Séminaire Delange-Pisot-Poitou. Théorie des nombres

Jacques Hily

Polynômes à valeurs entières

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 4 (1962-1963), exp. n° 1, p. 1-11

<http://www.numdam.org/item?id=SDPP_1962-1963__4__A1_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
4e année, 1962/63, n° 1

29 octobre 1962

POLYNÔMES À VALEURS ENTIÈRES

par Jacques HILY

Notations. - $\mathfrak{a}$ est un anneau d'entiers algébriques sur $\underset{\sim}{\mathbb{Q}}$. Ses éléments seront notés par des lettres grecques.

Les lettres gothiques désigneront des idéaux de $\mathfrak{a}$, (α) désignera l'idéal principal engendré par l'élément α, p désignera toujours un idéal premier de $\mathfrak{a}$. Les nombres de $\underset{\sim}{\mathbb{Z}}$ seront notés en caractères latins ; p désignera un nombre premier positif de $\underset{\sim}{\mathbb{Z}}$, N désignera un nombre positif arbitraire.

A chaque p on associe un nombre r tel que p^r soit la norme de p ou le nombre d'éléments du corps $\mathfrak{a}/p$.

$\mathfrak{a}[X]$ est l'anneau des polynômes à une indéterminée sur $\mathfrak{a}$; X, Y désigneront toujours des indéterminées.

1. Etude d'un système de représentants de l'anneau $\mathfrak{a}/p^n$.

LEMME. - Soit $\alpha_1 = 0, \ldots, \alpha_{p^r}$ un système de représentants du corps $\mathfrak{a}/p$. Soit $\beta \in p$, $\beta \notin p^2$.

Alors quel que soit $\gamma \in \mathfrak{a}$, il existe une suite $\alpha_{i(j)}$ de représentants de $\mathfrak{a}/p$ telle que

$$\gamma - \sum_{j=0}^{N-1} \alpha_{i(j)} \beta^j \in p^N .$$

L'application $i(j)$ ne dépend pas de N, et est unique.

Ceci est évident si on considère la valuation définie sur $\mathfrak{a}$ par p ; $\sum_{j=0}^{\infty} \alpha_{i(j)} \beta^j$ étant le développement de Hensel de γ, développement convergent au sens de cette valuation. De plus on sait que ce développement est unique.

En particulier, on vérifie facilement que toute relation de la forme $\gamma \in p^n$ peut toujours être écrite

$$\gamma \equiv \zeta \beta^n \bmod p^{n+N}$$

avec $N > 0$, et où ζ est défini par une suite $\sum_{j=0}^{N-1} \alpha_{i(j)} \beta^j$.

Remarque. - Si p est principal, on peut alors prendre pour β un générateur de l'idéal, et la relation $\gamma \in p^n$ s'écrit alors $\gamma = \beta^n \zeta$ avec $\zeta \in \mathfrak{a}$.

LEMME. - Si on a

$$\begin{cases} \gamma_1 - \zeta_1 \beta^{n_1} \in p^{n_1+N} \\ \gamma_2 - \zeta_2 \beta^{n_2} \in p^{n_2+N} \end{cases}$$

On a alors : $\gamma_1 \gamma_2 - \zeta_1 \zeta_2 \beta^{n_1+n_2} \in p^{n_1+n_2+N}$.

Il suffit de poser

$$\begin{cases} \gamma_1 - \zeta_1 \beta^{n_1} = \lambda_1 & \lambda_1 \in p^{n_1+N} \\ \gamma_2 - \zeta_2 \beta^{n_2} = \lambda_2 & \lambda_2 \in p^{n_2+N} \end{cases}$$

en identifiant ζ_1 et ζ_2 aux éléments de $\mathfrak{a}$ qui sont respectivement

$$\sum_{j=0}^{N-1} \alpha_{i_1(j)} \beta^j \quad \text{et} \quad \sum_{j=0}^{N-1} \alpha_{i_2(j)} \beta^j ,$$

on a

$$\gamma_1 \gamma_2 = \zeta_1 \zeta_2 \beta^{n_1+n_2} + \zeta_1 \lambda_2 \beta^{n_1} + \zeta_2 \lambda_1 \beta^{n_2} + \lambda_1 \lambda_2 .$$

D'où le résultat, puisque $\lambda_2 \beta^{n_1} \in p^{n_1+n_2+N}$ et $\lambda_1 \beta^{n_2} \in p^{n_1+n_2+N}$.

2. Etude des fonctions polynomiales telles que $P(\mathfrak{a}) \subset p^n$.

A tout polynôme $P(X) \in \mathfrak{a}[X]$ on associe la fonction de $\mathfrak{a}$ dans $\mathfrak{a}$ telle que $\xi \to P(\xi)$.

Deux fonctions polynomiales $P_1(\xi)$ et $P_2(\xi)$ seront dites congrues modulo p^n si, quel que soit $\xi \in \mathfrak{a}$, on a $P_1(\xi) - P_2(\xi) \in p^n$.

Nous cherchons les fonctions polynomiales congrues à 0 modulo p^n .

1° $\underline{n = 1}$. - On sait alors que ces fonctions sont fournies par les polynômes

$$P(X) = (X^{p^r} - X)\, P_1(X) + P_2(X)$$

avec $P_1(X) \in \mathfrak{A}[X]$ et $P_2(X) \in p\mathfrak{A}[X]$.

En particulier si : degré $P(X) < p^r$, alors $P(X) \in p\mathfrak{A}[X]$ c'est-à-dire que les coefficients de $P(X)$ sont congrus à 0 modulo p .

2° $\underline{n \geqslant 2}$. - Considérons la suite des polynômes

$$\begin{cases} Q_1(X) = X^{p^r} - X \\ Q_{\ell+1}(X) = Q_\ell^{p^r}(X) - \beta^{p^{r\ell}-1}\, Q_\ell(X) . \end{cases}$$

LEMME I. - Posons $m(\ell) = \sum_{i=0}^{\ell-1} p^{ri}$. On a

$$Q_\ell(\xi) \in p^{m(\ell)} .$$

Ceci est vrai pour $\ell = 1$. Démontrons ceci par récurrence sur ℓ .

On a

$$Q_\ell(\xi) \equiv \beta^{m(\ell)}\, \zeta_\ell \bmod p^{m(\ell)+N} .$$

Soit

$$Q_\ell^{p^r}(\xi) \equiv \beta^{m(\ell+1)-1}\, \zeta_\ell^{p^r} \bmod p^{m(\ell+1)-1+N} .$$

Et

$$\beta^{p^{r\ell}-1}\, Q_\ell(\xi) \equiv \beta^{m(\ell+1)-1}\, \zeta_\ell \bmod p^{m(\ell+1)-1+N} .$$

Soit par différence

$$Q_{\ell+1}(\xi) \equiv \beta^{m(\ell+1)-1}(\zeta^{p^r} - \zeta_\ell) \bmod p^{m(\ell+1)-1+N} .$$

En identifiant ζ_ℓ à un élément de $\mathcal{A}$ on a :

$$\zeta_\ell^{p^r} - \zeta_\ell \in \mathfrak{p} \ ,$$

ce qui peut s'écrire

$$\zeta_\ell^{p^r} - \zeta_\ell \equiv \beta\zeta_{\ell+1} \bmod \mathfrak{p}^N \ .$$

Soit en reportant

$$Q_{\ell+1}(\xi) \equiv \beta^{m(\ell+1)}\ \zeta_{\ell+1} \bmod \mathfrak{p}^{m(\ell+1)+N-1} \ ,$$

ce qui vérifie l'hypothèse de récurrence.

De plus si $N > 2$ on voit qu'on fait apparaître une suite $\zeta_0 = \xi \ , \ \dots \ , \ \zeta_\ell$ définie par la relation $\beta\zeta_{\ell+1} \equiv \zeta_\ell^{p^r} - \zeta_\ell \bmod \mathfrak{p}^N$. Cette suite dépend évidemment de ξ .

LEMME II. - Pour $m \geq \ell$, on a

$$\zeta_\ell(\xi + \beta^m \zeta_0) \equiv \zeta_\ell(\xi) + (-1)^\ell \beta^{m-\ell}\ \xi_0 \bmod \mathfrak{p}^{m-\ell+1} \ .$$

Ceci est vrai pour $\ell = 0$.

On le vérifie par récurrence sur ℓ ; on a alors $m > \ell$.

$$\beta\zeta_{\ell+1}(\xi + \beta^m \xi_0) \equiv [\zeta_\ell(\xi) + (-1)^\ell\ \beta^{m-\ell}\ \xi_0]^{p^r} - [\zeta_\ell(\xi) + (-1)^\ell \beta^{m-\ell}\ \xi_0] \bmod \mathfrak{p}^{m-\ell+1} \ .$$

Développons le premier crochet par la formule du binôme. Cela donne

$$\zeta_\ell^{p^r}(\xi) + (-1)^\ell\ \beta^{m-\ell}\ \xi_0 \Big[\sum_{q=1}^{p^r} C^q_{p^r}\ \zeta_\ell^{p^r-q}(\xi) \times (-1)^{\ell q}\ \beta^{(m-\ell)(q-1)}\ \xi_0^{q-1} \Big] \ .$$

Or $\mathfrak{p} \mid C^q_{p^r}$ pour $q \neq 0$ et $q \neq p^r$.

De plus $\mathfrak{p}$, en tant qu'élément de $\mathcal{A}$, est un élément de l'idéal $\mathfrak{p}$. Les éléments du crochet correspondant à $q \neq p^r$ sont donc des éléments de $\mathfrak{p}$. Si $q = p^r$

on a un monôme qui contient $\beta^{(m-\ell)(p^r-1)}$ qui est nul modulo p puisque nous avions $m > \ell$ et $p^r > 1$.

Soit $[\zeta_\ell(\xi) + (-1)^\ell \beta^{m-\ell} \xi_0]^{p^r} \equiv \zeta_\ell^{p^r}(\xi) \bmod p^{m-\ell+1}$.

En prenant dans la relation du lemme I, $N = m - \ell + 1$, on a

$$\beta\zeta_{\ell+1}(\xi) \equiv \zeta_\ell^{p^r}(\xi) - \zeta_\ell(\xi) \bmod p^{m-\ell+1} ,$$

Soit en reportant et en simplifiant par β ,

$$\zeta_{\ell+1}(\xi + \beta^m \xi_0) \equiv \zeta_{\ell+1}(\xi) + (-1)^{\ell+1} \beta^{m-\ell-1} \bmod p^{m-\ell} ,$$

ce qui vérifie l'hypothèse de récurrence.

De plus on voit que si pour un certain ξ on avait trouvé une valeur ℓ_1 pour laquelle $\zeta_{\ell_1} \equiv 0 \bmod p$ en formant $Q_{\ell_1}(\xi + \beta^{\ell_1} \xi_0)$ on obtiendrait

$$\zeta_{\ell_1}(\xi + \beta^{\ell_1} \xi_0) \equiv (-1)^{\ell_1} \xi_0 \bmod p ,$$

c'est-à-dire un ξ pour lequel $Q_{\ell_1}(\xi)$ n'est pas nul modulo une puissance de p supérieure à celle indiquée au lemme I.

LEMME III. - Si $P(\xi) \equiv 0 \bmod p^n$ pour tout ξ , on a

$$P(X) = \sum_{j=0}^{N} \gamma_j Q_\ell^{k_\ell}(X) \dots Q_1^{k_1}(X) X^{k_0} ,$$

avec

$$\begin{cases} j = k_\ell p^{r\ell} + \dots + k_1 p^r + k_0 & p^{r\ell} \leqslant j < p^{r(\ell+1)} \\ 0 \leqslant k_i < p^r \end{cases}$$

et $\gamma_j \equiv 0 \bmod p^{q(j)}$ où $q(j) = \max(0 , n - \sum_{i=1}^{\infty} [\frac{j}{p^{ri}}])$, $[\frac{j}{p^{ri}}]$ est la valeur entière de $\frac{j}{p^{ri}}$.

a. Les polynômes de la forme $Q_\ell^{k_\ell}(X) \dots Q_1^{k_1}(X) X^{k_0}$ forment une base de $\mathfrak{A}[X]$ car ils sont unitaires et que, quel que soit j , il est toujours possible de

trouver un ℓ et une suite unique d'entiers tels que :

$$j = k_\ell \, p^{r\ell} + \ldots + k_1 \, p^r + k_0 \, .$$

b. Par application du lemme II, on a

$$Q_\ell^{k_\ell}(\xi) \ldots Q_1^{k_1}(\xi) \, \xi^{k_0} \equiv 0 \bmod p^{n(j)} \, .$$

où $n(j) = \sum_{m=1}^{\ell} k_m \sum_{i=0}^{m-1} p^{ri}$.

Soit encore $n(j) = \sum_{i=1}^{\ell} \sum_{m=i}^{\ell} k_m \, p^{r(m-i)} = \sum_{i=1}^{\ell} [\frac{j}{p^{ri}}]$.

Comme pour $i > \ell$, on a $\frac{j}{p^{ri}} < 1$, soit $[\frac{j}{p^{ri}}] = 0$, on peut remplacer la dernière somme par

$$\sum_{i=1}^{\infty} [\frac{j}{p^{ri}}] \, .$$

De plus on voit que les seules fonctions polynomiales de la forme $Q_\ell^{k_\ell}(\xi) \ldots Q_1^{k_1}(\xi) \, \xi^k$ qui ne sont pas nulles modulo p sont celles qui correspondent aux $j < p^r$.

Donc si $n = 1$, l'énoncé du lemme III affirme que $\gamma_j \equiv 0 \bmod p$ pour $j < p^r$ ce qui coïncide avec la condition trouvée dans l'étude du cas $n = 1$.

c. On va faire une récurrence sur n .

P(X) satisfait aux conditions du lemme III, et est tel que $P(\xi) \in p^{n+1}$.

$$Q_\ell^{k_\ell}(\xi) \ldots Q_1^{k_1}(\xi) \, \xi^{k_0} \equiv \beta^{n(j)} \, \zeta_\ell^{k_\ell} \ldots \zeta_1^{k_1} \, \zeta_0^{k_0} \bmod p^{1+n(j)} \, .$$

Les termes tels que $n(j) \geqslant n + 1$ seront donc nuls modulo p^{n+1} quel que soit ξ . Il suffit donc de considérer ceux pour lesquels $n(j) \leqslant n$.

Pour ces termes l'hypothèse de récurrence donne

$$\gamma_j \equiv 0 \bmod p^{n-n(j)} \, .$$

Soit $\gamma_j \equiv \beta^{n-n(j)} \, \gamma_j' \bmod p^{n-n(j)+1}$.

Soit $P(\xi) \equiv \beta^n \sum_{j=0}^{N'} \gamma_j' \zeta_\ell^{k_\ell} \cdots \zeta_1^{k_1} \zeta_0^{k_0} \bmod p^{1+n}$, où N' est le plus grand entier tel que $\sum_{i=1}^{\infty} [\frac{N'}{p^{ri}}] \leqslant n$.

D'où, en tenant compte de l'hypothèse $P(\xi) \in p^{n+1}$,

$$\sum_{j=0}^{N'} \gamma_j' \zeta_\ell^{k_\ell} \cdots \zeta_1^{k_1} \zeta_0^{k_0} \equiv 0 \bmod p \ .$$

Soit ℓ_1 la plus grande valeur de l'indice ℓ intervenant dans cette fonction polynomiale, et formons $P(\xi + \beta^{\ell_1} \xi_0)$.

On a alors en appliquant le lemme II

$$\zeta_0(\xi + \beta^{\ell_1} \xi_0) \equiv \zeta_0(\xi) \bmod p \ ,$$

$$\zeta_{\ell_1-1}(\xi + \beta^{\ell_1} \xi_0) \equiv \zeta_{\ell_1-1}(\xi) \bmod p \ ,$$

$$\zeta_{\ell_1}(\xi + \beta^{\ell_1} \xi_0) \equiv \zeta_{\ell_1}(\xi) + (-1)^{\ell_1} \xi_0 \bmod p \ .$$

Il est donc possible de laisser fixes, modulo p , ζ_0 , ••• , ζ_{ℓ_1-1} , et de ne faire varier modulo p que ζ_{ℓ_1} .

La fonction polynomiale $\sum_{j=0}^{N'} \gamma_j' \zeta_\ell^{k_\ell} \cdots \zeta_1^{k_1} \zeta_0^{k_0}$ considérée comme fonction de la seule variable ζ_{ℓ_1} a un degré inférieur à p^r c'est-à-dire que ses coefficients sont nuls modulo p .

Or ceux-ci sont des polynômes ne faisant intervenir que ζ_{ℓ_1-1} , ••• , ζ_1 , ζ_0 avec des puissances inférieures à p^r .

Par réductions successives on obtient finalement $\gamma_j' \equiv 0 \bmod p$. Soit $\gamma_j \equiv 0 \bmod p^{n+1-n(j)}$ ce qui vérifie l'hypothèse de récurrence.

COROLLAIRES.

a. Si on impose que $P(X)$ ait 1 pour coefficient du terme de plus haut degré, et que $P(\xi) \in p^n$, alors le degré N de $P(X)$ est tel que

$$n(N) = \sum_{i=1}^{\infty} [\frac{N}{p^{ri}}] \geqslant n .$$

b. Soit N un entier.

$$N = \sum_{j=0}^{\ell_1} k_j \, p^{rj} ,$$

avec $0 \leqslant k_j < p^r$.

Considérons un système d'entiers non nécessairement distincts $\alpha_1 , \ldots , \alpha_N$ tel que ce système soit la réunion de k_{ℓ_1} systèmes de résidus de $\mathcal{A}/p^{\ell_1}$, ... , k_1 systèmes de résidus de $\mathcal{A}/p$ et k_0 entiers arbitraires.

Un tel système sera appelé un $S_{N_1,p}$.

Le système des nombres $\{\xi + \alpha_i\}_{i=1,\ldots,N}$ est encore un $S_{N,p}$. Or dans un $S_{N,p}$ il y a nécessairement $k_{\ell_1} p^{r(\ell_1-1)} + \ldots + k_1$ nombres congrus à 0 mod p soit $[\frac{N}{p^r}]$.

Parmi ces $[\frac{N}{p^r}]$ nombres, $k_{\ell_1} p^{r(\ell_1-2)} + \ldots + k_2$ sont congrus à 0 mod p^2 soit $[\frac{N}{p^{2r}}]$ etc.

Finalement on trouve

$$\prod_{i=1}^{N} (\xi + \alpha_i) \in p^{n(N)} .$$

Ceci nous fournit donc un autre procédé pour fabriquer des fonctions polynomiales nulles modulo p^n.

c. Si on multiplie tous les nombres d'un $S_{N,p}$ par un même nombre λ ($\lambda \not\equiv p$), on a encore un $S_{N,p}$.

Soient deux systèmes $S_{N,p_1} = \{\alpha_i^{(1)}\}$ et $S_{N,p_2} = \{\alpha_i^{(2)}\}$ et soient deux nombres λ_1 et λ_2 tels que

$$\lambda_1 \in p_2^N \qquad \lambda_1 \notin p_1 ,$$

$$\lambda_2 \in p_1^N \qquad \lambda_2 \notin p_2 .$$

Alors il est évident que le système $\{\lambda_1 \alpha_i^{(1)} + \lambda_2 \alpha_i^{(2)}\}_{i=1,\dots,N}$ est à la fois un S_{N,p_1} et un S_{N,p_2} .

On peut donc construire en itérant le procédé un système qui soit un $S_{N,p}$ pour tout p soit $\{\gamma_i\}_{i=1,\dots,N}$.

La fonction polynomiale

$$P_N(\xi) = \prod_{i=1}^{N} (\xi + \gamma_i) \quad \text{est alors nulle modulo} \quad \mathfrak{G}(N) = \prod_p p^{n(N)} ,$$

le produit étant convergent, car seuls interviennent avec une puissance non nulle les idéaux premiers, tels que $p^r < N$, qui sont en nombre fini. Les polynômes $P_N(X)$ auxquels on adjoint le polynôme $P_0(X) = 1$ forment alors une base de $\mathfrak{a}[X]$ puisqu'ils ont 1 pour coefficient du terme de plus haut degré et pour degré N .

Donc tout polynôme $P(X) \in \mathfrak{a}[X]$ s'écrit

$$P(X) = \sum_{n=0}^{\infty} \alpha_n P_n(X) ,$$

où seul un nombre fini de α_n sont non nuls.

$P(\xi)$ sera alors divisible par le plus grand commun diviseur des idéaux

$$\{\alpha_n \mathfrak{G}(n)\}_{\alpha_n \neq 0} ,$$

et $P(\xi)$ ne sera divisible, pour tout ξ , par aucun idéal plus petit, car sinon il serait possible de trouver un n et un polynôme P_n de coefficient du terme de degré n unité tel que $P_n(\xi)$ soit nul modulo un idéal plus petit que $\mathfrak{G}(n)$ ce qui contredirait le corollaire (a).

On en déduit que si une fonction polynomiale à coefficients dans le corps des quotients de $\mathfrak{A}$ est telle que l'image de $\mathfrak{A}$ soit dans $\mathfrak{A}$, elle est de la forme

$$\sum_{n=0}^{\infty} \frac{\alpha_n}{\beta_n} P_n(X)$$

où $\alpha_n \in \mathfrak{A}$, $\beta_n \in \mathfrak{A}$ $(\beta_n \neq 0)$ et où l'idéal (β_n) divise l'idéal $(\alpha_n)\ \mathfrak{G}(n)$.

En particulier si $\mathfrak{A}$ est un anneau à idéaux principaux, toutes les fonctions polynomiales à coefficients dans le corps de quotients de $\mathfrak{A}$, et prenant des valeurs entières pour les valeurs entières de la variable, sont de la forme

$$\sum_{n=0}^{\infty} a_n P_n(X)$$

où $\mathfrak{G}(n)$ désigne l'un des générateurs de l'idéal $\mathfrak{G}(n)$.

Applications.

1° Si $\mathfrak{A} = \mathbb{Z}$, on vérifie facilement que tout système de n nombres consécutifs est un S_n.

Dans ce cas, on a toujours $r = 1$ et $\mathfrak{G}(n) = (n!)$.

On retrouve le résultat classique [3] qui est que toute fonction polynomiale prenant des valeurs entières pour les valeurs entières de la variable est de la forme

$$P(X) = \sum_{n=0}^{\infty} \alpha_n P_n(X)$$

avec $P_0(X) = 1$ et $P_n(X) = \dfrac{X(X+1) \ldots (X+n-1)}{n!}$.

2° $\mathfrak{A}$ est anneau des entiers de Gauss.

Considérons les fonctions polynomiales de deux variables X et Y prenant des valeurs entières de Gauss si les variables sont des entiers naturels. D'après le résultat précédent, elles sont de la forme

$$P(X, Y) = \sum\!\!\!\!\!\!- \lambda_{m,n} P_m(X).P_n(Y)$$

où $P_n(X)$ est le polynôme de l'application précédente. $P(X, Y)$ sera un polynôme

de la variable $Z = X + iY$ si l'on a

$$\frac{\partial P}{\partial X} = i \frac{\partial P}{\partial Y} .$$

Soit, en appliquant la formule $\frac{d}{dX} P_m(X) = \sum_{k=0}^{m-1} \frac{P_k(X)}{m-k}$, on trouve le système

$$\sum_{N \geq k > m+n} \frac{\lambda_{k-m,n} + i\lambda_{m,k-n}}{k-m-n} = 0 .$$

Ce système n'admettra de solutions, avec $\lambda_{m,n}$ entier, que si le coefficient du terme de plus haut degré est un multiple entier de $\frac{1}{\mathfrak{G}(n)}$ puisque cet anneau est à idéaux principaux.

Soit

$$\lambda_{n,0} = \lambda(1+i)^{n(N)} \prod_{p \equiv 3 \pmod 4} p^{n_1(N)}$$

avec $n_1(N) = \sum_{j=0}^{\infty} [\frac{N}{p^{1+2j}}]$ et $n(N) = \sum_{j=1}^{\infty} [\frac{N}{2^j}]$, ce qui est une condition nécessaire.

BIBLIOGRAPHIE

[1] DICKSON (L. E.). - Introduction to the theory of numbers, 2nd printing. - New York, Dover Publications, 1957.

[2] HILBERT (David). - Théorie des corps de nombres algébriques. - Paris, A. Hermann, 1913.

[3] KEMPNER (Aubrey J.). - Polynomials and their residue systems, Trans. Amer. math. Soc., t. 22, 1921, p. 240-288.