Can. J. Math., Vol. XXIV, No. 5, 1972, pp. 747–754

POLYNOMES A VALEURS ENTIERES

PAUL-JEAN CAHEN

Introduction. Soit A un anneau intègre de corps des fractions K, on s'interesse ici aux polynômes de $K[X]$ qui prennent sur A leurs valeurs dans A. Ils forment bien évidemment un sous anneau de $K[X]$ qui contient $A[X]$, nous le notons A_S.

Cet article reprend, dans un langage moderne, les idées de deux publications assez anciennes, dues à Polya [3] et Ostrowsky [4], en 1919. Les auteurs montraient que si A est principal, A_S est un A-module libre qui admet sur A une base formée de polynômes de degré croissant; si A est plus généralement l'anneau des entiers d'un corps de nombres ils mettaient en évidence une suite d'idéaux fractionnaires de A. En exposant le cas de l'anneau A principal, pour un anneau de valisation discrète dans le premier paragraphe, puis en généralisant aux anneaux de Dedekind dans notre second paragraphe, nous pouvons énoncer de façon plus explicite, que A_S est un A-module projectif, que l'on peut décomposer canoniquement en somme d'idéaux fractionnaires de A.

1. Anneaux de valuation discrète. L'anneau de Dedekind le plus simple est un anneau de valuation discrète: On note A un tel anneau, v la valuation (de son corps des fractions K) qui lui est associée; on suppose v normalisée et on note π une uniformisante. Si $\mathfrak{m}$ désigne l'idéal maximal de A, on définit la norme de $\mathfrak{m}$, notée N, comme étant le cardinal du corps résiduel $A/\mathfrak{m}$.

Soit $(a_0, a_1, \ldots, a_{N-1})$ un système de représentants de A modulo $\mathfrak{m}$, où $a_0 = 0$. Si N est infini, la suite est infinie; sinon on la prolonge de la façon suivante (d'après Polya [4]): Ecrivant un entier n sous la forme

$$n = i_0 + i_1 N + \ldots + i_h N^h$$

où i_j est un entier tel que $0 \leqq i_j \leqq N - 1$ pour tout j dans $\{0, \ldots, h\}$. On pose

$$a_n = a_{i_0} + a_{i_1}\pi + \ldots + a_{i_h}\pi^h.$$

On peut alors faire deux remarques:

Remarque 1. $(a_0, a_1, \ldots, a_{N^h-1})$ est un système de représentants modulo $\mathfrak{m}^h$.

Remarque 2. $v(a_n - a_{n'})$ est la plus grande puissance de N qui divise $n - n'$. On note $v_N(x)$ la plus grande puissance de N qui divise un entier x (en prenant garde qu'il ne s'agit pas d'une valuation si N n'est pas premier). On écrit alors:

$$v(a_n - a_{n'}) = v_N(n - n').$$

Reçu le 10 mars, 1971 et in revu forme, le 19 janvier, 1972.

Que N soit fini ou infini, on peut alors définir une suite infinie de polynômes:

$$f_0 = 1, f_1 = X - a_0, \ldots, f_n = (X - a_0) \ldots (X - a_{n-1}), \ldots .$$

Si on désigne par $f_n(A)$ l'idéal engendré par les valeurs $f_n(\xi)$ de f_n sur les élements ξ de A, $f_n(A)$ est une puissance de l'idéal maximal puisque A est l'anneau d'une valuation discrète; notant $S(n)$ cette puissance on définit ainsi une fonction de l'entier n (à valeurs entières). Avec ces notations nous reformulons un lemme du à Polya:

LEMME (Polya). *$S(n)$ ne depend pas de l'anneau A autrement que par la norme N de $\mathfrak{m}$ et c'est une fonction croissante de n. On a en effet la formule*

$$S(n) = \sum_{h=1}^{n} v_N(h) = \sum_{\alpha=1}^{\infty} \left[\frac{n}{N^n}\right]$$

où $\left[\frac{n}{N^\alpha}\right]$ désigne la partie entière de $\frac{n}{N^\alpha}$. $f_n(a_n)$ engendre $f_n(A)$ autrement dit:

$$v[f_n(a_n)] = S(n).$$

Si N est infini on donne un sens raisonnable aux formules du lemme en posant $S(n) = 0$. Par ailleurs, il est clair que $f_n(a_n)$ est inversible; donc $v[f_n(a_n)] = 0 = S(n)$ pour tout n.

Si N est fini, il nous suffit de montrer que

$$v[f_n(\xi)] \geqq v[f_n(a_n)] = S(n).$$

Quand ξ parcourt A, et de vérifier les formules pour

$$S(n) = v[f_n(a_n)].$$

Si $f_n(\xi) = 0$, $v[f_n(\xi)]$ est infini; donc on peut supposer que $f_n(\xi)$ n'est pas nul et que $v[f_n(\xi)]$ est un entier w; comme $(a_0, a_1, \ldots a_{N^{w+1}-1})$ forme un système de représentants modulo $\mathfrak{m}^{w+1}$ on trouve a_μ tel que

$$v[\xi - a_\mu] \geqq w + 1,$$

et donc tel que

$$v[f_n(a_\mu)] = v[f_n(\xi)] = w.$$

Notons que $f_n(a_\mu)$ n'est pas nul; donc que l'on a $\mu \geqq n$. Par ailleurs,

$$\begin{aligned} w &= v[f_n(a_\mu)] \\ &= v[(a_\mu - a_0) \ldots (a_\mu - a_{n-1})] \\ &= \sum_{h=0}^{n-1} v(a_\mu - a_h) \\ &= \sum_{h=0}^{n-1} v_N(\mu - h) \end{aligned}$$

(d'après la Remarque 1). Mais alors

$$w = \sum_{h=0}^{\mu} v_N(h) - \sum_{h=0}^{\mu-n} v_N(h).$$

https://doi.org/10.4153/CJM-1972-071-2 Published online by Cambridge University Press

Nous laissons au lecteur la vérification purement arithmétique de l'égalité pour tout entier μ

$$(*) \qquad \sum_{h=0}^{\mu} v_N(h) = \sum_{\alpha=1}^{\infty} \left[\frac{\mu}{N^\alpha}\right].$$

On a donc

$$\begin{aligned} v[f_n(\xi)] &= w \\ &= \sum_{\alpha=1}^{\infty} \left[\frac{\mu}{N^\alpha}\right] - \sum_{\alpha=1}^{\infty} \left[\frac{\mu - n}{N^\alpha}\right] \\ &= \sum_{\alpha=1}^{\infty} \left(\left[\frac{\mu}{N^\alpha}\right] - \left[\frac{\mu - n}{N^\alpha}\right]\right) \\ &\geqq \sum_{\alpha=1}^{\infty} \left[\frac{n}{N^\alpha}\right]. \end{aligned}$$

Les formules pour $v[f_n(a_n)]$ se déduisent de ce calcul et de l'égalité (*) en remplaçant partout μ par n.

Comme les polynômes $f_0, f_1, \ldots, f_n, \ldots$ sont de degrés croissants ils forment une base du K-espace vectoriel $K[X]$; ainsi tout polynôme P de $K[X]$ de degré n peut s'écrire de façon unique.

$$P = \lambda_0 f_0 + \lambda_1 f_1 + \ldots + \lambda_n f_n \quad (\lambda_i \in K, i \in \{0, \ldots, n\}).$$

PROPOSITION 1. *Avec les notations précédentes, un polynôme P (de degré n) est dans A_S si et seulement si*

$$v(\lambda_i) \geqq -S(i) \quad (i \in \{0, \ldots, n\}).$$

Si on note I_n l'idéal fractionnaire

$$\mathfrak{m}^{-S(n)} = [f_n(A)]^{-1}$$

on a donc décomposé A_S en somme directe des idéaux $I_0, I_1, \ldots, I_n, \ldots$ selon les polynômes $f_0, f_1, \ldots, f_n, \ldots$.

Si d'abord $v(\lambda_i) \geqq -S(i)$, alors pour tout ξ dans A, $v[\lambda_i f_i(\xi)] \geqq 0$; donc $\lambda_i f_i$ est dans A_S, de même la somme $\lambda_0 f_0 + \ldots + \lambda_n f_n$ avec ces hypothèses.

Inversement, si P est dans A_S, alors $P(a_0)$ est dans A; mais alors λ_0 est dans A (car $f_i(a_0) = 0$ si $i > 0$) et $v[\lambda_0] \geqq -S(0) = 0$. Si par récurrence, les inégalités sont vérifiées pour $\lambda_0, \lambda_1 \ldots \lambda_{j-1}$, alors

$$Q_j = P - \lambda_0 f_0 - \lambda_1 f_1 \ldots - \lambda_{j-1} f_{j-1}$$

est dans A_S (d'après la première partie de cette preuve) et ainsi

$$Q_j(a_j) = \lambda_j f_j(a_j)$$

est dans A; soit

$$v(\lambda_j) \geqq -v[f_j(a_j)] = -S(j).$$

Comme les idéaux I_n sont tous principaux, A_S est un A-module libre; les polynômes $\pi^{-S(n)} f_n$ forment une base de A_S. Si N est infini, les idéaux I_n sont tous égaux à A et A_S est égal a $A[X]$.

2. Anneaux de Dedekind. Soit A un anneau de Dedekind de corps des fractions K. On note v la valuation correspondant à un idéal maximal $\mathfrak{m}_v$ de A, A_v l'anneau de valuation discrète associé (A_v est le localisé $A_{\mathfrak{m}_v}$), N_v la norme de $\mathfrak{m}_v$, et $S_v(n)$ la fonction de n (définie au § 1) sur l'anneau A_v.

Si I est un idéal fractionnaire de A, on désigne par $v(I)$ la puissance de $\mathfrak{m}_v$ dans la décomposition de I en produits d'idéaux maximaux.

PROPOSITION 2. *Soit P un polynôme de $K[X]$ de degré n. On note $v(P)$ la plus petite des valuations des coéfficients de P et $P(A)$ le sous-A module de K engendré par les valeurs de P sur A.*

Alors $P(A)$ est un idéal fractionnaire et on a l'inégalité, pour toute valuation v,

$$v(P) \leqq v[P(A)] \leqq S_v(n) + v(P).$$

Si d est le produit des dénominateurs des coefficients de P, dP est dans $A[X]$; donc $dP(A) \subset A$ et ainsi $P(A)$ est un idéal fractionnaire. D'ailleurs, il est clair que $v(P) \leqq v[P(A)]$. Enfin, si on choisit une uniformisante π_v de v,

$$Q = \pi_v^{-v[P(A)]}P$$

est tel que $Q(A) \subset A_{\mathfrak{m}_v}$. Dans un article précédent [**2**] on a montré qu'alors $Q(A_{\mathfrak{m}_v}) \subset A_{\mathfrak{m}_v}$; donc $Q \in (A_{\mathfrak{m}_v})_S$ et ainsi on a

$$\pi_v^{-v[P(A)]}P = \lambda_0 f_{0,v} + \lambda_1 f_{1,v} + \ldots + \lambda_n f_{n,v}$$

où les polynômes $f_{i,v}$ sont construits pour A_v comme dans le paragraphe précédent (en particulier, $f_{i,v}$ est dans $A_v[X]$), et on a aussi

$$v(\lambda_i) \geqq -S_v(i) \geqq -S_v(n).$$

En définitive,

$$P = \sum_{i=0}^{n} \pi_v^{v[P(A)]}\lambda_i f_{i,v};$$

donc

$$v(P) \geqq v[P(A)] - S_v(n).$$

En analogie avec le paragraphe précédent on cherchera une suite de polynômes $f_0, f_1, \ldots, f_n, \ldots$ de degré croissant de telle sorte que tout polynôme P de $K[X]$ peut s'écrire de façon unique

$$P = \lambda_0 f_0 + \lambda_1 f_1 + \ldots + \lambda_n f_n \quad (\lambda_i \in K,\ i \in \{0, \ldots, n\}),$$

et on posera:

Définition. A_S est décomposé en somme d'idéaux fractionnaires $I_0, I_1, \ldots, I_n, \ldots$ selon des polynômes $f_0, f_1, \ldots, f_n, \ldots$ s'il est équivalent d'avoir:

(i) $P \in A_S$; ou

(ii) $\lambda_j \in I_j$ ($j \in \{0, \ldots, n\}$).

Notons tout de suite que les polynômes $f_0, f_1, \ldots, f_n, \ldots$ avec cette definition ne sont pas nécessairement dans A_S. Montrons néanmoins d'abord qu'il éxiste une telle décomposition avec des polynômes unitaires de $A[X]$.

LEMME. *Dans un anneau de Dedekind A, pour tout entier n il n'y a qu'un nombre fini de valuations v telles que $N_v \leqq n$.*

Ou bien A est un corps fini, mais on écarte ce genre de trivialité dans notre problème, ou bien il éxiste x non nul dans A tel que $x^{n-1} - 1$ n'est pas nul, mais x ou x^{n-1} est dans tout idéal m_v tel que $N_v = n$, ces idéaux sont donc en nombre fini.

On peut donc définir une suite d'idéaux fractionnaires par la condition: $v(I_n) = -S_v(n)$ pour toute valuation v de K; on est en effet assuré que $S_v(n)$ est nul pour presque tout v.

On utilise le théorème d'approximation pour définir la suite de polynômes $f_0, f_1, \ldots, f_n, \ldots$: Si, en effet, $a_{0,v}, a_{1,v}, \ldots, a_{n,v}, \ldots$ est la suite d'éléments, que l'on construit au § 1, relative à l'anneau de valuation A_v, telle que l'on a la suite de polynômes de $(A_v)_S$:

$$f_{0,v} = 1, f_{1,v} = (X - a_{0,v}), \ldots, f_{n,v} = (X - a_{0,v})(X - a_{1,v}) \ldots (X - a_{n-1,v}).$$

On sait trouver dans A des élements $\beta_{i,n}$ tels que

$$v[\beta_{i,n} - a_{i,v}] > S_v(n) (i \in \{0, \ldots, n\})$$

pour les valuations v (en nombre fini) telles que

$$S_v(n) \neq 0.$$

Si on pose

$$f_0 = 1, \ldots, f_n = (X - \beta_{0,n}) \ldots (X - \beta_{n-1,n})$$

on a

$$v[f_{n,v} - f_n] > S_v(n)$$

et

$$v[f_n(A)] = v[f_n(\beta_{n,n})] = v[f_{n,v}(a_{n,v})] = S_v(n).$$

Pour les valuations v où $S_v(n)$ n'est pas nul, mais d'aprés la Proposition 2, si $S_v(n)$ est nul

$$0 = v[f_n] \leqq v[f_n(A)] \leqq v(f_n) + S_v(n) = v(f_n) = 0$$

(puisque f_n est unitaire dans $A[X]$). Donc encore

$$v[f_n(A)] = S_v(n).$$

En conclusion

$$f_n(A) = I_n^{-1}$$

THÉORÈME 1. *Avec les notations précédentes, A_S est décomposé en somme d'idéaux fractionnaires $I_0, I_1, \ldots, I_n, \ldots$ selon les polynômes $f_0, f_1, \ldots, f_n, \ldots$.*

On va montrer ce théorème en même temps que le suivant qui établit à quelle condition une suite de polynômes permet la décomposition de A_S en sommes d'idéaux:

THÉORÈME 2. *Soit $P_0, P_1, \ldots, P_n, \ldots$ une suite de polynômes de $K[X]$, telle que P_n est de degré n. On note x_n le coefficient directeur de P_n; alors les conditions suivantes sont équivalentes:*

https://doi.org/10.4153/CJM-1972-071-2 Published online by Cambridge University Press

(i) *Pour toute valuation v, et tout entier n, on a*:

$$v[P_n(A)] = v(x_n) + S_v(n).$$

(ii) A_S *se décompose en une somme d'idéaux* $J_0, J_1, \ldots, J_n, \ldots$ *sur les polynômes* $P_0, P_1, \ldots, P_n, \ldots$. *De plus on a alors les égalités*:

$$v(x_n) = v(P_n)$$

(*en particulier si* P_n *est unitaire il est dans* $A[X]$);

$$J_n = x_n^{-1} I_n$$

(*en particulier, si* P_n *est unitaire* $J_n = I_n$).

Il est d'abord clair que (i) entraine l'égalité $v(x_n) = v(P_n)$ puisque d'une part, on a $v(x_n) \geqq v(P_n)$ par définition de $v(P_n)$ et d'autre part

$$v[P_n(A)] = v(x_n) + S_v(n) \leqq v(P_n) + S_v(n)$$

(Proposition 2). Il est clair aussi que la suite $f_0, f_1, \ldots, f_n, \ldots$ du Théorème 1 vérifie la condition (1).

(i) $\Rightarrow$ (ii). Soit donc une suite de polynômes $P_0, P_1, \ldots, P_n, \ldots$ vérifiant la condition (i). Si *on pose* $J_n = x_n^{-1} I_n$ on a

$$v[J_n] = -v(x_n) - S_v(n);$$

donc $J_n^{-1} = P_n(A)$, pour tout n. Si λ_n est dans J_n, $\lambda_n P_n$ est donc dans A_S et de même une somme

$$\lambda_0 P_0 + \lambda_1 P_1 + \ldots + \lambda_n P_n$$

où chaque λ_i est dans J_i (i variant de 1 a n).

Si par ailleurs P est un polynôme de degré n dans A_S et $P = \lambda_0 P_0 + \ldots + \lambda_n P_n$, le coéfficient directeur de P provient uniquement de P_n et c'est $\lambda_n x_n$. On a donc

$$v[\lambda_n x_n] \geqq v(P) \geqq -S_v(n) + v[P(A)]$$

et puisque $P(A) \subset A$, alors

$$v(\lambda_n) \geqq -v(x_n) - S_v(n) = v(J_n)$$

et λ_n est dans J_n. Grâce à la premiere partie du raisonnement on conclut que $P - \lambda_n P_n$ est aussi dans A_S; donc en reprenant l'argument que λ_{n-1} est dans J_{n-1}, on poursuit sans peine. . . .

(ii) $\Rightarrow$ (i). Inversement, supposons a priori que A_S se décompose en une suite d'idéaux $J_0, J_1, \ldots, J_n, \ldots$ selon les polynômes $P_0, P_1, \ldots, P_n, \ldots$. Alors pour tout élement α de J_n, αP_n est dans A_S; donc

$$\alpha P_n = \lambda_0 f_0 + \lambda_1 f_1 + \ldots + \lambda_n f_n$$

où $\lambda_k \in I_k$ ($k \in \{0, \ldots n\}$) et $f_0, f_1, \ldots, f_n, \ldots$ est la suite de polynômes du Théoreme 1. En regardant les termes de degré n on a $\alpha x_n = \lambda_n$ d'où on tire $J_n x_n \subset I_n$.

https://doi.org/10.4153/CJM-1972-071-2 Published online by Cambridge University Press

Inversement, pour tout β de I_n, βf_n est dans A_S et

$$\beta f_n = \lambda_0 P_0 + \lambda_1 P_1 + \ldots + \lambda_n P_n$$

où $\lambda_k \in J_k$, $(k \in \{0, \ldots, n\})$ d'où on tire $\beta = \lambda_n x_n$ et $I_n \subset J_n x_n$.
En définitive

$$J_n = I_n x_n^{-1}$$

Comme, pour tout α de f_n, αP_n est dans A_S, $\alpha P_n(A)$ est inclus dans A; donc $P_n(A)$ est inclus dans $J_n^{-1} = x_n I_n^{-1}$:

$$v[P_n(A)] \geqq v(x_n) + S_v(n).$$

Inversement,

$$v[P_n(A)] \leqq v(P_n) + S_v(n) \leqq v(x_n) + S_v(n)$$

(Proposition 2).

On voit que, si l'on impose aux polynômes P_n d'être unitaires, la suite des idéaux $I_0, I_1, \ldots, I_n, \ldots$ est canonique. Donnons en deux définitions intrinsèques: I_n est l'idéal fractionnaire des coéfficients directeurs des polynômes de A_S de degré n. Pour la seconde définition, faisons d'abord une remarque.

Remarque. Si on note $A_S^{(n)}$ le sous A-module de A_S formé des polynômes de A_S de degré inférieur ou égal à n, $A_S^{(n)}$ est projectif de rang $(n + 1)$ puisqu'on peut l'identifier à la somme directe:

$$A_S^{(n)} \cong I_0 \oplus \ldots \oplus I_n$$

grâce à la décomposition selon $f_0, f_1, \ldots, f_n$.

Comme la suite des idéaux $I_0, I_1, \ldots, I_n, \ldots$ est croissante, il est facile de vérifier que I_n est l'inverse de l'annulateur du A-module $A_S^{(n)}/A[X] \cap A_S^{(n)}$

COROLLAIRE 1 (Polya). *A_S est libre avec une base de polynômes de degré croissant si et seulement si tous les idéaux I_n sont principaux.*

C'est une conséquence immédiate du Théorème 2. On peut introduire la:

Définition. A_S est bien libre s'il admet une base de polynômes de degré croissant.

On peut ajouter à ce sujet, de façon evidente:

COROLLAIRE 1 (bis). *On a de façon équivalente:*
(i) *A_S est bien libre.*
(ii) *Tous les modules $A_S^{(n)}$ sont libres.*

Notons bien toutefois que le A-module A_S *est toujours libre* puisque projectif de rang infini [**1**; VII, § 4, Exercises].

COROLLAIRE 2. *Si A est l'anneau des entiers d'un corps de nombres K, $n!\, I_n$ est un idéal entier de A. Autrement dit, si P est dans A_S et de degré n, $n!P$ est dans $A[X]$.*

Notons v_p la valuation p-adique de $\mathbf{Q}$, v une valuation de K qui prolonge donc une des valuations v_p, et e l'indice de ramification de v_p sur v. Comme la norme N_v de v est une puissance de p (puissance égale au degré résiduel de v_p sur v) on a

$$\begin{aligned} S_v(n) &= \sum_{\alpha=1}^{\infty} \left[\frac{n}{N_v{}^{\alpha}} \right] \\ &\leqq \sum_{\alpha=1}^{\infty} \left[\frac{n}{p^{\alpha}} \right] \\ &= S_{v_p}(n) \\ &= \sum_{h=1}^{n} v_p(h) \\ &= \frac{1}{e} v(n!) \\ &\leqq v(n!). \end{aligned}$$

Comme $v(I_n{}^{-1}) = S_v(n)$ on a donc $v[n!I_n] \geqq 0$. Comme la suite $I_0, I_1, \ldots, I_n$ est croissante, les idéaux $n!I_0, n^1I_1, \ldots, n!I_n$ sont tous entiers, et si P est dans A_S et de degré n, $n!P$ est dans $A[X]$.

Bibliographie

1. N. Bourbaki, *Algèbre commutative* (Hermann, Paris, 1961).

2. P. J. Cahen and J. L. Chabert, *Coéfficients et valeurs d'un polynome*, Bull. Sci. Math. *95* (1971), 295–304.

3. Alexander Ostrowski, *Über ganzwertige Polynome in algebraischen Zahlkörpern*, J. Reine Angew. Math. *149* (1919), 117–124.

4. G. Polya, *Uber ganzwertige Polynome in algebraischen Zahlkörpern*, J. Reine Angew. Math. *149* (1919), 97–116.

5. P. Samuel, *Théorie algébrique des nombres*, (Hermann, Paris, 1900).

Queen's University,
Kingston, Ontario