

S. AGOU

**Formules explicites intervenant dans la division euclidienne des polynômes à coefficients dans un anneau unitaire et applications diverses**

*Publications du Département de Mathématiques de Lyon*, 1971,  
tome 8, fascicule 1  
, p. 107-121

[http://www.numdam.org/item?id=PDML\\_1971\\_\\_8\\_1\\_107\\_0](http://www.numdam.org/item?id=PDML_1971__8_1_107_0)

© Université de Lyon, 1971, 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/>

**FORMULES EXPLICITES INTERVENANT  
 DANS LA DIVISION EUCLIDIENNE  
 DES POLYNOMES A COEFFICIENTS  
 DANS UN ANNEAU UNITAIRE  
 ET APPLICATIONS DIVERSES**

S. AGOU

PREMIERE PARTIE.

Soit  $A$  un anneau unitaire.

Soit  $f = X^n - \sigma_1 X^{n-1} - \dots - \sigma_n = (X - X_1) \dots (X - X_n)$  un polynôme de degré  $n \geq 1$  de  $A[X, X_1, \dots, X_n]$ . Enfin soit  $k \in \mathbb{N}^{\times}$  un entier. On désigne par  $\sum_{j=0}^{n-1} \alpha_{k,j} X^j$  le reste de la division euclidienne du monôme  $X^{k+n-1}$  par le polynôme  $f$  dans  $A[X_1, \dots, X_n][X]$ . On se propose dans cette partie de donner les expressions explicites des  $\alpha_{k,j}$ ,  $j=0, \dots, n-1$ . Il est immédiat que pour  $j=0, \dots, n-1$ ,  $\alpha_{k,j} \in A[X_1, \dots, X_n]$ . Les formules de Cramer, montrent que les coefficients  $\alpha_{k,j}$  pour  $j=0, \dots, n-1$ , sont des polynômes symétriques homogènes en les  $X_i$ ,  $i=1, \dots, n$ , et par conséquent s'expriment à l'aide des coefficients  $\sigma_j$ ,  $j=1, \dots, n$  de  $f$ .

De façon précise posons pour alléger les notations :

$$\sum_u' = \sum_{\substack{r_1+2r_2+\dots+n r_n = u \\ r_i \in \mathbb{N} \quad i=1, \dots, n}} \frac{(r_1+\dots+r_n)!}{r_1! \dots r_n!} \sigma_1^{r_1} \dots \sigma_n^{r_n} \quad \text{si } u \in \mathbb{N}$$

et

$$\sum_u' = 0 \quad \text{si } -n+1 \leq u < 0 \\ \text{(si } n > 1)$$

en convenant que  $0^0 = 1$ .

Ceci étant on a :

$$\alpha_{k,j} = \sum_{\substack{r_1+2r_2+\dots+n r_n = k+n-j-1 \\ r_i \in \mathbb{N}, \quad i=1, \dots, n}} \left( \frac{(r_1+\dots+r_n-1)!}{r_1! \dots r_n!} \sum_{t=0}^j r_{n-t} \right) \sigma_1^{r_1} \dots \sigma_n^{r_n}$$

pour  $j = 0, \dots, n-1$

avec également :

$$\alpha_{k,0} = \sigma_n \cdot \sum_{k-1}$$

PREUVES.

Etablissons tout d'abord que :

$$(1) \quad \alpha_{k,n-1} = \sum_k' \quad k \in \mathbb{N}^n$$

on a :  $\alpha_{k,n-1} = \frac{\begin{vmatrix} X_1^{k+n-1} & \dots & 1 \\ \vdots & & \vdots \\ X_n^{k+n-1} & \dots & 1 \end{vmatrix}}{\begin{vmatrix} X_1^{n-1} & \dots & 1 \\ \vdots & & \vdots \\ X_n^{n-1} & \dots & 1 \end{vmatrix}}$

mais :  $X^{k+n-1} \equiv \sigma_1 X^{n-1+k-1} + \dots + \sigma_n X^{k-1} \pmod{f}$  pour  $k \geq 1$ .

Procédons par récurrence sur  $k$ . Pour  $k = 1$  la formule (1) est vérifiée. Supposons la établie pour tous les entiers au plus égaux à  $k$ . Alors elle est vraie pour  $k+1$ , en effet, cela revient à vérifier que l'on a :

$$\sum_{k+1}' = \sigma_1 \sum_k' + \dots + \sigma_n \sum_{k-n+1}' \quad *$$

les deux membres sont des polynômes symétriques homogènes en  $X_1, \dots, X_n$  de degré  $k+1$ . Il n'y a donc qu'à vérifier l'égalité

des coefficients des monômes  $\sigma_1^{r_1} \dots \sigma_n^{r_n}$  dans chacune des expressions, ce qui résulte aisément de l'identité :

$$\frac{(r_1 + \dots + r_n)!}{r_1! \dots r_n!} = \frac{(r_1 + \dots + r_{n-1})!}{(r_1 - 1)! \dots r_n!} + \dots + \frac{(r_1 + \dots + r_{n-1})!}{r_1! \dots (r_n - 1)!}$$

en convenant que  $\frac{1}{(-1)!} = 0$ .

Etablissons maintenant les expressions des  $\alpha_{k,j}$  pour  $0 \leq j < n-1$  (si  $n > 1$ ).

On a :  $X^{k+n} = X \cdot X^{k+n-1} \equiv \alpha_{k,n-1} X^n + \dots + \alpha_{k,0} X \pmod{f}$

d'où pour  $k \geq 0$ ,

$$(i) \quad \alpha_{k+1,0} = \sigma_n \cdot \alpha_{k,n-1}$$

$$(ii) \quad \alpha_{k+1,j} = \sigma_{n-j} \alpha_{k,n-1} + \alpha_{k,j-1} \quad \text{si } j \geq 1$$

de (i) on déduit que  $\alpha_{k,0} = \sigma_n \cdot \sum_{k-1}^{\prime}$ .

On déduit de (ii) que :

$$\alpha_{k+1,j} = \sigma_{n-j} \alpha_{k,n-1} + \sigma_{n-j+1} \alpha_{k-1,n-1} + \dots + \sigma_n \alpha_{k-j,n-1}$$

ce qui conduit à l'expression :

$$\alpha_{k,j} = \sum_{t=0}^j (\sigma_{n-j+t} \sum_{k-t-1}^{\prime}) \text{ pour } k \in \mathbb{N}^* \text{ et } j \geq 1$$

On tire de la relation  $\mathfrak{R}$  :

$$\sum_{k+n-j-1}^{\prime} = \sigma_1 \sum_{k+n-j-2}^{\prime} + \dots + \sigma_{n-j-1} \sum_k^{\prime} + \alpha_{k,j}$$

Formules explicites intervenant dans la division euclidienne ...

et donc  $\alpha_{k,j} = \binom{k+n-j-1}{k+n-j-1} \sigma_1 \binom{k+n-j-2}{k+n-j-2} \dots \sigma_{n-j-1} \binom{k+n-j-1}{k}$

ainsi :

$$\alpha_{k,j} = \sum_{\substack{r_1+2r_2+\dots+nr_n=k+n-j-1 \\ r_i \in \mathbb{N}, i=1, \dots, n}} \frac{(r_1+\dots+r_n-1)!}{r_1! \dots r_n!} \left( \sum_{t=0}^j r_{n-t} \right) \sigma_1^{r_1} \dots \sigma_n^{r_n}$$

pour  $k \geq 1$ .

c.q.f.d.

Complétons les résultats qui précèdent, en donnant l'expression du quotient  $\chi(X)$  de la division Euclidienne du monôme  $X^{k+n-1}$  par le polynôme  $f = X^n - \sigma_1 X^{n-1} \dots - \sigma_n$ .

On a : 
$$\chi(X) = \sum_{t=0}^{k-1} \left( \sum_{k-1-t} \right) X^t$$

En effet, posons  $\sigma_0 = -1$ .

Il suffit de montrer que

$$\deg(X^{k+n-1} + \left( \sum_{j=0}^n \sigma_{n-j} X^j \right) \left( \sum_{t=0}^{k-1} \left( \sum_{k-1-t} \right) X^t \right)) \leq n-1$$

Ecrivons que  $\left( \sum_{j=0}^n \sigma_{n-j} X^j \right) \left( \sum_{t=0}^{k-1} \sum_{k-1-t} X^t \right) = \sum_{u=0}^{k+n-1} c_u X^u$  ;

Considérons les coefficients  $c_u$  d'indices  $u$ ,  $n \leq u \leq k+n-1$ .

$$\text{On a } c_u = \sum_{t+j=u} \sigma_{n-j} \sum_{k-1-t}^{\prime} = \sum_{j=n}^0 \sigma_{n-j} \sum_{k-1+j-u}^{\prime}$$

avec  $0 \leq j \leq n$ ,  $0 \leq t \leq k-1$ .

On voit alors aisément que  $c_{k+n-1} = \sigma_0 = -1$ , et que si  $n \leq u \leq k+n-1$  (si  $k \geq 2$ )  $c_u = 0$ , en vertu de la relation  $\kappa$ .

Par conséquent on peut écrire :

$$\begin{aligned} X^{k+n-1} &= (X^n - \sigma_1 X^{n-1} \dots - \sigma_n) \cdot \left( \sum_{t=0}^{k-1} \left( \sum_{\substack{r_1+2r_2+\dots+nr_n=k-1-t \\ r_1, \dots, r_n \in \mathbb{N}}} \frac{(r_1+\dots+r_n)!}{r_1! \dots r_n!} \sigma_1^{r_1} \dots \sigma_n^{r_n} \right) X^t \right) \\ &+ \sum_{j=0}^{n-1} \left( \sum_{\substack{r_1+2r_2+\dots+nr_n=k+n-j-1 \\ r_1, \dots, r_n \in \mathbb{N}}} \frac{(r_1+\dots+r_n-1)!}{r_1! \dots r_n!} \left( \sum_{t=0}^j r_{n-t} \right) \sigma_1^{r_1} \dots \sigma_n^{r_n} \right) X^j. \end{aligned}$$

## DEUXIEME PARTIE.

### APPLICATIONS.

#### 1. Identités dans les corps finis.

Prenons pour  $A$  le corps fini  $\mathbb{F}_q$ .

a/. Soit  $f = X^2 - \sigma_1 X - \sigma_2 \in \mathbb{F}_q[X]$ .

. si  $\sigma_1^2 + 4\sigma_2 \neq 0$  alors 
$$\sum_{q-1} ' = \frac{\begin{vmatrix} x_1^q & 1 \\ x_2^q & 1 \\ x_1 & 1 \\ x_2 & 1 \end{vmatrix}}$$

en désignant par  $x_1$  et  $x_2$  les racines de  $f$  dans  $\mathbb{F}_{q^2}$

par suite : 
$$\sum_{q-1} ' = (\sigma_1^2 + 4\sigma_2)^{\frac{q-1}{2}}$$

. si  $\sigma_1^2 + 4\sigma_2 = 0$ , considérons la congruence.

$$X^q \equiv \sum_{q-1} ' \cdot X + \sigma_2 \sum_{q-2} ' \pmod{f}$$

si on la dérive il vient

$$- \sum_{q-1} ' = \chi f' + \chi' f, \text{ en désignant par } \chi \text{ le quotient de la}$$

division Euclidienne de  $X^q$  par  $f$ .

et donc 
$$\sum_{q-1} ' = 0 .$$



Ainsi dans tout corps fini  $F_q$  on a l'identité :

$$(\sigma_1^2 + 4\sigma_2)^{\frac{q-1}{2}} = \sum_{\substack{r_1+2r_2=q-1 \\ r_1, r_2 \in \mathbb{N}}} \frac{(r_1+r_2)!}{r_1!r_2!} \sigma_1^{r_1} \sigma_2^{r_2}$$

b/. On peut établir de même d'autres identités dans  $F_q$  par le même procédé.

Par exemple prenons  $f = X^3 - \sigma_1 X^2 - \sigma_2 X - \sigma_3 \in \mathbb{F}_q[X]$  et désignons par  $x_1, x_2, x_3$  ses racines dans  $\mathbb{F}_{q^6}$ . On a si les racines sont distinctes :

$$\begin{vmatrix} x_1^2 & x_1 & 1 \\ x_2^2 & x_2 & 1 \\ x_3^2 & x_3 & 1 \end{vmatrix} = \sum_{\substack{r \\ q^2-2}} \delta \text{ avec } \delta = \begin{vmatrix} x_1^2 & x_1 & 1 \\ x_2^2 & x_2 & 1 \\ x_3^2 & x_3 & 1 \end{vmatrix}$$

mais

$$\begin{vmatrix} x_1^2 & x_1 & 1 \\ x_2^2 & x_2 & 1 \\ x_3^2 & x_3 & 1 \end{vmatrix} = \begin{vmatrix} x_1^2 & x_1^6 & 1 \\ x_2^2 & x_2^6 & 1 \\ x_3^2 & x_3^6 & 1 \end{vmatrix} = \left( - \begin{vmatrix} x_1^4 & x_1 & 1 \\ x_2^4 & x_2 & 1 \\ x_3^4 & x_3 & 1 \end{vmatrix} \right)^{q^2}$$

$$\text{Ainsi } \sum_{\substack{r \\ q^2-2}} \delta = (-\delta \cdot \sum_{\substack{r \\ q^4-2}} \delta)^{q^2}$$

et comme  $\delta \neq 0$  
$$\sum_{q^2-2}^{\prime} = (-1)^{q^2} \delta^{q^2-1} \sum_{q^4-2}^{\prime} .$$

Si donc on désigne par D le discriminant de f ( $D = \delta^2$ )

on a : 
$$\sum_{q^2-2}^{\prime} = (-1)^{q^2} D^{\frac{q^2-1}{2}} \cdot \sum_{q^4-2}^{\prime}$$

Supposons désormais la caractéristique de  $F_q$  différente de 2.

Supposons qu'il y ait une racine triple.

On a : 
$$X^{q^2} - \alpha_{q^2-2,2} X^2 - \alpha_{q^2-2,1} X - \alpha_{q^2-2,0} = \chi f$$

En dérivant deux fois il vient 
$$\alpha_{q^2-2,2} = 0 .$$

Un calcul élémentaire montre que,

$$D = \sigma_1^2 \sigma_2^2 + 4\sigma_2^3 - 4\sigma_1^3 \sigma_3 - 27\sigma_3^2 - 18\sigma_1 \sigma_2 \sigma_3$$

finalement :

si  $D \neq 0$  on a dans tout corps fini  $\mathbb{F}_q$  la relation :

$$\sum_{q^2-2}^{\prime} = (-1)^{q^2} D^{\frac{q^2-1}{2}} \cdot \sum_{q^4-2}^{\prime}$$

si f a une racine triple, l'identité précédente subsiste dans les corps finis dont la caractéristique est différente de 2.

2. Conditions suffisantes d'irréductibilité d'un polynôme à coefficients dans un corps de nombres algébriques.

Soient  $K$  un corps de nombres algébriques,  $A$  l'anneau des entiers de  $K$  et  $f$  un polynôme de  $K[X]$  de degré  $n \geq 1$ . Pour étudier l'irréductibilité de  $f$  sur  $K$ , il est loisible de supposer que  $f$  est monique et qu'il appartient à  $A[X]$ .

Soit  $\mathfrak{p}$  un idéal premier non nul de  $A$  de norme  $q$ .

Pour tout entier  $s$ ,  $1 \leq s \leq n$ , on désigne par  $E_s$  l'ensemble des suites strictement décroissantes de  $s$  entiers de l'intervalle  $[0, n-1]$ . Si  $v = (i_1, \dots, i_s)$  est une telle suite, on dénotera par  $q^{[v]}$  l'entier  $q^{i_1} + q^{i_2} + \dots + q^{i_s}$ . Enfin l'ensemble des  $v \in E_s$  tels que  $q^{[v]} \leq n-1$  sera noté  $E'_s$ .

Si  $\varphi$  est le morphisme :  $A[X] \rightarrow A/\mathfrak{p}[X]$ , une condition suffisante pour que  $f$  soit irréductible sur  $K$  est que  $\varphi(f)$  soit irréductible dans  $A/\mathfrak{p}[X]$ . En utilisant des résultats établis dans [1] et [2] on a donc, avec les notations précédentes la :

*PROPOSITION.* Soit  $f = X^n - \sigma_1 X^{n-1} \dots - \sigma_n$  un polynôme monique de  $A[X]$ , de degré  $n \geq 1$ . Si pour tout entier  $s \in [1, \dots, n]$  on a :

$$\sum_{j=0}^{n-1} \left( \sum_{v \in E'_s - E'_s} \left( \sum_{\substack{r_1 + 2r_2 + \dots + nr_n = q^{[v]} - j \\ r_1, \dots, r_n \in \mathbb{N}}} \frac{(r_1 + \dots + r_n - 1)!}{r_1! \dots r_n!} \left( \sum_{t=0}^j r_{n-t} \right) \sigma_1^{r_1} \dots \sigma_n^{r_n} \right) + \sum_{v \in E'_s} \delta_{q^{[v]}, j} \right) X^{j+(-1)^s} \sigma_s \in \mathfrak{p}[X]$$

alors le polynôme  $f$  est irréductible sur  $K$ .

$(\delta_q[v], j)$  désigne le symbole de Kronecker, et, par convention,

on a  $\sum_{v \in E'_s} = 0$  si  $E'_s = \emptyset$  pour un entier  $s$ ).

### 3. Suites définies par certaines relations de récurrence linéaires.

Soit  $A$  un anneau commutatif unitaire,  $n$  un entier  $\geq 1$  et  $a_1, \dots, a_n$   $n$  éléments de  $A$ .

Soit la suite  $(u_m)_{m \in \mathbb{N}}$  définie par la relation de récurrence  $u_{k+n} = a_1 u_{k+n-1} + \dots + a_n u_k$  pour  $k \geq 0$ , et les valeurs initiales  $u_0, \dots, u_{n-1} \in A$ .

Nous allons dans ce paragraphe établir l'expression explicite de  $u_{k+n}$ , à l'aide des coefficients  $a_1, \dots, a_n$ , et des valeurs initiales  $u_0, \dots, u_{n-1}$ .

Pour ce faire, considérons une infinité d'indéterminées  $(X_i)_{i \in \mathbb{N}}$  et soit  $\mathfrak{A}$  l'idéal propre de  $A[X_i]_{i \in \mathbb{N}}$  engendré par les polynômes :

$$X_{k+n} - (a_1 X_{k+n-1} + \dots + a_n X_k) \quad k \geq 0.$$

Formules explicites intervenant dans la division euclidienne ...

Désignons par  $B$  le  $A$ -module  $\frac{A[X_i]_{i \in \mathbb{N}}}{\mathfrak{a}}$  et par  $u_j$  la classe de  $X_j$  dans  $B$ . On identifiera les éléments de  $A$  et leurs classes modulo  $\mathfrak{a}$ . Dans  $A[X]$ , la division Euclidienne de  $X^{k+n}$  par  $X^n - a_1 X^{n-1} \dots - a_n$  permet d'écrire :

$$X^{k+n} = (X^n - a_1 X^{n-1} \dots - a_n) \chi(X) + \sum_{j=0}^{n-1} \alpha_{k+1, j} X^j$$

avec  $\alpha_{k+1, j} = \sum_{\substack{r_1 + 2r_2 + \dots + nr_n = k+n-j \\ r_i \in \mathbb{N} \quad i=1, 2, \dots, n}}$

$$\frac{(r_1 + \dots + r_n - 1)!}{r_1! \dots r_n!} \left( \sum_{t=0}^j r_{n-t} \right) a_1^{r_1} \dots a_n^{r_n}$$

en désignant par  $\chi(X)$  le quotient. On fait de  $B$  une algèbre sur  $A$  en posant  $u_i \cdot u_j = u_{i+j}$  pour  $0 \leq i, j \leq n-1$ . On vérifie alors aisément que  $u_i \cdot u_j = u_{i+j}$  pour  $(i, j) \in \mathbb{N} \times \mathbb{N}$ .

Soit alors  $\psi$  le morphisme d'algèbre  $A[X] \rightarrow B$ , défini par  $\psi(X^j) = u_j$  pour  $j \in \mathbb{N}$ .

On déduit, en appliquant à l'identité précédente le morphisme  $\psi$  que :  $u_{k+n} =$

$$= \sum_{j=0}^{n-1} \left( \sum_{\substack{r_1 + 2r_2 + \dots + nr_n = k+n-j \\ r_1, \dots, r_n \in \mathbb{N}}} \frac{(r_1 + \dots + r_n - 1)!}{r_1! \dots r_n!} \left( \sum_{t=0}^j r_{n-t} \right) a_1^{r_1} \dots a_n^{r_n} \right) u_j.$$

Donnons une conséquence immédiate de cette formule .

Soit maintenant  $\theta$  l'endomorphisme du  $A$  module libre  $\sum_{i=0}^{n-1} A u_i$ , défini par  $\theta(u_i) = u_{i+1}$  pour  $i \geq 0$ . La matrice

de  $\theta$  par rapport à la base  $u_0, \dots, u_{n-1}$  est :

$$M = \begin{pmatrix} 0 & 0 & & a_n \\ 1 & 0 & & \cdot \\ 0 & 1 & & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & 1 & a_1 \end{pmatrix}$$

Cette matrice a pour polynôme minimal le polynôme :

$$X^n - a_1 X^{n-1} \dots - a_n$$

Désignons par  $(u_m)$  la matrice unicolonne, dont les éléments sont les composantes de  $u_m$  sur la base  $u_0, \dots, u_{n-1}$ . On a les relations

$$\begin{aligned} M^{n+k}(u_0) &= (u_{n+k}) \\ M^{n+k}(u_1) &= (u_{n+k+1}) \\ &\dots \\ M^{n+k}(u_{n-1}) &= (u_{2n+k-1}) \end{aligned}$$

il en résulte pour  $k \geq 0$  que :

$$M^{n+k} = \begin{pmatrix} \alpha_{k+1,0} & \alpha_{k+2,0} & \dots & \alpha_{k+n,0} \\ \alpha_{k+1,1} & \alpha_{k+2,1} & \dots & \alpha_{k+n,1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k+1,n-1} & \alpha_{k+2,n-1} & \dots & \alpha_{k+n,n-1} \end{pmatrix} .$$

---

BIBLIOGRAPHIE

- [1] S. AGOU *Sur la décomposition de certains idéaux Premiers.* Publications du Département de Mathématiques - Lyon I. t. 7 fasc. 1.
- [2] S. AGOU *Polynômes sur un corps fini.* Bull. Sc. Math. 2ème série Tome 95.(1971).
- [3] N. BOURBAKI *Algèbre.* Ch. 4 et Ch. 5. A.S.I. 110 2. Hermann.
- [4] J. BRACONNIER *Bases de la théorie des Nombres.* Séminaire du Département de Mathématiques de Lyon - 1966-1967 . 1968-1969.
- [5] S. LANG *Algebra.* Addison-Wesley. Publishing Company.

- [6] P. SAMUEL      *Théorie Algébrique des Nombres.* Hermann.
- [7] O. ZARISKI  
P. SAMUEL      *Commutative Algebra.* Van Nostrand.  
Volumes 1 et 2.
- 

Manuscrit reçu le 13 septembre 1971.

S. AGOU  
Maître-assistant  
U.E.R. de Math.  
Département de Mathématiques  
43, bd du 11 novembre 1918  
69 - VILLEURBANNE