_{t=0}^{j} r_{m-t} \Big) \sigma_1^{r_1} \ldots \sigma_m^{r_m} = 0,$$

pour les entiers $j \in [0,\ldots,m-1]$.

Avec l'hypothèse faite sur f(X), il est clair que S possède h solutions et h seulement dans $(\mathbb{F}_q)^m$, puisque le système S exprime que le reste de la division euclidienne de f(X) par le polynôme $X^m - \sigma_1 X^{m-1} \ldots - \sigma_m$, est nul.

Il en résulte qu'en substituant aux inconnues $\sigma_1,\ldots,\sigma_m$, les q éléments de $\mathbb{F}_q$, donc au plus après q^m essais, on obtiendra les h solutions du système S, ce qui fournira ainsi la factorisation effective de f(X), sur $\mathbb{F}_q$ en produit de polynômes irréductibles.

Compte tenu des remarques 1,2,3,4, du paragraphe 4, et éventuellement par applications réitérées de celles-ci, il s'ensuit que l'on peut ainsi factoriser tout polynôme à coefficients dans un corps fini.

5. EXEMPLE.

Soit $f(X) = X^8 + X^7 + X^5 + X^4 + X^3 + X + 1$ un polynôme de $\mathbb{F}_2[X]$.
On vérifie que $X^{2^4} \equiv X(f(X))$.
Prenons m = 4, et calculons les $\pi_{f,4,j}$ pour j = 0,1,2,3.

On a :

$$\pi_{f,4,0} = 1+\sigma_4+\sigma_1\sigma_4+\sigma_1^3\sigma_4+\sigma_3\sigma_4+\sigma_1^4\sigma_4+\sigma_1^2\sigma_2\sigma_4+\sigma_2^2\sigma_4+\sigma_4^2 ,$$

$$\pi_{f,4,1} = 1+\sigma_3+\sigma_1\sigma_3+\sigma_4+\sigma_1^3\sigma_3+\sigma_3^2+\sigma_1^2\sigma_4+\sigma_2\sigma_4+\sigma_1^4\sigma_3+\sigma_1^2\sigma_2\sigma_3+\sigma_2^2\sigma_3+\sigma_1^3\sigma_4,$$

$$\pi_{f,4,2} = \sigma_2+\sigma_1\sigma_2+\sigma_3+\sigma_1^3\sigma_2+\sigma_1^2\sigma_3+\sigma_1\sigma_4+\sigma_1^4\sigma_2+\sigma_1^2\sigma_2^2+\sigma_2^3+\sigma_1^3\sigma_3+\sigma_3^2+\sigma_1^2\sigma_4 ,$$

$$\pi_{f,4,3} = 1+\sigma_1+\sigma_1^2+\sigma_2+\sigma_1^4+\sigma_1^2\sigma_2+\sigma_2^2+\sigma_4+\sigma_1^5+\sigma_1\sigma_2^2+\sigma_1^2\sigma_3 ,$$

avec $\sigma_1 = X + X^2 + X^4 + X^8$, $\sigma_2 = X^3 + X^5 + X^6 + X^9 + X^{10} + X^{12}$,

$\sigma_3 = X^7 + X^{11} + X^{13} + X^{14}$, $\sigma_4 = X^{15}$.

On a $\sigma_1^2 \equiv \sigma_1(f)$, $\sigma_2^2 \equiv \sigma_2(f)$, $\sigma_3^2 \equiv \sigma_3(f)$, $\sigma_4 \equiv 1(f)$.

Par suite :

$$\pi_{f,4,0} \equiv 1 + \sigma_1 + \sigma_2 + \sigma_3 + \sigma_1\sigma_2 \quad (f) ,$$

$$\pi_{f,4,1} \equiv \sigma_2 + \sigma_1\sigma_3 + \sigma_2\sigma_3 + \sigma_1\sigma_2\sigma_3 \quad (f) ,$$

$$\pi_{f,4,2} \equiv 0 \quad (f) ,$$

$$\pi_{f,4,3} \equiv \sigma_1\sigma_3 \quad (f).$$

Mais $1 + \sigma_1 + \sigma_2 + \sigma_3 + \sigma_1\sigma_2 \equiv 0$ (f) et $\sigma_2 \equiv 0$ (f) ; donc $\pi_{f,4,1} \equiv 0$ (f), et $\pi_{f,4,3} \equiv 0$(f).

Ainsi $\Delta_{f,4} = f.f$ est donc le produit de deux polynômes du 4ème degré irréductibles sur $\mathbb{F}_2$. Pour les déterminer écrivons le système S :

$$S \begin{cases} 1 + \sigma_1\sigma_4 + \sigma_2\sigma_4 + \sigma_3\sigma_4 + \sigma_1\sigma_2\sigma_4 = 0 \\ 1 + \sigma_4 + \sigma_1\sigma_3 + \sigma_1\sigma_2\sigma_3 + \sigma_2\sigma_3 + \sigma_2\sigma_4 = 0 \\ 1 + \sigma_4 + \quad + \sigma_1\sigma_3 \qquad\qquad\qquad = 0 \end{cases}$$

Ce système a deux solutions et deux seulement dans $(\mathbb{F}_2)^4$.

En effet S est équivalent à :

$$S' \begin{cases} \sigma_1 + \sigma_3 = 1 , \quad \sigma_2 = 0 , \\ \sigma_1\sigma_3 = 0 \quad \sigma_4 = 1. \end{cases}$$

Ainsi $f(X) = (X^4+X+1)(X^4+X^3+1)$.

BIBLIOGRAPHIE.

I Simon AGOU, Formules explicites intervenant dans la division euclidienne des polynômes à coefficients dans un anneau unitaire et applications diverses. *Publ. Dep. Math. Lyon* , (1971) tome 8 fasc. 1 p. 107-121.

Manuscrit remis en octobre 1975.

Simon AGOU
Département de Mathématiques
Université Claude Bernard
43, bd du 11 novembre 1918
69621 VILLEURBANNE