

SIMON AGOU

Sur la décomposition de certains idéaux premiers

Publications du Département de Mathématiques de Lyon, 1970,
tome 7, fascicule 1
, p. 41-46

http://www.numdam.org/item?id=PDML_1970__7_1_41_0

© Université de Lyon, 1970, tous droits réservés.

L'accès aux archives de la série « Publications du Département de mathématiques de Lyon » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR LA DECOMPOSITION DE CERTAINS IDEaux PREMIERS

par Simon AGOU

1. Soit p un nombre entier premier et s un entier ≥ 1 ; si $q = p^s$, on note $\mathbb{F}_q$ le corps à q éléments

Soit $f = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{F}_q[X]$ un polynome monique de degré $n > 1$. Supposons qu'il existe un polynome irréductible $g \in \mathbb{F}_q[X]$ tel que $f = g^d$, où d est un diviseur de n . Le degré m de g est n/d et $\mathbb{F}_q[X]/g\mathbb{F}_q[X]$ est isomorphe à $\mathbb{F}_{q^m}$. Si $\Theta \in \mathbb{F}_{q^m}$ est une racine de g ,

$\{\Theta, \Theta^q, \dots, \Theta^{q^{m-1}}\}$ est l'ensemble des racines de g , puisque $\mathbb{F}_{q^m}$ est une extension cyclique de $\mathbb{F}_q$. Ainsi, on a

$$g = \prod_{i=0}^{m-1} (X - \Theta^{q^i}) = X^m + \sigma_{q,d,m-1}(\Theta)X^{m-1} + \dots + \sigma_{q,d,0}(\Theta), \text{ où,}$$

pour $0 \leq i \leq m-1$, les coefficients $\sigma_{q,d,i}(\Theta)$ sont, au signe près, les fonctions élémentaires des racines de g . On peut alors écrire f sous la forme

$$f = X^n + \sum_{j,d,n-1}(\Theta)X^{n-1} + \dots + \sum_{j,d,0}(\Theta)$$

où les coefficients $\sum_{j,d,j}(\Theta)$ ($0 \leq j \leq n-1$) peuvent être exprimés en fonction de d et des $\sigma_{q,d,i}(\Theta)$ ($0 \leq i \leq m-1$), puisque $f = g^d$.

On a $X^{q^m} - X \in g\mathbb{F}_q[X]$. Considérons les polynomes $\sum_{j,d,j}(X) - a_j \in g\mathbb{F}_q[X]$ pour $0 \leq j \leq n-1$. Les résultants de ces polynomes, pris deux à deux, sont nuls. Désignons par $r_{q,d,j,k} \in \mathbb{F}_q$ ces résultants, pour tout couple (j,k) d'indices tels que $0 \leq j < k \leq n-1$.

Si donc pour tout diviseur d de n , il existe un couple (j,k) d'indices tel que $0 \leq j < k \leq n-1$ et que $r_{q,d,j,k} \neq 0$, alors le polynome f n'est pas une puissance d'un polynome irréductible de $\mathbb{F}_q[X]$. S'il en est ainsi, on dit que le polynome f est *q-décomposé*.

2. Soient K un corps de nombres algébriques et A l'anneau des entiers de K . Soit $\mathfrak{p}$ un idéal premier et non nul de A ; $\mathfrak{p}$ est au-dessus d'un entier premier que l'on désigne par p . $A/\mathfrak{p}$ est un corps fini ayant $q = p^s$ éléments, que l'on identifie à $\mathbb{F}_q$; d'où un homomorphisme $\varphi : A[X] \rightarrow \mathbb{F}_q[X]$.

Soient L une extension de degré fini $n > 1$ de K et B la fermeture intégrale de A dans L . Soit x un élément primitif de L sur K ; il existe $a \in A$ tel que $y = ax \in B$ et que y soit un élément primitif de L sur K .

Soit $f_{y,K}$ le polynome minimal de y sur K ; $f_{y,K}$ est monique, irréductible de degré n et appartient à $A[X]$. Comme $L = K(y)$, L est canoniquement isomorphe à $K[X]/f_{y,K}K[X]$.

Soit $f \in \mathbb{F}_q[X]$ l'image de $f_{y,K}$ par φ .

Proposition : *Si le polynome f est q-décomposé, l'idéal $\mathfrak{p}$ est décomposé dans B .*

Soit $A' = \sum_{i=0}^{n-1} Ay^i$; A' est un A -module libre de rang n et on a

$A \subset A' \subset B$; donc B est entier sur A' et A' est entier sur A . Pour démontrer la proposition, il suffit de prouver qu'il existe des idéaux premiers distincts $\mathfrak{P}_1$ et $\mathfrak{P}_2$ de A' , au-dessus de l'idéal $\mathfrak{p}$. Pour ce faire, on suit une démarche due à Kummer.

Par hypothèse, dans $\mathbb{F}_q[X]$, on a $f = \prod_{i=1}^t f_i^{e_i}$, où t est un entier ≥ 2

et où, pour $1 \leq i \leq t$, f_i est un polynome irréductible et e_i un entier > 0 .

Considérons, pour $1 \leq i \leq t$, l'homomorphisme composé

$$A[X] \xrightarrow{\varphi} \mathbb{F}_q[X] \xrightarrow{\beta_i} \mathbb{F}_q[X] / f_i \mathbb{F}_q[X].$$

Son noyau N_i est $g_i A[X] + \mathfrak{P}[X]$, où $g_i \in A[X]$ est tel que

$$\varphi(g_i) = f_i. \text{ On a } f_{y,K} = \prod_{i=1}^t g_i \in \mathfrak{P}[X]; \text{ par suite } f_{y,K} \in N_i.$$

D'autre part, $A = A[y]$ est isomorphe à $A[X] / f_{y,K} A[X]$.

Pour $1 \leq i \leq t$, on a le diagramme commutatif

$$\begin{array}{ccc} A[X] & \xrightarrow{\varphi} & \mathbb{F}_q[X] \\ \alpha \downarrow & & \downarrow \beta_i \\ A' & \xrightarrow{\psi_i} & \mathbb{F}_q[X] / f_i \mathbb{F}_q[X] \end{array}$$

où ψ_i est défini à l'aide de φ par passage aux quotients. Le noyau $\mathfrak{P}_i$ de ψ_i est un idéal maximal de A' puisque $\mathbb{F}_q[X] / f_i \mathbb{F}_q[X]$ est un corps. On a $\mathfrak{P} \subset \mathfrak{P}_i$, car $\alpha(\mathfrak{P}) \subset N_i$. Par suite, on a $\mathfrak{P}_i \cap A = \mathfrak{P}$.

Ainsi, pour $1 \leq i \leq t$, $\mathfrak{P}_i$ est au-dessus de $\mathfrak{P}$. Mais les polynômes f_i ($1 \leq i \leq t$) sont distincts, les corps $\mathbb{F}_q[X] / f_i \mathbb{F}_q[X]$ le sont aussi et il en est de même des idéaux $\mathfrak{P}_i$. Comme B est entier sur A' , la proposition s'ensuit immédiatement.

3. Condition nécessaire et suffisante d'irréductibilité d'un polynôme sur un corps fini.

Soit $f = x^n + a_{n-1}X^{n-1} + \dots + a_0$ un polynôme monique de $\mathbb{F}_q[X]$, de degré $n > 1$. Si f est irréductible sur $\mathbb{F}_q$ il divise les polynômes $\sigma_{q,1,k}(X)$

pour $k = 0, \dots, n-1$. On notera désormais par $\sigma_k(X)$ les polynômes $(-1)^{n-k} \sigma_{q,1,k}(X)$ et on les appellera les *polynômes associés* à f .

Réciproquement, supposons que f divise ses polynômes associés σ_k ($k = 0, \dots, n-1$).

On a : $\sigma_{n-1} = X^{q^{n-1}} + X^{q^{n-2}} + \dots + X + a_{n-1}$ et $\sigma'_{n-1} = 1$. Ainsi σ_{n-1} n'a que des racines simples. Par suite, f n'a que des racines simples. Soit alors m un entier tel que $0 < m < n$. Les polynômes $\sigma_0, \dots, \sigma_{n-1}$, $X^{q^m} - X$ sont premiers entre eux dans leur ensemble. En effet, dans le cas contraire, pour un entier $m < n$, il existerait $\xi \in \mathbb{F}_{q^m}$ tel que $\sigma_k(\xi) = 0$ pour $k = 0, \dots, n-1$, et, par conséquent, on aurait

$$f = (X - \xi)(X - \xi^q) \dots (X - \xi^{q^{n-1}}) ;$$

mais $\xi^{q^m} = \xi$, f aurait donc au moins une racine double. Il en résulte que les seuls facteurs irréductibles éventuels de f sont de degré n ; donc f est irréductible dans $\mathbb{F}_q[X]$. D'où :

Proposition : *Pour qu'un polynôme monique $f \in \mathbb{F}_q[X]$ soit irréductible, il faut et il suffit que f divise ses polynômes associés.*

(Remarquons que si f , est du premier degré, f est identique à son polynome associé.)

On peut sensiblement améliorer le résultat, en procédant de la façon suivante :

Considérons : le polynome nul :

$$(X-X)(X-X^q)\dots(X-X^{q^{n-1}}) = 0$$

Développé il s'écrit :

$$\begin{aligned} 0 = X^n - (\sigma_{n-1}(X) - a_{n-1})X^{n-1} + \dots + (-1)^k (\sigma_{n-k}(X) + (-1)^k a_{n-k})X^{n-k} + \\ + (-1)^n (\sigma_0(X) + (-1)^n a_0) \end{aligned}$$

soit encore : $f - \sigma_{n-1}(X).X^{n-1} + \dots + (-1)^n \sigma_0(X) = 0$. Pour que f divise ses n polynômes associés, il faut et il suffit qu'il divise les polynômes $\sigma_k(X)$ d'indices $k = 1, \dots, n-1$.

Comme conséquence dans le cas où $n = 2$ on a :

Corollaire : Pour que $X^2 + a_1X + a_0$ soit irréductible dans $\mathbb{F}_q[X]$, il faut et il suffit que $X^q + X + a_1 \equiv 0 \pmod{X^2 + a_1X + a_0}$

4. Voici un exemple d'application du paragraphe 3.

Soit $f = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ un polynôme de degré 4 de $\mathbb{F}_2[X]$. Si le polynôme f est irréductible, on a $a_0 = 1$, $(a_1 + a_2)a_3 = 0$, $(1 + a_3)a_2 = 0$, $(1 + a_1)(1 + a_3) = 0$, et réciproquement.

En effet, il est clair que $a_0 = 1$. De plus, f divise $u = X^8 + X^4 + X^2 + X + a_3$ et, bien entendu, le reste r de la division euclidienne de u par f^2 ; le reste de la division euclidienne de r par f est

$(a_1 + a_2)a_3X^3 + (1 + a_1 + a_3(a_0 + a_1))X^2 + (1 + a_1 + a_0a_3 + a_1a_2 + a_1a_3 + a_1a_2a_3)X^2$
 $+ a_3 + a_0a_2 + a_0a_3 + a_0a_2a_3$. En écrivant que ce reste est nul, on trouve les conditions mentionnées ci-dessus

Ces conditions entraînent que dans $\mathbb{F}_2$, on a $a_0 = 1$, $a_1 = 1$, $a_2 = a_3 = 0$ ou bien $a_0 = 1$, $a_1 = a_2$, $a_3 = 1$. (on retrouve la condition $a_1 + a_2 + a_3 = f(1) = 1$).

Par suite, les polynômes irréductibles de $\mathbb{F}_2[X]$, de degré 4 ne peuvent être que les trois polynômes (sur les quatre possibles) :

$$X^4 + X + 1, \quad X^4 + X^3 + 1, \quad X^4 + X^3 + X^2 + X + 1 \quad (\text{polynôme cyclotomique}).$$

Et on s'assure facilement que ces polynômes sont irréductibles dans $\mathbb{F}_2[X]$, car on sait que le nombre des polynômes irréductibles de $\mathbb{F}_2[X]$ de degré 4 est $(2^4 - 2^2)/2 = 3$.

En fait, dans ce cas particulier, la seule considération du polynôme associé à f de plus bas degré a permis de conclure.

BIBLIOGRAPHIE

- [1] N. BOURBAKI Algèbre, ch. 4 et 6, Act. Scient. et Indus: 1959.
 - [2] N. BOURBAKI Algèbre commutative, ch. 5 et 7
Act. Scient. et Indust. 1964 (1308).
 - [3] J. BRACONNIER Bases de la théorie des nombres,
Séminaire du Département de mathématiques
de Lyon, 1966-1967 - 1968-1969.
 - [4] P. SAMUEL Théorie algébrique des nombres.
 - [5] O. ZARISKI et
P. SAMUEL Commutative algebra. Vol. 1 Van Nostrand
1960.
-

Manuscrit remis en décembre 1969.

AGOU Simon
Maître-assistant
Département de Mathématiques
Faculté des Sciences
43, bd du 11 novembre 1918
69 - VILLEURBANNE