FACTORISATION SUR UN CORPS FINI F_{p^n} DES POLYNÔMES COMPOSÉS $f(X^s)$ LORSQUE f(X) EST UN POLYNÔME IRRÉDUCTIBLE DE $F_{p^n}[X]$

Autor(en): **Agou, Simon**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **22 (1976)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **05.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-48189

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

FACTORISATION SUR UN CORPS FINI $\mathbf{F}_{p^n}$ DES POLYNÔMES COMPOSÉS $f(X^s)$ LORSQUE $f(X)$ EST UN POLYNÔME IRRÉDUCTIBLE DE $\mathbf{F}_{p^n}[X]$

par Simon AGOU

Soient p un entier premier, a un élément non nul algébrique sur $\mathbf{F}_p$, de degré m et s un entier $\geqslant 1$ et étranger à p.

On pose $q = p^m$; on a donc $\mathbf{F}_q = \mathbf{F}_p(a)$.

§ 0. Rappels.

Pour lire ce qui suit il convient de garder présentes à l'esprit les propriétés suivantes des corps finis.

Les démonstrations détaillées de ces propriétés peuvent être trouvées dans l'article de J. R. JOLY intitulé « Equations et variétés algébriques sur un corps fini » (*Enseignement Mathématique* 19, pp. 1-118).

Soient $\mathbf{F}_q$ et $\mathbf{F}_{q'}$ deux corps finis.

i) *Le groupe multiplicatif* $\mathbf{F}_q^\times$ *est cyclique d'ordre* $q-1$.

ii) *L'inclusion* $\mathbf{F}_q \subset \mathbf{F}_{q'}$ *équivaut à* q' *est une puissance de* q.

iii) *Si on pose* $K = \mathbf{F}_q$, $K' = \mathbf{F}_{q'}$, $q = p^l$, $q' = p^{l'}$ *on a:*

$$K \cap K' = \mathbf{F}_{p^{\mathrm{pgcd}(l,\, l')}}.$$

Le plus petit corps fini qui contient K *et* K' *est le corps* $\mathbf{F}_{p^{\mathrm{ppcm}(l,\, l')}}$.

iv) *Soit* $a \in \mathbf{F}_{q'}^\times$. *Pour que* a *soit une puissance* s*-ième dans* $\mathbf{F}_{q'}$ *il faut et il suffit que:*

$$a^{(q'-1)/\mathrm{pgcd}(s,\, q'-1)} = 1. \tag{1}$$

(Indiquons brièvement la démonstration de ce dernier point.
Si

$$a \in \mathbf{F}_{q'}^s,\ a = b^s \text{ et } a^{(q'-1)/\mathrm{pgcd}(s,\, q'-1)} = (b^{q'-1})^{s/\mathrm{pgcd}(s,\, q'-1)} = 1.$$

Réciproquement, la relation de Bezout montre qu'il existe $u \in \mathbf{Z}$ tel que:

$$us/\mathrm{pgcd}(s, q'-1) \equiv 1 \mod ((q'-1)/\mathrm{pgcd}(s, q'-1)).$$

Si $a = \gamma^\alpha$, où γ est un générateur du groupe $\mathbf{F}_{q'}^\times$, est tel que (1) soit satisfaite alors $\alpha \equiv 0 \bmod (\mathrm{p\,g\,c\,d}\,(s, q'-1))$. Par suite

$$(\alpha u / \mathrm{p\,g\,c\,d}\,(s, q'-1))\, s \equiv \alpha \mod ((\alpha / \mathrm{p\,g\,c\,d}\,(s, q'-1))(q'-1)).$$

Il en résulte que $a = \gamma^\alpha \in \mathbf{F}_{q'}^s$).

On se propose, d'abord, d'étudier la décomposition du binôme $X^s - a$ en facteurs irréductibles sur $\mathbf{F}_q$, puis d'étudier celle de $f(X^s)$ où f est un polynôme monique [1]) et irréductible de $\mathbf{F}_{p^n}[X]$.

NOTATIONS. Pour ce faire, nous utiliserons les notations suivantes.

On désigne par $\mathcal{O}$ l'ensemble des ordres de p dans les groupes $(\mathbf{Z}/d\mathbf{Z})^\times$, où d est un diviseur de s.

Pour $\rho \in \mathcal{O}$, on note Δ_ρ l'ensemble des diviseurs d de s tels que p soit d'ordre ρ dans $(\mathbf{Z}/d\mathbf{Z})^\times$.

§ 1. On désigne par $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$.

Soit $\xi \in \overline{\mathbf{F}}_p$ une racine de $X^s - a$; on note $h(\xi) = [\mathbf{F}_q(\xi) : \mathbf{F}_q]$ son degré sur $\mathbf{F}_q$, on désigne par h le *plus petit* des entiers $h(\xi)$.

1.1. LEMME. a) *h est le plus petit des entiers $\geqslant 1$ tels que*

$$a^{(q^h-1)/\mathrm{p\,g\,c\,d}\,(s,\, q^h-1)} = 1.$$

b) *Soit $\xi_0 \in \overline{\mathbf{F}}_p$ une racine de $X^s - a$, de degré h sur $\mathbf{F}_q$. Pour toute racine ξ de $X^s - a$ on a:*

$$\mathbf{F}_{q^h} = \mathbf{F}_q(\xi_0) \subset \mathbf{F}_q(\xi).$$

Preuve. Il est clair qu'il existe des entiers h_1 tels que:

$$a^{(p^{h_1}-1)/\mathrm{p\,g\,c\,d}\,(s,\, p^{h_1}-1)} = 1.$$

Comme $\mathbf{F}_p(a) = \mathbf{F}_{p^m}$ et qu'il existe une racine s-ième de a dans $\mathbf{F}_{p^{h_1}}$ on a $h_1 \in m\mathbf{Z}$, puisque $a \in \mathbf{F}_{p^{h_1}}$. Soit donc h le plus petit entier $\geqslant 1$ tel que

$$a^{(q^h-1)/\mathrm{p\,g\,c\,d}\,(s,\, q^h-1)} = 1.$$

Il existe par conséquent un élément ξ_0 de $\mathbf{F}_{q^h}$ tel que $a = \xi_0{}^s$. Mais $\mathbf{F}_q(\xi_0) \subset \mathbf{F}_{q^h}$ et a est une puissance s-ième dans $\mathbf{F}_q(\xi_0)$, par suite puisque h est minimal, on a $\mathbf{F}_q(\xi_0) = \mathbf{F}_{q^h}$.

---

[1]) Ou polynôme unitaire: le coefficient du terme de plus haut degré est égal à 1.

Soit maintenant ξ une racine de $X^s - a$; a est une puissance s-ième dans $\mathbf{F}_q(\xi)$. Posons $\mathbf{F}_q(\xi) = \mathbf{F}_{q^l}$.

La relation de Bezout montre qu'il existe $u, v \in \mathbf{Z}$ tels que:

$$u(q^l - 1) + v(q^h - 1) = q^{\mathrm{pgcd}(l,h)} - 1;$$

d'où en divisant par $\mathrm{pgcd}(s, q^{\mathrm{pgcd}(l,h)} - 1) = \delta$,

$$u\frac{(q^l - 1)}{\delta} + v\frac{q^h - 1}{\delta} = \frac{q^{\mathrm{pgcd}(l,h)} - 1}{\delta}.$$

On a alors

$$A = \frac{q^l - 1}{\delta} = \frac{q^l - 1}{\mathrm{pgcd}(s, q^l - 1)} \cdot \frac{\mathrm{pgcd}(s, q^l - 1)}{\delta},$$

$$B = \frac{q^h - 1}{\delta} = \frac{q^h - 1}{\mathrm{pgcd}(s, q^h - 1)} \cdot \frac{\mathrm{pgcd}(s, q^h - 1)}{\delta};$$

donc $a^A = 1$ et $a^B = 1$.

Il en résulte que $a^{(q^{\mathrm{pgcd}(l,h)} - 1)/\delta} = 1$.

Comme h est minimal, $\mathrm{pgcd}(l, h) = h$ et donc $\mathbf{F}_q(\xi_0) \subset \mathbf{F}_q(\xi)$.

1.2. Lemme. *Soient* $\xi_0, \eta \in \overline{\mathbf{F}}_p$, $\xi_0 \neq 0$. *On suppose que* $\mathbf{F}_q(\xi_0) \subset \mathbf{F}_q(\xi_0\eta)$ *et on note* ρ *le degré* $[\mathbf{F}_p(\eta) : \mathbf{F}_p]$ *et* h *le degré* $[\mathbf{F}_q(\xi_0) : \mathbf{F}_q]$. *Alors le degré* $[\mathbf{F}_q(\xi_0\eta) : \mathbf{F}_p]$ *est* $\mathrm{ppcm}(hm, \rho)$.

Comme $\mathbf{F}_q(\xi_0) \subset \mathbf{F}_q(\xi_0\eta)$, en posant $\mathbf{F}_q(\xi_0\eta) = \mathbf{F}_{p^k}$ on a: $hm \mid k$. De plus $(\xi_0\eta)^{p^k} = \xi_0^{p^k}\eta^{p^k} = \xi_0\eta = \xi_0\eta^{p^k}$; donc $\eta \in \mathbf{F}_{p^k}$ et donc $\rho \mid k$. Ainsi $\mathrm{ppcm}(hm, \rho) \mid k$.

Enfin $\xi_0\eta \in \mathbf{F}_{p^{\mathrm{ppcm}(hm,\rho)}}$; donc $\mathbf{F}_q(\xi_0\eta) \subset \mathbf{F}_{p^{\mathrm{ppcm}(hm,\rho)}}$ et $k \mid \mathrm{ppcm}(hm, \rho)$.

C.Q.F.D.

§ 2. On pose $D = \{\mathrm{ppcm}(hm, \rho) / m\}_{\rho \in \mathcal{O}}$, où h est l'entier défini au §1. Si $k \in D$, on note $\mathcal{O}_k$ l'ensemble des $\rho \in \mathcal{O}$ tels que $\mathrm{ppcm}(hm, \rho) = km$. Enfin, si $k \in D$, on pose

$$\nu(k) = \frac{1}{k} \sum_{\rho \in \mathcal{O}_k} \left(\sum_{d \in \Delta_\rho} \varphi(d) \right)$$

(où φ est l'indicateur d'Euler).

2.1. Proposition. *Dans* $\mathbf{F}_q[X]$ *le binôme* $X^s - a$ *est un produit de facteurs irréductibles distincts dont les degrés sont les éléments de* D. *Pour chaque* $k \in D$, *le nombre de facteurs irréductibles de degré* k *est* $\nu(k)$.

Dans le lemme 1.1, on a établi qu'il existait dans $\mathbf{F}_{q^h}$ une racine ξ_0 de $X^s - a$ telle que $\mathbf{F}_q(\xi_0) = \mathbf{F}_{q^h}$.

Les racines de $X^s - a$, sont donc les $\xi_0\eta$, où η est une racine de $X^s - 1$. Mais, dans $\mathbf{F}_p[X]$, on a $X^s - 1 = \prod_{d|s} \phi_d(X)$. Chaque polynôme cyclotomique $\phi_d(X)$ se décompose en polynômes irréductibles en nombre $\varphi(d)/\rho$, où ρ est l'ordre de p dans le groupe $(\mathbf{Z}/d\mathbf{Z})^\times$. Par suite, si η est une racine de $X^s - 1$ telle que $\mathbf{F}_p(\eta) = \mathbf{F}_{p^\rho}$, les lemmes 1.1 et 1.2 montrent que $\mathbf{F}_q(\xi_0\eta) = \mathbf{F}_{p^{\mathrm{ppcm}(hm,\rho)}}$.

Ainsi les racines de $X^s - a$ ont sur $\mathbf{F}_q$ des polynômes minimaux de degrés $\mathrm{ppcm}(hm, \rho)/m$, où ρ parcourt $\mathcal{O}$.

Pour chaque diviseur d de s, tel que l'ordre de p dans $(\mathbf{Z}/d\mathbf{Z})^\times$ soit ρ, il y a $\varphi(d)$ racines.

Le nombre de racines dont les polynômes minimaux ont pour degrés k $(k \in D)$ est donc $\sum_{\rho \in \mathcal{O}_k} \left(\sum_{d \in \Delta_\rho} \varphi(d)\right)$; par suite il y a $v(k)$ polynômes irréductibles factorisant $X^s - a$ dans $\mathbf{F}_q[X]$.

Il est évident qu'ils sont distincts, puisque s est étranger à p. Comme $X^s - a$ a $\mathrm{pgcd}(s, q^h - 1)$ racines dans $\mathbf{F}_{q^h}$, il en résulte que $h \mid \mathrm{pgcd}(s, q^h - 1)$.

C.Q.F.D.

2.2. *Exemples.*

(2.2.1) $p = 5,\ s = 12,\ m = 1,\ a = 3,\ X^{12} - 3 \in \mathbf{F}_5[X]$.

On trouve $h = 4$. $\mathcal{O} = \{1, 2\}$, $\Delta_1 = \{1, 2\}$, $\Delta_2 = \{3, 4, 6, 12\}$ et $D = \{4\}$. Les polynômes irréductibles de $\mathbf{F}_5[X]$ divisant $X^{12} - 3$ sont donc de degrés 4. On a $v(4) = \frac{1}{4} \sum_{d|12} \varphi(d) = 3$.

On a en effet $X^{12} - 3 = (X^4 - 2)(X^4 + 2X^2 + 3)(X^4 + 3X^2 + 3)$.

(2.2.2) $p = 5,\ s = 9,\ m = 1,\ a = 3,\ X^9 - 3 \in \mathbf{F}_5[X]$.

On trouve $h = 1$.

$$\mathcal{O} = \{1, 2, 6\} \qquad \Delta_1 = \{1\},\ \Delta_2 = \{3\},\ \Delta_6 = \{9\},$$
$$D = \{1, 2, 6\} \qquad \mathcal{O}_1 = \{1\},\ \mathcal{O}_2 = \{2\},\ \mathcal{O}_6 = \{6\}.$$
$$v(1) = v(2) = v(6) = 1.$$

On a donc trois polynômes irréductibles de degrés 1, 2, 6, divisant $X^9 - 3$ dans $\mathbf{F}_5[X]$.

On trouve en effet $X^9 - 3 = (X-3)(X^2+3X+4)(X^6+2X^3+4)$, avec $X^6 + 2X^3 + 4 = f(X^3)$ et $f(X) = X^2 + 2X + 4$, que l'on peut tester à l'aide de [I] ou de ce qui suit (cf. Proposition 2.3).

(2.2.3) $p = 7$, $s = 15$, $m = 1$, $a = 2$, $X^{15} - 2 \in \mathbf{F}_7[X]$:

On a $(\varphi(15), 15) = 1$. On trouve $h = 3$.

$$\begin{aligned} &\mathcal{O} = \{1,4\}, \quad \Delta_1 = \{1,3\}, \quad \Delta_4 = \{5,15\}, \\ &D = \{3,12\}, \quad \mathcal{O}_3 = \{1\}, \quad \mathcal{O}_{12} = \{4\}, \\ &v(3) = 1, \quad v(12) = 1. \end{aligned}$$

$X^{15} - 2$ est donc le produit d'un polynôme irréductible de degré 3 par un polynôme irréductible de degré 12.

On a $X^{15} - 2 = (X^3-4)(X^{12}+4X^9+2X^6+X^3+4)$ dans $\mathbf{F}_7[X]$, le dernier polynôme étant égal à $f(X^3)$ avec $f(X) = X^4 + 4X^3 + 2X^2 + X + 4$ (on peut le tester à l'aide des résultats parus dans [1] ou à l'aide de ce qui suit, cf. proposition 2.3.).

2.3. Proposition. *Soit $f(X)$ un polynôme monique irréductible de $\mathbf{F}_{p^n}[X]$, de degré s', tel que $f(0) \neq 0$. On appelle m le plus petit entier $\geqslant 1$ tel que $X^{p^m-1} \equiv 1 \bmod f(X)$ et on désigne par h le plus petit entier $\geqslant 1$ tel que*

$$X^{(q^h-1)/\mathrm{pgcd}(s,\, q^h-1)} - 1 \equiv 0 \bmod f(X), \text{ où } q = p^m.$$

Alors $f(X^s)$ se décompose dans $\mathbf{F}_{p^n}[X]$, en un produit de polynômes irréductibles distincts de degrés $s'k / \mathrm{pgcd}(k, ns'/m)$ où l'entier k décrit D. Pour chaque entier k il y a $\mathrm{pgcd}(k, ns'/m)\, v(k)$ polynômes irréductibles de degrés $ks' / \mathrm{pgcd}(k, ns'/m)$ divisant $f(X^s)$.

Preuve. Il existe $\theta \in \mathbf{F}_{p^{ns'}}^{\times}$, tel que $\mathbf{F}_{p^n}(\theta) = \mathbf{F}_{p^{ns'}}$. Soit m l'entier tel que $\mathbf{F}_p(\theta) = \mathbf{F}_{p^m}$. Il est clair que m est le plus petit entier tel que $X^{p^m} \equiv X \bmod f(X)$. De plus on a $m / \mathrm{pgcd}(m, n) = s'$. Dans $\mathbf{F}_q[X]$ on peut écrire:

$$f(X^s) = \prod_{j=0}^{s'-1} (X^s - \theta^{p^{nj}}).$$

La proposition 2.1 permet de décomposer chaque binôme $X^s - \theta^{p^{nj}}$, pour $j = 0, \ldots, s'-1$, en produit de polynômes irréductibles de $\mathbf{F}_q[X]$. (Il est clair, avec les hypothèses faites que $f(X^s)$ n'a que des racines simples.)

Les degrés de ces polynômes sont les éléments de D. Et pour chaque entier $k \in D$ il y en a $v(k)$.

Par le théorème 48 de [5] on sait comment se décomposent ces polynômes, dans $\mathbf{F}_{p^{ns'}}[X]$. On remarquera que $ns' = \text{p p c m}\,(m, n)$.

Si g est un tel polynôme de degré k, de $\mathbf{F}_q[X]$, g se décompose dans $\mathbf{F}_{p^{ns'}}[X]$ en $\text{p g c d}\,(k, ns'/m)$ polynômes de degrés $k/\text{p g c d}\,(k, ns'/m)$.

On sait aussi que $f(X^s)$ se décompose dans $\mathbf{F}_{p^n}[X]$ en un produit de polynômes irréductibles de degrés multiples de s'.

Soit donc $s'\lambda$ un degré d'un tel polynôme, irréductible. Celui-ci se décompose par le théorème 48 de [5] dans $\mathbf{F}_{p^{ns'}}[X]$ en $\text{p g c d}\,(s'\lambda, s') = s'$ polynômes irréductibles de degrés $s'\lambda/s' = \lambda$.

On a donc $\lambda = k/\text{p g c d}\,(k, ns'/m)$.

Ainsi les degrés des facteurs irréductibles de $f(X^s)$ sur $\mathbf{F}_{p^n}$ sont de la forme $s'k/\text{p g c d}\,(k, ns'/m)$, où $k \in D$. Le produit des s' binômes $X^s - \theta^{p^{nj}}$ $(j=0, \ldots, s'-1)$ de $\mathbf{F}_q[X]$, pour chaque entier $k \in D$, est divisible par $s' \,.\, v(k) \,.\, \text{p g c d}\,(k, ns'/m)$ polynômes irréductibles de $\mathbf{F}_{p^{ns'}}[X]$ de degrés $k/\text{p g c d}\,(k, ns'/m)$. Par ailleurs, ces polynômes proviennent de la décomposition dans $\mathbf{F}_{p^{ns'}}[X]$ des facteurs irréductibles sur $\mathbf{F}_{p^n}$ de $f(X^s)$ de degré $s'\lambda$, où $\lambda = k/\text{p g c d}\,(k, ns'/m)$. Il en résulte que le nombre de polynômes irréductibles sur $\mathbf{F}_{p^n}$, factorisant $f(X^s)$ est pour chaque entier $k \in D$, $v(k)\,\text{p g c d}\,(k, ns'/m)$.

C.Q.F.D.

Remarques. 1) Soit $s'' = s \,.\, p^{k'}$ un entier avec s et p étrangers. Le polynôme $f(X^{s''})$ de $\mathbf{F}_{p^n}[X]$ peut s'écrire $f(X^{s''}) = (g(X^s))^{p^{k'}}$, où $g(X)$ est un polynôme irréductible de $\mathbf{F}_{p^n}[X]$. On peut donc appliquer la proposition 2.3 à $g(X^s)$.

2) Pour que $f(X^s)$ soit irréductible dans $\mathbf{F}_{p^n}[X]$, il faut et il suffit que $h = s$ et que $\text{p g c d}\,(s, ns'/m) = 1$.

Illustrons la proposition 2.3.

Il est conseillé d'utiliser les tables [4].

2.4. *Exemples.*

(2.4.1.) Prenons $p = 2$, $n = 1$, $s = 15$ et soit $f(X)$ le polynôme irréductible $X^2 + X + 1$ de $\mathbf{F}_2[X]$.

On a $s' = 2$, et $m = 2$ car $X^2 + X + 1$ divise $X^3 - 1$ et de plus $3 = 2^m - 1 = 2^2 - 1$.

Etudions la factorisation de $f(X^{15}) = X^{30} + X^{15} + 1$ dans $\mathbf{F}_2[X]$.

On a $q = 2^m = 4$, et h est le plus petit entier tel que:

$$X^{(4^h-1)/\text{p g c d}\,(15,\,4^h-1)} - 1 \equiv 0 \mod (X^2+X+1)\,.$$

Il faut donc déterminer le plus petit entier h (nécessairement un diviseur de p g c d $(15, 4^h - 1)$) tel que:

$$(4^h - 1) / \mathrm{p\,g\,c\,d}(15, 4^h - 1) \equiv 0 \mod (2^2 - 1).$$

On trouve aisément $h = 3$.

Les diviseurs d de 15 sont les entiers 1, 3, 5, 15.

Les ordres de 2 dans les groupes $(\mathbf{Z}/d\mathbf{Z})^\times$ sont les entiers 1, 2, 4, car $2^1 \equiv 1 \mod 1$, $2^2 \equiv 1 \mod 3$, $2^4 \equiv 1 \mod 15$.

Ainsi $\mathcal{O} = \{1, 2, 4\}$, $\Delta_1 = \{1\}$, $\Delta_2 = \{3\}$ et $\Delta_4 = \{5, 15\}$. L'ensemble D est défini par:

$$D = \{\mathrm{p\,p\,c\,m}(hm, \rho)/m\}_{\rho \in \mathcal{O}} = \{\mathrm{p\,p\,c\,m}(6, \rho)/2\}_{\rho \in \{1,2,4\}} = \{3, 6\}.$$

On a donc $\mathcal{O}_3 = \{1, 2\}$, $\mathcal{O}_6 = \{4\}$.

Les degrés des polynômes irréductibles qui factorisent $X^{30} + X^{15} + 1$ dans $\mathbf{F}_2[X]$ sont donc les éléments de l'ensemble:

$$\{s'k / \mathrm{p\,g\,c\,d}(k, ns'/m)\}_{k \in D} = \{2k\}_{k \in D} = \{6, 12\}.$$

Calculons pour $k \in D$, les entiers $\nu(k)$ p g c d $(k, ns'/m) = \nu(k)$:

$$\nu(3) = \frac{1}{3} \sum_{\rho \in \mathcal{O}_3} \left(\sum_{d \in \Delta_\rho} \mathcal{S}(d) \right) = \frac{1}{3} \left(\mathcal{S}(1) + \mathcal{S}(3) \right) = 1,$$

$$\nu(6) = \frac{1}{6} \sum_{\rho \in \mathcal{O}_6} \left(\sum_{d \in \Delta_\rho} \mathcal{S}(d) \right) = \frac{1}{6} \left(\mathcal{S}(5) + \mathcal{S}(15) \right) = 2.$$

$X^{30} + X^{15} + 1$ est donc le produit de trois polynômes irréductibles de $\mathbf{F}_2[X]$. L'un est de degré 6, les deux autres sont de degré 12. On trouve en effet:

$$X^{30} + X^{15} + 1 = (X^6 + X^3 + 1)(X^{12} + X^3 + 1)(X^{12} + X^9 + 1).$$

Profitons de cette décomposition, pour utiliser la remarque 2, *sans recourir aux théorèmes classiques de* [5].

(2.4.2). Etude du polynôme $X^6 + X^3 + 1$ de $\mathbf{F}_2[X]$.

$$X^6 + X^3 + 1 = f(X^3) \quad \text{avec} \quad f(X) = X^2 + X + 1.$$

On a $p = 2$, $s' = 2$, $n = 1$, $m = 2$, $s = 3$. h est le plus petit entier tel que:

$$(2^{2h} - 1) / \mathrm{p\,g\,c\,d}(3, 2^{2h} - 1) \equiv 0 \mod (2^2 - 1),$$

d'où $h = s = 3$; la deuxième condition de la remarque 2 est satisfaite. $X^6 + X^3 + 1$ est donc irréductible sur $\mathbf{F}_2$.

(2.4.3) Etude du polynôme $X^{12} + X^3 + 1$ de $\mathbf{F}_2[X]$.

$X^{12} + X^3 + 1 = f(X^3)$ avec $f(X) = X^4 + X + 1$, qui est irréductible dans $\mathbf{F}_2[X]$.

On a $p = 2$, $s' = 4$, $n = 1$, $m = 4$, $s = 3$. h est le plus petit entier tel que:

$$(2^{4h} - 1) / \mathrm{pgcd}(3, 2^{4h} - 1) \equiv 0 \mod (2^4 - 1),$$

d'où $h = s = 3$; la deuxième condition de la remarque 2 est satisfaite. $X^{12} + X^3 + 1$ est donc irréductible sur $\mathbf{F}_2$.

(2.4.4) Etude du polynôme $X^{12} + X^9 + 1$ de $\mathbf{F}_2[X]$.

$X^{12} + X^9 + 1 = f(X^3)$ avec $f(X) = X^4 + X^3 + 1$, qui est irréductible dans $\mathbf{F}_2[X]$.

On a $p = 2$, $s' = 4$, $n = 1$, $m = 4$, $s = 3$ et comme ci-dessus: $h = s = 3$; la deuxième condition de la remarque 2 est satisfaite. $X^{12} + X^9 + 1$ est donc irréductible sur $\mathbf{F}_2$.

BIBLIOGRAPHIE

[1] Agou S., Critères d'irréductibilité des polynômes composés à coefficients dans un corps fini. *Acta Arithmetica 30*, n° 3 (à paraître).

[1'] —— Factorisation sur un corps fini $\mathbf{F}_{p^n}$ des polynômes composés $f(X^{p^r} - aX)$ lorsque $f(X)$ est un polynôme irréductible de $\mathbf{F}_{p^n}[X]$ (à paraître dans *Journal of Number Theory*).

[2] Borevitch Z. L. et I. R. Chaffarevitch. *Théorie des Nombres*. Gauthier-Villars, Paris.

[3] Bourbaki, N. *Polynômes et fractions rationnelles. Chap. 4 et 5. Corps commutatifs*. A.S.I. Hermann, Paris.

[4] Church, R. Tables of irreducible polynomials for the first four prime moduli. *Annals of Math. 36*, n° 1 (1935).

[5] Dickson L. E., *Linear groups with an exposition of the Galois field theory*. Dover Pub., Inc., New York.

C'est après avoir rédigé ce travail que j'ai appris l'existence par A. Schinzel, de l'article de M. C. R. Butler: The irreducible factors of $f(X^m)$ over a finite field. *J. London Math. Soc. 4* (1955), pp. 480-482.

On pourra cependant remarquer que nos résultats procèdent d'une méthode totalement différente de celle utilisée par Butler; de plus, les entiers $v(k)$ que nous définissons ne se trouvent pas dans Butler.

(Reçu le 25 mai 1976)

Simon Agou

Département de Mathématiques
Université de Lyon 1
43, bd du 11 novembre 1918
69621 Villeurbanne