ACTA ARITHMETICA
LXIII.2 (1993)

Dérivées et différences divisées à valeurs entières

par

Jean-Luc Chabert (Paris)

Introduction

1. On connaît bien, depuis Newton [21] au moins, les polynômes binomiaux

$$\binom{X}{n} = \frac{X(X-1)\dots(X-n+1)}{n!}\,.$$

Introduits à propos de l'interpolation linéaire et des différences finies (Gregory [16]), ils constituent une base du $\mathbb{Z}$-module des polynômes à valeurs entières sur $\mathbb{Z}$, c'est-à-dire des polynômes P à coefficients rationnels prenant des valeurs entières sur les entiers. Il s'agit essentiellement de la formule de Gregory–Newton :

$$P(X) = \sum_{n\geq 0} \Delta^n P(0) X(X-1)(X-2)\dots(X-n+1)/n!\,.$$

2. Plus récemment, Straus [27] a étudié l'ensemble $\mathbf{D}$ des polynômes à valeurs entières ainsi que toutes leurs dérivées et montré que $\mathbf{D}$ est un $\mathbb{Z}$-module libre admettant pour base les polynômes

$$d_n \binom{X}{n} \quad \text{où } d_n = \prod_p p^{[n/p]}\,.$$

De son côté, de Bruijn [14] a caractérisé l'ensemble $\mathbf{\Delta}^1$ des polynômes P à valeurs entières ainsi que leurs premières différences divisées :

$$\Delta P_m(X) = [P(X+m) - P(X)]/m \quad \text{pour } m \in \mathbb{Z},\ m \neq 0\,.$$

L'ensemble $\mathbf{\Delta}^1$ est un $\mathbb{Z}$-module libre admettant pour base les polynômes

$$\delta_n^1 \binom{X}{n} \quad \text{où } \delta_n^1 = \operatorname{ppcm}\{1,2,\dots,n\}\,.$$

Carlitz [10] a étendu cette caractérisation à l'ensemble $\mathbf{\Delta}^k$ des polynômes à valeurs entières ainsi que leurs k premières différences divisées successives;

il s'agit encore d'un $\mathbb{Z}$-module libre admettant pour base les polynômes

$$\delta_n^k \binom{X}{n} \quad \text{où } \delta_n^k = \text{ppcm}\{t_1 t_2 \dots t_r \mid r \leq k,\ t_1 + t_2 + \dots + t_r \leq n\}.$$

Pour $k = 1$, il s'agit du résultat de de Bruijn et, pour $k = \infty$, on voit que l'ensemble $\mathbf{\Delta}$ des polynômes à valeurs entières ainsi que toutes leurs différences divisées coïncide avec l'ensemble $\mathbf{D}$ étudié par Straus (cf. aussi [20]).

3. Or, dès 1919, Pólya [23] et Ostrowski [22] avaient considéré la notion de polynôme à valeurs entières sur un anneau d'entiers de corps de nombres et l'on pouvait se demander si l'égalité $\mathbf{D} = \mathbf{\Delta}$, démontrée par Carlitz pour $\mathbb{Z}$, subsistait pour tout anneau d'entiers. Ayant rencontré les différences divisées à propos de l'étude des fonctions lipschitziennes en analyse p-adique, Barsky [1] est amené à donner une réponse affirmative ([1], proposition III.6).

Le contre-exemple simple suivant relatif au corps de nombres $\mathbb{Q}(\sqrt{2})$ laisse penser que la réponse est plus nuancée. En effet, le polynôme

$$P(X) = X^2(X-1)^2/2$$

est à valeurs entières sur l'anneau des entiers $A = \mathbb{Z}[\sqrt{2}]$, ainsi que toutes ses dérivées puisque $P'(X)$ appartient à $A[X]$, alors que la différence divisée

$$[P(\sqrt{2}) - P(0)]/\sqrt{2} = -2 + 3\sqrt{2}/2$$

n'appartient pas à A.C'est pourquoi nous nous proposons de caractériser ici les anneaux d'entiers de corps de nombres pour lesquels l'égalité $\mathbf{D} = \mathbf{\Delta}$ a effectivement lieu. A cet effet, nous allons nous placer pour commencer dans un cadre plus général.

Notations et définitions

4. Pour l'instant A désigne un anneau intègre quelconque de corps des fractions K. Notons $\mathbf{B}_A$ l'anneau des *polynômes à valeurs entières sur* A :

$$\mathbf{B}_A = \{P \in K[X] \mid P(A) \subset A\}.$$

Pour tout entier naturel k, notons $\mathbf{D}_A^k$ l'anneau des *polynômes à valeurs entières sur* A *ainsi que leurs* k *premières dérivées* :

$$\mathbf{D}_A^k = \{P \in \mathbf{B}_A \mid P' \in \mathbf{D}_A^{k-1}\}$$

et $\mathbf{\Delta}_A^k$ l'anneau des *polynômes à valeurs entières sur* A *ainsi que leurs* k *premières différences divisées* :

$$\mathbf{\Delta}_A^k = \{P \in \mathbf{B}_A \mid \Delta_h P \in \mathbf{\Delta}_A^{k-1},\ h \in A - \{0\}\}$$

où

$$\Delta_h P(X) = [P(X+h) - P(X)]/h\,.$$

Bien sûr, nous convenons que

$$\mathbf{D}_A^0 = \mathbf{\Delta}_A^0 = \mathbf{B}_A\,.$$

Considérons enfin l'ensemble $\mathbf{D}_A$ des polynômes à valeurs entières sur A ainsi que toutes leurs dérivées :

$$\mathbf{D}_A = \bigcap_k \mathbf{D}_A^k\,,$$

et l'ensemble des polynômes à valeurs entières ainsi que toutes leurs différences divisées :

$$\mathbf{\Delta}_A = \bigcap_k \mathbf{\Delta}_A^k\,.$$

[N'oublions pas que, comme pour les dérivées, les différences divisées d'ordre $n+1$ d'un polynômes de degré n sont toutes nulles.]i

L'étude des anneaux $\mathbf{B}$ est entreprise en particulier dans [4], [8], [11]; celle des anneaux $\mathbf{D}^k$ dans [3], [5], [13], [24] et celle des anneaux $\mathbf{\Delta}^k$ dans [17]–[19], [28].

Les inclusions

5. Lorsqu'il ne peut y avoir de confusion, nous omettrons la référence à l'anneau de base A.

Proposition. *Pour tout entier k, l'anneau $\mathbf{\Delta}^k$ est inclus dans l'anneau $\mathbf{D}^k$.*

Il s'agit d'un résultat de Carlitz [10] pour $A = \mathbb{Z}$ et de Haouat et Grazzini [17] pour un anneau intègre A quelconque. Nous en redonnons la démonstration car il y a une petite erreur dans la formulation de [17] :

Lemme. *Si P appartient à $\mathbf{\Delta}^k$ $(k > 0)$, alors P' appartient à $\mathbf{\Delta}^{k-1}$.*

Démonstration. Pour tout polynôme P de $K[X]$, on a

$$P(X+Y) = P(X) + YP'(X) + Y^2 Q(X,Y) \quad \text{où } Q(X,Y) \in K[X,Y]\,.$$

Soit h un élément non nul de A tel que $hQ(X,Y)$ appartienne à $A[X,Y]$. Alors,

$$P'(X) = [P(X+h) - P(X)]/h - hQ(X,h)\,,$$

c'est-à-dire,

$$P'(X) = \Delta_h P(X) + R(X) \quad \text{où } R(X) \in A[X]\,.$$

Par suite, si P appartient à $\mathbf{\Delta}^k$ $(k > 0)$, alors $\Delta_h P$ appartient à $\mathbf{\Delta}^{k-1}$ et donc P' aussi.

Démonstration de la proposition. Montrons par récurrence sur k que $\mathbf{\Delta}^k$ est inclus dans $\mathbf{D}^k$. Pour $k = 0$ cela résulte des définitions. Soit $k > 0$ quelconque : si P appartient à $\mathbf{\Delta}^k$, alors P' appartient à $\mathbf{\Delta}^{k-1}$ d'après le lemme; par hypothèse de récurrence, $\mathbf{\Delta}^{k-1}$ est inclus dans $\mathbf{D}^{k-1}$, donc P appartient à $\mathbf{D}^k$.

Corollaire. *L'anneau $\mathbf{\Delta}$ est inclus dans l'anneau $\mathbf{D}$.*

6. On peut résumer la situation de la façon suivante :

$$\begin{array}{ccccccccccc} A[X] \subset \mathbf{\Delta} & \subset \ldots \subset & \mathbf{\Delta}^k & \subset & \mathbf{\Delta}^{k-1} & \subset \ldots \subset & \mathbf{\Delta}^1 & & & & \\ \cap & & \cap & & \cap & & \cap & & & & \\ \mathbf{D} \subset \ldots & \subset & \mathbf{D}^k & \subset & \mathbf{D}^{k-1} & \subset \ldots \subset & \mathbf{D}^1 & \subset & \mathbf{B} & \subset & K[X] \end{array}$$

Dans le cas de $\mathbb{Z}$, l'égalité entre $\mathbf{D}$ et $\mathbf{\Delta}$ mise à part, toutes les inclusions ci-dessus sont strictes :

$\mathbb{Z}[X] \neq \mathbf{\Delta}$ car $X^2(X-1)^2/2 \in \mathbf{D} - \mathbb{Z}[X]$ et $\mathbf{D} = \mathbf{\Delta}$.

$\mathbf{B} \neq K[X]$ est évident et $\mathbf{D}^1 \neq \mathbf{B}$ car $X(X-1)/2 \in \mathbf{B} - \mathbf{D}^1$.

$\mathbf{\Delta}^k \neq \mathbf{\Delta}^{k+1}$ peut se vérifier en utilisant la caractérisation des éléments de $\mathbf{\Delta}^k$ donnée par Carlitz (cf. §2); ainsi, pour tout nombre premier p, la puissance de p qui divise $\delta^k_{p^3}$ pour $k = p$ est p^{2p} et pour $k = p^2$ est p^{p^2}.

$\mathbf{D}^1 \not\subset \mathbf{\Delta}^1$ car, si $g(X) = [X^p - X]/p$, alors $g_1(X) = g(X)^p \in \mathbf{D}^1$, tandis que $\Delta_p g_1(0) = (p^{p-1} - 1)^p/p \notin \mathbb{Z}$; et même $\mathbf{D}^k \not\subset \mathbf{\Delta}^1$, pour tout $k \geq 1$, car $g_k(X) = g(X)^{pk} \in \mathbf{D}^k$, tandis que $\Delta_p g_k(0) \notin \mathbb{Z}$; a fortiori $\mathbf{D}^k \not\subset \mathbf{\Delta}^k$ pour tout $k \geq 1$.

$\mathbf{D}^k \neq \mathbf{D}^{k+1}$, sinon $\mathbf{D}^k = \mathbf{D}^{k+1} = \mathbf{D}^{k+2} = \ldots = \mathbf{D} = \mathbf{\Delta} \subset \mathbf{\Delta}^1$; ou encore, p désignant un nombre premier au moins égal à $k+2$:

$h(X) = [X(X-1)\ldots(X-p+1)]^{k+1}/p \in \mathbf{D}^k - \mathbf{D}^{k+1}$ (exemple de [2]).

Dans le cas d'un anneau A d'entiers de corps de nombres on verra que, mise à part l'éventuelle égalité entre $\mathbf{D}$ et $\mathbf{\Delta}$ que l'on sait complètement caractériser, toutes ces inclusions sont encore strictes (cf. §15).

Localisation

7. Soit S une partie multiplicative de A. On sait [8] que tout polynôme à valeurs entières sur A est encore à valeurs entières sur $S^{-1}A$, autrement dit

$$S^{-1}(\mathbf{B}_A) \subset \mathbf{B}_{S^{-1}A}\,.$$

Par suite :

Proposition. *Pour toute partie multiplicative S de A, on a*

$$S^{-1}(\mathbf{R}_A) \subset \mathbf{R}_{S^{-1}A}$$

où $\mathbf{R}$ désigne indifféremment l'un des anneaux : $\mathbf{B}$, $\mathbf{\Delta}^k$, $\mathbf{D}^k$, $\mathbf{\Delta}$ ou $\mathbf{D}$.

Démonstration. La vérification des inclusions concernant les anneaux $\mathbf{D}$ est immédiate compte tenu du rappel précédent; celle concernant les anneaux $\mathbf{\Delta}$ nécessite l'utilisation répétée de cette inclusion initiale (cf. Haouat et Grazzini [19]). Le principe est le suivant : soit P dans $\mathbf{\Delta}^1_A$; alors, pour tout $h \in A-\{0\}$, $\mathbf{\Delta}_h P$ appartient à $\mathbf{B}_A$, donc à $\mathbf{B}_{S^{-1}A}$. Fixons x dans $S^{-1}A$ et considérons le polynôme $Q_x(Y) = [P(x+Y)-P(x)]/Y = \Delta_Y P(x)$. Pour $h \in A - \{0\}$, $Q_x(h)$ appartient à $S^{-1}A$, donc $Q_x(A)$ est inclus dans $S^{-1}A$ et $Q_x(S^{-1}A)$ aussi, c'est-à-dire $\Delta_h P(x)$ appartient à $S^{-1}A$ pour tout x dans $S^{-1}A$ et pour tout h dans $S^{-1}A - \{0\}$.

On vérifie sans peine les égalités

$$\mathbf{R}_A = \bigcap_{\mathfrak{m}\in \mathrm{Max}(A)} \mathbf{R}_{A_\mathfrak{m}}$$

où, là encore, $\mathbf{R}$ désigne indifféremment : $\mathbf{B}$, $\mathbf{\Delta}^k$, $\mathbf{D}^k$, $\mathbf{\Delta}$ ou $\mathbf{D}$. D'où :

Corollaire. *Pour que l'égalité* $\mathbf{D}_A = \mathbf{\Delta}_A$ *ait lieu, il suffit que, pour tout idéal maximal* $\mathfrak{m}$ *de* A, $\mathbf{D}_{A_\mathfrak{m}} = \mathbf{\Delta}_{A_\mathfrak{m}}$.

Cependant cette condition n'est pas toujours nécessaire. Considérons le cas de l'anneau A de tous les entiers algébriques : $\mathbf{B}_A = A[X]$ et donc $\mathbf{D}_A = \mathbf{\Delta}_A = A[X]$, tandis qu'il existe des idéaux maximaux $\mathfrak{m}$ de A de corps résiduel fini, au-dessus d'un nombre premier p et dont l'indice de ramification absolu est supérieur à p. Donc, compte tenu du §13 ci-dessous, on a $\mathbf{D}_{A_\mathfrak{m}} \neq \mathbf{\Delta}_{A_\mathfrak{m}}$ pour les localisés $A_\mathfrak{m}$ correspondants.

8. Par contre, si l'anneau A est supposé noethérien, les inclusions de la proposition précédente deviennent des égalités :

Proposition. *Si l'anneau* A *est noethérien, alors, pour toute partie multiplicative* S *de* A, *on a*

$$S^{-1}(\mathbf{R}_A) = \mathbf{R}_{S^{-1}A}$$

où $\mathbf{R}$ *désigne indifféremment l'un des anneaux* : $\mathbf{B}$, $\mathbf{\Delta}^k$, $\mathbf{D}^k$, $\mathbf{\Delta}$ *ou* $\mathbf{D}$.

Démonstration. Pour les anneaux $\mathbf{D}$, la preuve est analogue à celle de $\mathbf{B}$: si P appartient à $\mathbf{D}^k_{S^{-1}A}$, c'est-à-dire si $P, P', \ldots, P^{(k)}$ appartiennent à $\mathbf{B}_{S^{-1}A}$, alors il existe s dans S tels que $sP, sP', \ldots, sP^{(k)}$ appartiennent à $\mathbf{B}_A$, c'est-à-dire sP appartient à $\mathbf{D}^k_A$; en effet, le A-module engendré par les valeurs de $P, P', \ldots, P^{(k)}$ sur A étant contenu dans le A-module de type fini engendré par les coefficients de $P, P', \ldots, P^{(k)}$ est lui-même de type fini. Ce raisonnement s'étend à $\mathbf{D}$ puisqu'un polynôme P n'a qu'un nombre fini de dérivées non nulles.

Pour les anneaux $\mathbf{\Delta}$, indiquons la démonstration dans le cas de $\mathbf{\Delta}^1$. Pour tout polynôme P, posons

$$P(X+Y) = P(X) + YP'(X) + Y^2P^{[2]}(X) + \ldots + Y^dP^{[d]}(X)$$

et soit N le A-module de type fini engendré par les coefficients de P, P', $P^{[2]}, \ldots, P^{[d]}$. Si P appartient à $\mathbf{\Delta}^1_{S^{-1}A}$, alors, pour tout h dans $A - \{0\}$ et pour tout x dans A, les $\Delta_h P(x) = [P(x+h) - P(x)]/h = P'(x) + hP^{[2]}(x) + \ldots + h^{d-1}P^{[d]}(x)$ appartiennent au A-module de type fini $N \cap S^{-1}A$. Soit s dans S tel que $s(N \cap S^{-1}A)$ soit inclus dans A; alors sP appartient à $\mathbf{\Delta}^1_A$.

Corollaire. *Lorsque A est noethérien, pour que $\mathbf{D}_A = \mathbf{\Delta}_A$ il faut et il suffit que, pour tout idéal maximal $\mathfrak{m}$ de A, $\mathbf{D}_{A_\mathfrak{m}} = \mathbf{\Delta}_{A_\mathfrak{m}}$.*

Etude locale

9. Commençons par évacuer les cas simples où $\mathbf{B} = A[X]$ et où donc a fortiori $\mathbf{D}_A = \mathbf{\Delta}_A$. Dans le cas contraire où $\mathbf{B} \neq A[X]$, un certain nombre des inclusions considérées sont par contre toujours strictes pour les "petites valeurs" de k :

Proposition. *Supposons l'anneau intègre A noethérien, local, d'idéal maximal $\mathfrak{m}$.*

(i) *Si $A/\mathfrak{m}$ est fini (de caractéristique p) et si $\mathfrak{m} \in \mathrm{Ass}(K/A)$, alors $\mathbf{D} \neq A[X]$ et, pour tout k tel que $1 \leq k < p$, on a*

$$\mathbf{\Delta}^{k-1} \not\subset \mathbf{D}^k \quad \textit{et, a fortiori,} \quad \mathbf{\Delta}^{k-1} \neq \mathbf{\Delta}^k \textit{ et } \mathbf{D}^{k-1} \neq \mathbf{D}^k\,.$$

(ii) *Sinon, $\mathbf{B} = A[X]$ et donc, pour tout k,*

$$\mathbf{\Delta} = \mathbf{D} = \mathbf{\Delta}^k = \mathbf{D}^k = A[X]\,.$$

L'assertion (ii) résulte du :

Rappel. Supposons A local d'idéal maximal $\mathfrak{m}$.

(i) Si $A/\mathfrak{m}$ est infini, alors $\mathbf{B} = A[X]$ [8].

(ii) Si A est noethérien et si $A/\mathfrak{m}$ est fini, alors $\mathbf{B} = A[X]$ si et seulement si $\mathrm{prof}(K/A) > 0$, c'est-à-dire $A = \bigcap_{\mathfrak{p} \neq \mathfrak{m}} A_\mathfrak{p}$ [12].

Démonstration de (i). Soit α un élément de $K \backslash A$ tel que $\mathfrak{m}\alpha \subset A$. Posons $g_k(X) = \alpha(X^q - X)^k$. Nous allons montrer que, pour $1 \leq k < p$, $g_k(X)$ appartient à $\mathbf{\Delta}^{k-1}$ et n'appartient pas à $\mathbf{D}^k$; de plus, $g_p(X)$ appartient à $\mathbf{D}$ et n'appartient pas à $A[X]$.

Posons $s(X) = X^q - X$ et vérifions que les polynômes différences divisées d'ordre $\leq k-1$ de $s^k(X)$ sont tous à valeurs dans $\mathfrak{m}$ sur A.

Soit h dans $A-\{0\}$; alors

$$\Delta_h s^k(X) = \Delta_h s(X) \sum_{i=0}^{k-1} s^i(X+h)s^{k-i-1}(X)$$

où $\Delta_h s(X) \in A[X]$ et, pour $k-1>0$, chaque terme $s^i(X+h)s^{k-i-1}(X)$ est à valeurs dans $\mathfrak{m}$.

Soit l dans $A-\{0\}$; alors

$$\begin{aligned}\Delta_l s^i(X+h)s^{k-i-1}(X)&\\ &= s^i(X+h+l)\Delta_l s^{k-i-1}(X) + s^{k-i-1}(X)\Delta_l s^i(X+h)\\ &= s^i(X+h+l)\Delta_l s(X) \sum_{j=0}^{k-i-2} s^j(X+l)s^{k-i-j-2}(X)\\ &\quad + s(X)^{k-i-1}\Delta_l s(X+h)\sum_{j=0}^{i-1} s^j(X+h+l)s^{i-j-1}(X+h)\end{aligned}$$

où $\Delta_l s(X)$ et $\Delta_l s(X+h) \in A[X]$ et les termes du type $s^i(X+h+l)s^j(X+l)s^{k-i-j-2}(X)$ sont à valeurs dans $\mathfrak{m}$ dès que $i+j+(k-i-j-2)=k-2>0$.

Et ainsi de suite, d'où $g_k(X)$ appartient à $\mathbf{\Delta}^{k-1}$. Par ailleurs, supposant toujours $1 \le k < p$, on vérifie par récurrence sur i, que pour $0 \le i \le k$, $g_k^{(i)}(X) = \alpha(X^q - X)^{k-i}r_i(X)$ où $r_i(X) \in A[X]$ et $r_i(y) \notin \mathfrak{m}$ pour $y \in \mathfrak{m}$.

Par suite, $g_k^{(i)}(X)$ appartient à $\mathbf{B}$ pour $0 \le i < k$, tandis que $g_k^{(k)}(y)$ n'appartient pas à A dès que y est dans $\mathfrak{m}$. Ainsi, g_k appartient à $\mathbf{D}^{k-1}$ (ce que l'on savait puisque $\mathbf{\Delta}^{k-1} \subset \mathbf{D}^{k-1}$), mais n'appartient pas à $\mathbf{D}^k$.

Enfin, $g_p(X)$ appartient à $\mathbf{D}$, puisque $g_p'(X)$ est dans $A[X]$.

10. Seul le cas (i) de la proposition précédente se présente pour les localisés d'anneaux d'entiers de corps de nombres. Si nous nous limitons à la dimension 1, la situation à considérer est la suivante :

Hypothèses. L'anneau intègre A est noethérien, de dimension 1, local, d'idéal maximal $\mathfrak{m}$, de corps résiduel fini de cardinal $q = p^f$. Notons aussi A' la clôture intégrale de A et A^* le complété de A pour la topologie $\mathfrak{m}$-adique.

Si les anneaux $\mathbf{D}$ et $\mathbf{\Delta}$ coïncident, ils ont le même spectre et en particulier le même nombre d'idéaux premiers au-dessus de $\mathfrak{m}$. On va voir qu'en général les anneaux $\mathbf{D}^k$ et $\mathbf{\Delta}^k$ sont très différents au niveau de leur spectre et en particulier au niveau des idéaux premiers au-dessus de $\mathfrak{m}$.

Rappels. Sous les hypothèses ci-dessus:

(i) Les idéaux premiers de $\mathbf{B}$ au-dessus de $\mathfrak{m}$ sont de la forme $\mathfrak{m}_x = \{P \in \mathbf{B} \mid P(x) \in \mathfrak{m}A^*\}$ où x est un élément quelconque de A^* [12].

(ii) Lorsque A est unibranche, c'est-à-dire lorsque A' a un seul idéal maximal $\mathfrak{m}'$, les idéaux $\mathfrak{m}_x$ distincts sont en nombre infini (en bijection avec l'adhérence de A dans le complété de A' pour la topologie $\mathfrak{m}'$-adique [7]).

(iii) Lorsque A n'est pas unibranche, les idéaux $\mathfrak{m}_x$ distincts sont en nombre fini (en bijection avec le quotient de A par un idéal [6] et [15]).

(iv) Les idéaux premiers de $\mathbf{\Delta}^k$ au-dessus de $\mathfrak{m}$ sont de la forme $\mathfrak{m}_a(\mathbf{\Delta}^k) = \mathfrak{m}_a \cap \mathbf{\Delta}^k = \{P \in \mathbf{\Delta}^k \mid P(a) \in \mathfrak{m}\}$ et ceux de $\mathbf{\Delta}$ de la forme $\mathfrak{m}_a(\mathbf{\Delta}) = \mathfrak{m}_a \cap \mathbf{\Delta} = \{P \in \mathbf{\Delta} \mid P(a) \in \mathfrak{m}\}$ où a décrit un système de représentants de A modulo $\mathfrak{m}$; leur nombre est exactement q [19].

(v) Pour tout polynôme Q de $\mathbf{B}$ et pour tout entier k, il existe un entier s tel que Q^s appartienne à $\mathbf{D}^k$ [13].

Proposition. *Sous les hypothèses ci-dessus, lorsqu'en outre A est unibranche, pour tout entier k, l'anneau $\mathbf{\Delta}^k$ est strictement contenu dans l'anneau $\mathbf{D}^k$. Lorsque de plus A est de caractéristique p, l'anneau $\mathbf{\Delta}$ est strictement contenu dans l'anneau $\mathbf{D}$.*

Démonstration. En effet, pour tout entier k, l'application $\mathfrak{m}_x \to \mathfrak{m}_x(\mathbf{D}^k) = \mathfrak{m}_x \cap \mathbf{D}^k$ est une bijection entre les idéaux premiers de $\mathbf{B}$ au-dessus de $\mathfrak{m}$ et ceux de $\mathbf{D}^k$ au-dessus de $\mathfrak{m}$ (rappel (v)). L'anneau A étant supposé unibranche, $\mathrm{Spec}(\mathbf{B}/\mathfrak{m}\mathbf{B})$ est infini (rappel (ii)), donc aussi $\mathrm{Spec}(\mathbf{D}^k/\mathfrak{m}\mathbf{D}^k)$, alors que $\mathrm{Spec}\,(\mathbf{\Delta}^k/\mathfrak{m}\mathbf{\Delta}^k)$ est de cardinal fini q (rappel (iv)).

[Lorsque A n'est pas unibranche, le nombre fini des idéaux $\mathfrak{m}_x$ distincts (rappel (iii)) n'étant pas systématiquement connu, la question reste ouverte.]

Lorsque A est unibranche et de caractéristique p, alors, pour tout polynôme Q de $\mathbf{B}$, Q^p appartient à $\mathbf{D}$ et le raisonnement précédent fonctionne encore pour $\mathbf{D}$ et $\mathbf{\Delta}$.

[Nous allons voir par contre que, si A est de caractéristique nulle, alors $\mathrm{Spec}(\mathbf{D}/\mathfrak{m}\mathbf{D})$ est fini (cf. §12).]

Cas local de caractéristique 0

11. Hypothèses. L'anneau intègre noethérien local A, de dimension 1, de corps résiduel fini (de caractéristique p), est supposé maintenant de caractéristique 0. Il existe alors un entier r tel que $\mathfrak{m}^{r(p-1)}$ soit contenu dans l'idéal pA.

Proposition. *Sous les hypothèses ci-dessus, si $\mathfrak{m}^{p-1} \subset pA$, alors $\mathbf{D} = \mathbf{\Delta}$.*

En effet, pour montrer que $\mathbf{D}$ est contenu dans $\mathbf{\Delta}$ il suffit de vérifier que $\mathbf{D}$ est stable par les opérateurs Δ_h où $h \in A - \{0\}$; cela résulte du lemme suivant dans le cas où $r = 1$.

LEMME. *Quel que soit le polynôme P de $\mathbf{D}$ et quel que soit l'élément non nul h de $\mathfrak{m}^r$, le polynôme $\Delta_h(P)$ appartient encore à $\mathbf{D}$.*

Démonstration. Soient P dans $\mathbf{D}$ et h dans $\mathfrak{m}^r$; alors

$$\Delta_h(P(X)) = [P(X+h) - P(X)]/h = \sum_{n\geq 1}(h^{n-1}/n!)P^{(n)}(X)$$

où les $P^{(n)}(X)$ sont dans $\mathbf{D}$ et les $h^{n-1}/n!$ dans A, car quel que soit $h \in \mathfrak{m}^r$ et quel que soit $n \in \mathbb{N}$, $h^{n-1}/n!$ appartient à A.

En effet, l'élément h^{n-1} appartient à $\mathfrak{m}^{r(n-1)}$, donc à $\mathfrak{m}^{kr(p-1)}$ où k désigne la partie entière de $(n-1)/(p-1)$, donc à p^kA. Tout entier premier à p étant inversible dans l'anneau local A, il suffit de montrer que $k \geq v_p(n!)$ où $v_p(n!)$ désigne la plus grande puissance de p divisant $n!$. Cela revient à$(n-1)/(p-1) \geq v_p(n!)$, c'est-à-dire $n-1 \geq (p-1)v_p(n!)$ ou $n > (p-1)v_p(n!)$. Or,

$$v_p(n!) = [n/p] + [n/p^2] + [n/p^3] + \ldots < n/p + n/p^2 + n/p^3 + \ldots = n/(p-1).$$

Remarque. Par contre, s'il existe h dans $\mathfrak{m}$ tel que h^{p-1} n'appartienne pas à pA tandis que $\mathfrak{m}^p$ est inclus dans pA, alors $\mathbf{D} \not\subset \mathbf{\Delta}^1$ et donc $\mathbf{D} \neq \mathbf{\Delta}$.

En effet, $g(X) = (X^q - X)^p/p$ appartient à $\mathbf{B}$ et $g'(X)$ appartient à $A[X]$—donc $g(X)$ est dans $\mathbf{D}$—puisque $\mathfrak{m}^p \subset pA$. Par ailleurs, $\Delta_h g(0) = (h^{q-1} - 1)^p h^{p-1}/p$ n'est dans A pour h dans $\mathfrak{m}$ que si $h^{p-1} \in pA$.

EXEMPLE. Soit $A = \mathbb{Z}[\sqrt{d}]$ où d est un entier sans facteurs carrés et soit $\mathfrak{m}$ un idéal premier de A au-dessus de 2. L'anneau $A_{\mathfrak{m}}$ est noethérien, de dimension 1, local, de corps résiduel fini de caractéristique $p = 2$. On a $\mathfrak{m}^2 \subset 2A$, mais $\mathfrak{m} \not\subset 2A$; donc $\mathbf{D}_{A_{\mathfrak{m}}} \neq \mathbf{\Delta}_{A_{\mathfrak{m}}}$.

12. Toujours en caractéristique 0, les idéaux premiers de $\mathbf{D}$ au-dessus de $\mathfrak{m}$ sont en nombre fini. De manière précise :

PROPOSITION. *Si $a \equiv b \pmod{\mathfrak{m}^r}$, alors $\mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})$ où $\mathfrak{m}_a(\mathbf{D})$ désigne l'idéal maximal $\{P \in \mathbf{D} \mid P(a) \in \mathfrak{m}\}$.*

En effet, pour P dans $\mathbf{D}$, $[P(b) - P(a)]/(b-a) = \Delta_{b-a}(P(a))$ appartient à A (lemme du §11), donc $P(b) - P(a)$ appartient à $\mathfrak{m}^r$ et $P \in \mathfrak{m}_a(\mathbf{D})$ équivaut à $P \in \mathfrak{m}_b(\mathbf{D})$.

COROLLAIRE 1. *Lorsque $\mathfrak{m}^{p-1} \subset pA$, on a : $\mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})$ si et seulement si $a \equiv b \pmod{\mathfrak{m}}$.*

En effet, d'une façon générale, si $\mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})$ alors nécessairement $a \equiv b \pmod{\mathfrak{m}}$, puisque $X - a$ appartient à $\mathfrak{m}_a(\mathbf{D})$. La réciproque résulte de la proposition quand $r = 1$.

COROLLAIRE 2. *Lorsque A est unibranche de caractéristique 0, les anneaux $\mathbf{D}^k$ sont tous distincts.*

En effet, si l'on avait $\mathbf{D}^k = \mathbf{D}^{k+1}$ pour un certain entier k, $\mathbf{D}$ serait égal à $\mathbf{D}^k$, en contradiction avec le fait que $\mathrm{Spec}(\mathbf{D}^k/\mathfrak{m}\mathbf{D}^k)$ est infini (cf. §10), alors que $\mathrm{Spec}(\mathbf{D}/\mathfrak{m}\mathbf{D})$ est fini (proposition précédente).

Cas d'un anneau de valuation discrète

13. Lorsque A est l'anneau d'une valuation discrète v de corps résiduel fini, pour tout k, les anneaux $\mathbf{D}^k$ et $\mathbf{\Delta}^k$ sont distincts (§10) et, lorsqu'en outre A est de caractéristique 0, les anneaux $\mathbf{D}^k$ et $\mathbf{D}^{k+1}$ sont eux-aussi distincts (§12). De plus :

Soit $h(x) = [(X^q - X)/t]^p$, où t désigne l'uniformisante de v. Alors $h(X) \in \mathbf{B}$, mais $D_t h(0) = [h(t) - h(0)]/t = (t^{q-1} - 1)^p/t$ n'est pas dans A, donc $h \notin \mathbf{\Delta}^1$. Si $v(p) \geq p$, alors $h'(x) = (X^q - X)^{p-1}(qX^{q-1} - 1)p/t^p$ appartient à $A[X]$, donc $h(X)$ appartient à $\mathbf{D}$ et $\mathbf{D} \not\subset \mathbf{\Delta}^1$, a fortiori $\mathbf{D} \neq \mathbf{\Delta}$. D'où :

Proposition. *Si A désigne l'anneau d'une valuation discrète v, les anneaux $\mathbf{D}$ et $\mathbf{\Delta}$ sont égaux si et seulement si le corps résiduel de v est infini ou si sa caractéristique p vérifie $v(p) < p$.*

Démonstration. La condition suffisante résulte du §9 lorsque le corps résiduel est infini et du §11 sinon, puisqu'alors A est nécessairement de caractéristique 0. La condition nécessaire résulte du contre-exemple précédent. Lorsque A est de caractéristique p, le contre-exemple fonctionne encore, mais l'assertion résulte aussi du §10.

On notera que cette condition $v(p) < p$ apparaît incidemment dans [2] à propos d'une remarque sur le spectre de $\mathbf{D}$, dans [24] à propos de la difficulté de détermination d'une base du A-module $\mathbf{D}$, mais aussi à plusieurs reprises dans [5] en particulier à propos de la non noethérianité de $\mathbf{D}$.

14. Supposons encore que A soit l'anneau d'une valuation discrète v de corps résiduel fini et que sa caractéristique soit nulle. Non seulement l'ensemble des idéaux premiers de $\mathbf{D}$ au-dessus de $\mathfrak{m}$ est fini (§12), mais il est en bijection avec $A/\mathfrak{m}$ lorsque $v(p) \leq p-1$ (équivalence (β) ci-dessous), et avec $A/\mathfrak{m}^2$ lorsque $p \leq v(p) \leq 2(p-1)$ (implication (δ) ci-dessous). Par contre, la question du nombre des idéaux premiers de $\mathbf{D}$ au-dessus de $\mathfrak{m}$ pour $v(p) \geq 2p-1$ reste ouverte.

En effet, la proposition du §12 se traduit par

$$(\alpha) \qquad [v(p) \leq r(p-1) \text{ et } v(a-b) \geq r] \;\Rightarrow\; [\mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})]\,,$$

et son corollaire 1 par

$$[v(p) < p] \Rightarrow [v(a-b) \geq 1 \Leftrightarrow \mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})]\,.$$

Par ailleurs, si $v(p) \geq p$, le polynôme $h(X)$ de l'exemple précédent appartient à $\mathfrak{m}_0(\mathbf{D})$, mais non à $\mathfrak{m}_t(\mathbf{D})$; donc $v(p) \geq p$ et $v(a-b) \geq 1$ n'impliquent pas $\mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})$. Finalement,

$$(\beta) \qquad [v(p) < p] \Leftrightarrow [v(a-b) \geq 1 \Leftrightarrow \mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})]\,.$$

Mais on a aussi

$$(\gamma) \qquad [v(p) \geq p(q^s-1)/(q-1) \text{ et } \mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})] \;\Rightarrow [v(a-b) > s]\,.$$

En effet, supposons que $v(a-b) \leq s$ et considérons un système de représentants de A modulo $\mathfrak{m}^s$, $a_1, a_2, \ldots, a_{q^s}$, contenant a mais non b. Posons $w(s) = (q^s-1)/(q-1)$ et $g(X) = t^{-w(s)}(X-a_1)(X-a_2)\ldots(X-a_{q^s})$. Alors $g(X)$ appartient à $\mathbf{B}$, $g(a) = 0$ tandis que $v(g(b)) = 0$ (cf. [11]). Si $v(p) \geq pw(s)$, alors $(g^p)'$ appartient à $A[X]$, g^p est dans $\mathbf{D}$ et finalement appartient à $\mathfrak{m}_a(\mathbf{D})$, mais non à $\mathfrak{m}_b(\mathbf{D})$.

En particulier, pour $s = 1$,

$$[v(p) \geq p \text{ et } \mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})] \;\Rightarrow\; [v(a-b) \geq 2]\,,$$

alors que, pour $r = 2$,

$$[v(p) \leq 2(p-1) \text{ et } v(a-b) \geq 2] \;\Rightarrow [\mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})]\,;$$

d'où

$$(\delta) \qquad [p \leq v(p) \leq 2(p-1)] \;\Rightarrow\; [v(a-b) \geq 2 \Leftrightarrow \mathfrak{m}_a(\mathbf{D}) = \mathfrak{m}_b(\mathbf{D})]\,.$$

Globalisation

15. Les §§8 et 13 conduisent au

THÉORÈME. *Soit A un anneau de Dedekind. Les anneaux $\mathbf{D}$ et $\mathbf{\Delta}$ sont égaux si et seulement si, pour tout idéal maximal $\mathfrak{m}$ de A, ou bien le corps résiduel $A/\mathfrak{m}$ est infini, ou bien sa caractéristique p vérifie $\mathfrak{m}^{p-1} \subset pA_{\mathfrak{m}}$.*

Application au cas de l'anneau des entiers d'un corps de nombres :

PROPOSITION. *Soit A l'anneau des entiers d'un corps de nombres K. Pour que $\mathbf{D} = \mathbf{\Delta}$ il faut et il suffit que chaque idéal maximal $\mathfrak{m}$ de A vérifie les conditions équivalentes suivantes (où p désigne le nombre premier au-dessous de $\mathfrak{m}$) :*

(i) *l'indice de ramification $e = e(\mathfrak{m}/p)$ de $\mathfrak{m}$ dans l'extension $K/\mathbb{Q}$ est majoré par $p-1$,*

(ii) *l'exposant s de $\mathfrak{m}$ dans la différente $\mathcal{D}_{A/\mathbb{Z}}$ est majoré par $p-2$.*

Démonstration. La condition (i) est celle du théorème. Il s'agit de montrer l'équivalence de (i) et (ii). On sait ([26], chap. III) que, d'une façon générale, l'exposant s de $\mathfrak{m}$ dans la différente $\mathcal{D}_{A/\mathbb{Z}}$ est toujours au moins égal à $e-1$ et que l'égalité $s=e-1$ a lieu si et seulement si p ne divise pas e. Ici, si $e \leq p-1$, alors p ne divise pas e et donc $s=e-1 \leq p-2$; d'où (i)⇒(ii). Inversement, si $s \leq p-2$, comme $s \geq e-1$, on a $e \leq s+1 \leq p-1$; d'où (ii)⇒(i).

De plus :

Proposition. *Lorsque A est l'anneau des entiers d'un corps de nombres, l'éventuelle égalité entre $\mathbf{D}$ et $\mathbf{\Delta}$ mise à part, toutes les inclusions suivantes sont strictes* :

$$\begin{array}{ccccccccccc} A[X] \subset \mathbf{\Delta} & \subset & \ldots & \subset & \mathbf{\Delta}^k & \subset & \mathbf{\Delta}^{k-1} & \subset & \ldots & \subset & \mathbf{\Delta}^1 \\ \cap & & & & \cap & & \cap & & & & \cap \\ \mathbf{D} & \subset & \ldots & \subset & \mathbf{D}^k & \subset & \mathbf{D}^{k-1} & \subset & \ldots & \subset & \mathbf{D}^1 \subset \mathbf{B} \subset K[X] \end{array}$$

Démonstration. Pour tout entier k, l'anneau $\mathbf{\Delta}^k$ est strictement contenu dans l'anneau $\mathbf{D}^k$ (§§8 et 10) et l'anneau $\mathbf{D}^k$ est lui-même strictement contenu dans l'anneau $\mathbf{D}^{k-1}$ (§§8 et 12). Il reste à s'assurer que les anneaux $\mathbf{\Delta}^{k-1}$ et $\mathbf{\Delta}^k$ sont eux-aussi distincts. Or, pour tout k, il existe un nombre premier $p>k$ et un idéal maximal $\mathfrak{m}$ de A au-dessus de p. Pour le localisé $A_{\mathfrak{m}}$ correspondant, on a $\mathbf{\Delta}_{A_{\mathfrak{m}}}^{p-1} \neq \mathbf{\Delta}_{A_{\mathfrak{m}}}^{p-2}$ (§9) , par suite $\mathbf{\Delta}_A^{p-1} \neq \mathbf{\Delta}_A^{p-2}$ (§8) et donc $\mathbf{\Delta}_A^k \neq \mathbf{\Delta}_A^{k-1}$.

16. *Corps quadratiques.* Lorsque A est l'anneau des entiers d'un corps quadratique $K=\mathbb{Q}[\sqrt{d}]$ où d est un entier sans facteurs carrés, l'égalité $\mathbf{D}=\mathbf{\Delta}$ a lieu si et seulement si $d \equiv 1 \pmod 4$.

En effet, puisque $[K/\mathbb{Q}]=2$, $e=e(\mathfrak{m}/p)=1$ ou 2 et le seul cas à rejeter est celui où $e=2$ et $p=2$. Or, 2 est ramifié si et seulement si $d \equiv 2$ ou $3 \pmod 4$ ([25], chap. V); reste donc le cas où $d \equiv 1 \pmod 4$ et $A=\mathbb{Z}+(1+\sqrt{d})/2\,\mathbb{Z}$.

Corps cyclotomiques. Lorsque A est l'anneau des entiers d'un corps cyclotomique $K=\mathbb{Q}[\zeta]$ où ζ désigne une racine primitive $n$ième de l'unité, l'égalité $\mathbf{D}=\mathbf{\Delta}$ a lieu si et seulement si n est un produit de nombres premiers distincts.

En effet, les nombres premiers p ramifiés dans l'extension $A/\mathbb{Z}$ sont ceux qui divisent n et l'indice de ramification correspondant est égal à $p^{k-1}(p-1)$ où p^k désigne la plus grande puissance de p divisant n ([26], chap. IV). Pour que la condition du théorème soit réalisée, il faut et il suffit donc que $k=1$.

Contre-exemples (pour lesquels $\mathbf{\Delta}$ est strictement contenu dans $\mathbf{D}$).

(i) L'anneau A d'une courbe plane irréductible et non singulière sur un corps fini $\mathbb{F}_q$ (cf. §10).

(ii) L'anneau A des entiers du corps de nombres $K = \mathbb{Q}[\sqrt[p]{p}]$ où p désigne un nombre premier quelconque.

En effet, si ξ désigne une racine $p$ième de p, on a $\xi^p = p$ où $p = [K : \mathbb{Q}]$, donc $\mathfrak{m} = \xi A$ est le seul idéal premier de A au-dessus de p et $e(\mathfrak{m}/p) = p$. En particulier, pour $p = 2$, on retrouve l'exemple $\mathbb{Z}[\sqrt{2}]$ donné en introduction.

(iii) L'anneau $\mathbb{Z}[i]$ des entiers de Gauss.

En effet, $i = \sqrt[2]{-1}$ et $-1 \equiv 3 \pmod 4$ (cas quadratique) ou encore $i = \sqrt[4]{1}$ et $4 = 2^2$ (cas cyclotomique!).

(iv) L'anneau $\mathbb{Z}[\sqrt{d}]$ où d est un entier sans facteurs carrés.

En effet, si $d \equiv 2$ ou $3 \pmod 4$, il s'agit de l'anneau des entiers de $\mathbb{Q}[\sqrt{d}]$. Par contre, lorsque $d \equiv 1 \pmod 4$, cela résulte de la remarque du §11 : si $\mathfrak{m}$ désigne un idéal maximal de A au-dessus de 2, $\mathbf{D}_{A_\mathfrak{m}} \neq \mathbf{\Delta}_{A_\mathfrak{m}}$.

Bibliographie

[1] D. Barsky, *Fonctions k-lipschitziennes sur un anneau local et polynômes à valeurs entières*, Bull. Soc. Math. France 101 (1973), 397–411.

[2] D. Brizolis, *Ideals in rings of integer-valued polynomials*, J. Reine Angew. Math. 285 (1976), 28–52.

[3] D. Brizolis and E. G. Straus, *A basis for the ring of doubly integer-valued polynomials*, ibid. 286/287 (1976), 187–195.

[4] P.-J. Cahen, *Polynômes à valeurs entières*, Canad. J. Math. 24 (1972), 747–754.

[5] —, *Polynômes et dérivées à valeurs entières*, Ann. Sci. Univ. Clermont-Ferrand Sér. Math. 10 (1975), 25-43.

[6] —, *Polynômes à valeurs entières sur un anneau non analytiquement irréductible*, J. Reine Angew. Math. 418 (1991), 131–137.

[7] —, *Integer-valued polynomials on a subset*, Trans. Amer. Math. Soc., à paraître.

[8] P.-J. Cahen et J.-L. Chabert, *Coefficients et valeurs d'un polynôme*, Bull. Sci. Math. 95 (1971), 295–304.

[9] P.-J. Cahen et Y. Haouat, *Polynômes, dérivées et différences finies divisées à valeurs entières sur un anneau de pseudo-valuation*, C. R. Acad. Sci. Paris Sér. I 306 (1988), 581–584.

[10] L. Carlitz, *A note on integral-valued polynomials*, Indag. Math. Ser. A 62 (1959), 294–299.

[11] J.-L. Chabert, *Anneaux de "polynômes à valeurs entières" et anneaux de Fatou*, Bull. Soc. Math. France 99 (1971), 273–283.

[12] —, *Les idéaux premiers de l'anneau des polynômes à valeurs entières*, J. Reine Angew. Math. 293/294 (1977), 275–283.

[13] —, *Polynômes à valeurs entières ainsi que leurs dérivées*, Ann. Sci. Univ. Clermont-Ferrand Sér. Math. 18 (1979), 47–64.

[14] N. G. de Bruijn, *Some classes of integer-valued functions*, Nederl. Akad. Wetensch. Proc. Ser. A 58 (1955), 363–367.

[15] R. Gilmer, W. Heinzer and D. Lantz, *The Noetherian property in rings of integer-valued polynomials*, Trans. Amer. Math. Soc., à paraître.

[16] J. Gregory, Lettre à John Collins du 23 novembre 1670, dans : *The Correspondence of Isaac Newton*, Cambridge Univ. Press, 1959, I, 45–49.

[17] Y. Haouat et F. Grazzini, *Polynômes et différences finies divisées*, C. R. Acad. Sci. Paris Sér. A 284 (1977), 1171–1173.
[18] —,—, *Différences finies divisées sur un anneau $S(2)$*, ibid. 286 (1978), 723–725.
[19] —,—, *Polynômes de Barsky*, Ann. Sci. Univ. Clermont-Ferrand Sér. Math. 18 (1979), 65–81.
[20] V. Laohakosol et P. Ubolsri, *A short note on integral-valued polynomials*, Southeast Asian Bull. Math. 4 (1980), 43–47.
[21] I. Newton, Lettre à John Smith du 8 mai 1675, dans : *Mathematical Papers*, Cambridge Univ. Press, 1967-1976, IV, 14–21.
[22] A. Ostrowski, *Über ganzwertige Polynome in algebraischen Zahlkörpern*, J. Reine Angew. Math. 149 (1919), 117–124.
[23] G. Pólya, *Über ganzwertige Polynome in algebraischen Zahlkörpern*, ibid., 97–116.
[24] K. Rogers and E. G. Straus, *Infinitely integer-valued polynomials over an algebraic number field*, Pacific J. Math. 118 (1985), 507–522.
[25] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris 1967.
[26] J.-P. Serre, *Corps locaux*, Hermann, Paris 1962.
[27] E. G. Straus, *On the polynomials whose derivatives have integral values at integers*, Proc. Amer. Math. Soc. 2 (1951), 24–27.
[28] C. G. Wagner, *Polynomials over* $\mathrm{GF}(q, x)$ *with integral-valued differences*, Arch. Math. (Basel) 27 (1976), 495–501.

76 RUE CHARLOT
75003 PARIS, FRANCE

Reçu le 18.12.1991 (2208)