Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 22 (1976)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: 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: Agou, Simon
Bibliographie
DOI: https://doi.org/10.5169/seals-48189

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:

$$(2^{4h} - 1) / \mathrm{p\,g\,c\,d}(3, 2^{4h} - 1) \equiv 0 \mod (2^4 - 1),$$

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