

**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>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 05.04.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

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:

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

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  $\nu(k)$  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