Can. J. Math. Vol. **45** (1), 1993 pp. 6–21

POLYNÔMES À VALEURS ENTIÈRES ET BINÔMES DE FERMAT

JEAN-LUC CHABERT ET GILBERT GERBOUD

RESUME Soit A un anneau intègre de corps des fractions K et soit $A[X]_{\text{sub}} = \{P(X) \in K[X] \ , \ P(A) \subset A\}$ l'anneau des polynômes à valeurs entières sur A Lorsque la caractéristique de A est nulle, le A-module $A[X]_{\text{sub}}$ est contenu dans le A-module $\{P(X) \in K[X] \ , \ P(\mathbb{Z}) \subset A\}$ engendré par les polynômes binomiaux $B_n(X) = X(X-1) \quad (X-n+1)/n!$ Nous caractérisons ici les anneaux de Dedekind A pour lesquels ces A-modules sont égaux

Puis nous étudions la situation plus générale dans laquelle $A[X]_{\text{sub}} = \{P(X) \in K[X] \ , \ P(A_0) \subset A\}$ où A_0 désigne un anneau de Dedekind contenu dans A Ce sont alors des polynômes généralisant les binômes de Fermat $F_p(X) = (X^q - X)/p$ qui jouent le rôle central

ASTRACT Let A be a domain with quotient field K and let $A[X]_{\text{sub}} = \{P(X) \in K[X] \ , \ P(A) \subset A\}$ the ring of integer-valued polynomials over A When A is of characteristic zero, the A-module $A[X]_{\text{sub}}$ is contained in the A-module $\{P(X) \in K[X] \ , \ P(\mathbb{Z}) \subset A\}$ generated by the binomial polynomials $B_n(X) = X(X-1) \quad (X-n+1)/n!$ We characterize the Dedekind domains A for which these A-modules coincide

Then, we study a more general situation let A_0 be any Dedekind domain contained in A, the ring $A[X]_{\text{sub}}$ is included in the ring $\{P(X) \in K[X] \ , \ P(A_0) \subset A\}$ We give equivalent conditions for which these two rings coincide, making use of polynomials such that Fermat binomials $F_p(X) = (X^q - X)/p$

Introduction. Soit A un anneau intègre de corps des fractions K. On appelle polynôme à valeurs entières sur A tout polynôme à coefficients dans K qui prend sur A ses valeurs dans A.

Nous noterons $A[X]_{\text{sub}}$ l'ensemble des polynômes à valeurs entières sur A :

$$A[X]_{\text{sub}} = \{P(X) \in K[X] \ ; \ P(A) \subset A\}.$$

Il est clair que $A[X]_{\text{sub}}$ est un sous-anneau de $K[X]$ contenant $A[X]$, et qu'il peut être considéré comme un sous-module du A-module $K[X]$. Nous allons étudier ici à quelles conditions, portant sur l'anneau A, $A[X]_{\text{sub}}$ peut être engendré en tant que A-module ou en tant qu'anneau par certains types de polynômes simples comme les polynômes binomiaux $B_n(X) = X(X-1)\cdots(X-n+1)/n!$ ou les binômes de Fermat $F_p(X) = (X^q - X)/p$.

Reçu par les éditeurs le March 18, 1991

Classification de l'AMS par sujet 13B25, 13F05, 13F20, 11C08, 11S05

PREMIÈRE PARTIE : LES POLYNÔMES BINOMIAUX.

1. **Généralités.** Supposons que l'anneau A soit de caractéristique nulle et considérons les polynômes binomiaux suivants :

NOTATION 1.1. Posons $B_0(X) = 1$ et, pour tout entier $n > 0$,

$$B_n(X) = X(X-1)\cdots(X-n+1)/n!,$$

et notons $A[X]_{\text{bin}}$ le A-module libre engendré par les polynômes $B_n(X)$.

PROPOSITION 1.2. *Le A-module $A[X]_{\text{bin}}$ est aussi l'ensemble des polynômes :*

$$A[X]_{\text{bin}} = \{P(X) \in K[X] \; ; \; P(\mathbb{Z}) \subset A\}.$$

DÉMONSTRATION. Il est clair que les polynômes binomiaux prennent sur $\mathbb{Z}$ leurs valeurs dans $\mathbb{Z}$, donc dans A. Par conséquent $A[X]_{\text{bin}} \subset \{P(X) \in K[X] \; ; \; P(\mathbb{Z}) \subset A\}$.

Inversement, si $P(X)$ est un polynôme non nul de $K[X]$ tel que $P(\mathbb{Z})$ soit inclus dans A, alors, comme les polynômes binomiaux forment une base du K-espace vectoriel $K[X]$, nous pouvons écrire :

$$P(X) = t_0B_0(X) + t_1B_1(X) + \cdots + t_mB_m(X)$$

où m est le degré de P(X) et $t_0, t_1, \ldots, t_m$ sont des éléments de K. Mais, t_0 est un élément de A car $t_0 = P(0)$. De plus, si $t_0, \ldots, t_{q-1}$ $(0 < q \leq m)$ sont des éléments de A, alors

$$t_q = P(q) - t_0B_0(q) - \cdots - t_{q-1}B_{q-1}(q)$$

est aussi un élément de A. D'où la proposition.

Ceci montre en particulier que le A-module $A[X]_{\text{bin}}$ est aussi muni d'une structure d'anneau, et nous avons les inclusions :

$$A[X] \subset A[X]_{\text{sub}} \subset A[X]_{\text{bin}} \subset K[X].$$

On dispose déjà de nombreux résultats relatifs aux anneaux A tels que $A[X]_{\text{sub}} = A[X]$ (les anneaux substitutiels de [5], § 4 ; *cf.* aussi [7], § 2 ou [14]). Ici, nous nous intéressons à l'autre inclusion, au cas où $A[X]_{\text{sub}} = A[X]_{\text{bin}}$. Bien sûr, $\mathbb{Z}[X]_{\text{sub}} = \mathbb{Z}[X]_{\text{bin}}$. Nous allons donner des caractérisations des anneaux de Dedekind A pour lesquels cette égalité a lieu et notamment la suivante :

Tout nombre premier p, qui n'est pas inversible dans A, y est totalement décomposé, c'est-à-dire est produit d'idéaux maximaux de A de norme p deux à deux distincts.

Commençons par une remarque valable en toute généralité.

NOTATION 1.3. Pour tout entier $n \geq 0$, notons $I_n(A)$—ou plus simplement I_n si aucune confusion n'est à craindre—le sous-module du A-module K formé de 0 et des coefficients directeurs des polynômes à valeurs entières sur A de degré $\leq n$.

Définis en toute caractéristique, ces I_n sont des idéaux fractionnaires de A et on vérifie facilement que :

PROPOSITION 1.4. *Une suite $Q_0(X), Q_1(X), \ldots, Q_n(X), \ldots$ de polynômes à valeurs entières sur A, tels que* $\deg Q_n(X) = n$, *est une base du A-module* $A[X]_{\mathrm{sub}}$ *si et seulement si, quel que soit l'entier n, le coefficient directeur de* $Q_n(X)$ *engendre* I_n.

COROLLAIRE 1.5. *Si un anneau A de caractéristique nulle vérifie* $A[X]_{\mathrm{sub}} = A[X]_{\mathrm{bin}}$ *alors, pour tout entier* $n \geq 0$, $I_n = (1/n!)A$.

2. Caractérisation des anneaux de Dedekind A pour lesquels $A[X]_{\mathrm{sub}} = A[X]_{\mathrm{bin}}$.

P.-J. Cahen [3] a donné une autre description des idéaux fractionnaires I_n lorsque A est un anneau de Dedekind.

NOTATIONS 2.1. Notons $[q]$ la partie entière d'un nombre rationnel q. Si h et N désignent deux entiers naturels tels que $h > 0$ et $N > 1$, notons $v_N(h)$ l'exposant de la plus haute puissance de N qui divise h.

Si M désigne un idéal maximal de A, notons $N(M)$ sa norme, c'est-à-dire le cardinal (éventuellement infini) du corps résiduel A/M ; et si I désigne un idéal fractionnaire non nul de A, notons $v_M(I)$ l'exposant de M apparaissant dans la décomposition de I en produit d'idéaux maximaux de A.

Enfin, pour tout entier naturel n, posons

$$w_N(n) = \begin{cases} \sum_{h=1}^{n} v_N(h) = \sum_{r\geq 1}[\frac{n}{N^r}] & \text{si } N \text{ est un entier} > 1 \\ 0 & \text{si } N \text{ est un cardinal infini.} \end{cases}$$

PROPOSITION 2.2 (CAHEN [3], § 2). *Pour un anneau de Dedekind A, les idéaux fractionnaires* I_n *sont caractérisés par :* $v_M(I_n) = -w_{N(M)}(n)$, *pour tout idéal maximal M de A.*

Supposons désormais l'anneau A de caractéristique nulle.

LEMME 2.3. *Soit A un anneau de Dedekind de caractéristique nulle. Si un nombre premier p se décompose sous la forme :*

$$pA = M_1 \cdots M_d$$

où d est un entier > 0 *et* $M_1, \ldots, M_d$ *sont des idéaux maximaux de A de norme p deux à deux distincts, alors le binôme* $F_p(X) = (X^p - X)/p$ *est à valeurs entières sur A.*

DÉMONSTRATION. Soit a un élément de A et soit $i \in \{1, \ldots, d\}$. Comme A/M_i est un corps de cardinal p, nous avons $\bar{a}^p - \bar{a} = 0$ si $\bar{a}$ désigne la classe de a dans A/M_i. Donc $a^p - a$ est un élément de M_i. Par suite :

$$a^p - a \in M_1 \cap \cdots \cap M_d = M_1 \cdots M_d = pA.$$

Ainsi, quel que soit l'élément a de A, $F_p(a) = (a^p - a)/p$ est aussi un élément de A : $F_p(X)$ est un polynôme à valeurs entières sur A.

LEMME 2.4. *Soit A un anneau de Dedekind de caractéristique nulle. Si, quel que soit le nombre premier p, le binôme $F_p(X) = (X^p - X)/p$ est à valeurs entières sur A, alors :*

$$A[X]_{\mathrm{sub}} = A[X]_{\mathrm{bin}}.$$

DÉMONSTRATION. Les polynômes $B_0(X), B_1(X), \ldots, B_n(X), \ldots$ constituent évidemment une base de $\mathbb{Z}[X]_{\mathrm{sub}}$. Par ailleurs, nous savons construire une autre base de $\mathbb{Z}[X]_{\mathrm{sub}}$ formée de polynômes $Q_0(X), Q_1(X), \ldots, Q_n(X), \ldots$ qui sont obtenus par combinaisons linéaires à coefficients dans $\mathbb{Z}$ de produits d'itérés des binômes $F_p(X) = (X^p - X)/p$ ([8], § 2).

Si, donc, on suppose que, quel que soit le nombre premier p, $F_p(X)$ est un polynôme de $A[X]_{\mathrm{sub}}$, alors, par construction, les polynômes $Q_0(X), Q_1(X), \ldots, Q_n(X), \ldots$ sont à valeurs entières sur A et, par suite, il en est de même des polynômes $B_0(X), B_1(X), \ldots, B_n(X), \ldots$ qui se décomposent sur cette base : $A[X]_{\mathrm{bin}}$ est inclus dans $A[X]_{\mathrm{sub}}$, d'où le résultat puisque l'on a toujours l'autre inclusion.

THÉORÈME 2.5. *Soit A un anneau de Dedekind de caractéristique nulle. Les quatre propriétés suivantes sont équivalentes :*

(*a*) $A[X]_{\mathrm{sub}} = A[X]_{\mathrm{bin}}$ *;*

(*b*) *quel que soit l'entier $n \geq 0$, $I_n = (1/n!)A$;*

(*c*) *tout nombre premier p, qui n'est pas inversible dans A, se décompose sous la forme :*

$$pA = M_1 \cdots M_d$$

où d est un entier > 0 et $M_1, \ldots, M_d$ sont des idéaux maximaux de A de norme p deux à deux distincts ;

(*d*) *quel que soit le nombre premier p, le binôme $F_p(X) = (X^p - X)/p$ est à valeurs entières sur A.*

DÉMONSTRATION. L'implication (a) $\Rightarrow$ (b) résulte du Corollaire 1.5.

Montrons l'implication (b) $\Rightarrow$ (c). Supposons donc que, quel que soit l'entier $n \geq 0$, $I_n = (1/n!)A$ et soit p un nombre premier. Alors, $I_p = I_{p-1}.(1/p)A$, et par conséquent :

$$pA = I_{p-1}.I_p^{-1}.$$

Soit M un idéal maximal de A de norme N. On a :

$$v_M(pA) = v_M(I_{p-1}) - v_M(I_p)$$

c'est-à-dire (Proposition 2.2),

$$v_M(pA) = w_N(p) - w_N(p-1).$$

Revenons à la définition de w_N. Si $N > p$, $w_N(p) = w_N(p-1) = 0$, et donc $v_M(pA) = 0$. Si $N < p$, $w_N(p) = w_N(p-1) + v_N(p) = w_N(p-1)$, et donc $v_M(pA) = 0$. Ainsi, si $N \neq p$,

M n'intervient pas dans la décomposition de pA en produit d'idéaux maximaux de A. Et si $N = p$, alors $w_N(p) = 1$, $w_N(p-1) = 0$, et $v_M(pA) = 1$. D'où le (c).

Montrons l'implication (c) $\Rightarrow$ (d). Soit p un nombre premier. Si p est inversible dans A, $F_p(X) = (X_p - X)/p$ est un polynôme de $A[X]$ et donc de $A[X]_{\text{sub}}$. Et si p n'est pas inversible dans A, le Lemme 2.3 ci-dessus permet de conclure.

Enfin, l'implication (d) $\Rightarrow$ (a) n'est autre que le Lemme 2.4.

REMARQUE 2.6. Lorsque l'anneau A vérifie les conditions équivalentes du théorème précédent et que son corps des fractions K est algébrique sur $\mathbb{Q}$, K est un corps de nombres et l'entier d de la condition (c) n'est autre que le degré de l'extension $K/\mathbb{Q}$, il ne dépend donc pas du nombre permier p (*cf.* [13], V).

3. **Exemples.**

PROPOSITION 3.1. *Pour tout anneau d'entiers O d'un corps de nombres K distinct du corps $\mathbb{Q}$ des nombres rationnels, nous avons :*

$$O[X] \underset{\neq}{\subset} O[X]_{\text{sub}} \underset{\neq}{\subset} O[X]_{\text{bin}}.$$

DÉMONSTRATION. Les inclusions ont lieu en général ; il s'agit de montrer qu'ici elles sont strictes. Pour la deuxième, cela résulte de ce que, K étant distinct de $\mathbb{Q}$, il existe toujours des nombres premiers ramifiés dans O et donc l'assertion (c) du Théorème 2.5 n'est pas vérifiée. Pour la première, le résultat est classique ([3], [4], [5], [6], [7]). Il résulte par exemple de ce qu'il existe une infinité de nombres premiers p totalement décomposés, *i.e.*, tels que $pO = M_1 \cdots M_d$ où $M_1, \ldots, M_d$ sont des idéaux maximaux de O de norme p et deux à deux distincts (*cf.* [1], V, § 3). Pour un tel nombre premier p, le polynôme $F_p(X) = (X^p - X)/p$ appartient à $O[X]_{\text{sub}}$ d'après le Lemme 2.3, mais non à $O[X]$.

EXEMPLE 3.2. Soit O l'anneau des entiers d'un corps de nombres K de degré d. Soit T la partie multiplicative engendrée par les nombres premiers p qui ne sont pas totalement décomposés dans K et soit A le localisé $T^{-1}O$. Alors,

$$A[X]_{\text{sub}} = A[X]_{\text{bin}}.$$

En effet, tout nombre premier p qui n'est pas inversible dans A est totalement décomposé sous la forme $pA = M_1 \cdots M_d$ où $M_1, \ldots, M_d$ sont des idéaux maximaux de A de degré résiduel 1 deux à deux distincts. On sait d'ailleurs, on l'a dit, qu'il existe une infinité de tels nombres premiers.

Par exemple, pour l'anneau $O = \mathbb{Z}[\sqrt{-1}]$, T est engendré par l'ensemble des nombres premiers qui ne sont pas congrus à 1 modulo 4 (*cf.* [13], V).

EXEMPLE 3.3. L'anneau $A = \mathbb{Z}[(1 + \sqrt{17})/2]_{2\mathbb{Z}}$ vérifie :

$$A[X]_{\text{sub}} = A[X]_{\text{bin}}.$$

https://doi.org/10.4153/CJM-1993-002-8 Published online by Cambridge University Press

En effet, 2 est totalement décomposé dans l'anneau $\mathbb{Z}[(1+\sqrt{17})/2]$ des entiers du corps $\mathbb{Q}[\sqrt{17}]$.

EXEMPLE 3.4. L'anneau $A = \mathbb{Z}[\sqrt{7}]_{3\mathbb{Z}}$ vérifie :

$$A[X]_{\text{sub}} = A[X]_{\text{bin}}.$$

En effet, 3 est totalement décomposé dans l'anneau $\mathbb{Z}[\sqrt{7}]$ des entiers du corps $\mathbb{Q}[\sqrt{7}]$.

EXEMPLE 3.5. Soit p un nombre premier.
Si $\mathbb{Z}_p$ désigne l'anneau des entiers p-adiques, alors

$$\mathbb{Z}_p[X]_{\text{sub}} = \mathbb{Z}_p[X]_{\text{bin}}.$$

DEUXIÈME PARTIE : LES BINÔMES DE FERMAT.

4. **Généralités.** À propos de l'égalité :

$$\mathbb{Z}[X]_{\text{sub}} = \{P(X) \in \mathbb{Q}[X] \; ; P(\mathbb{Z}) \subset \mathbb{Z}\}.$$

on peut se poser deux questions correspondant à deux points de vue symétriques :

D'une part, dans quelle mesure peut-on restreindre l'ensemble en lequel on calcule les valeurs des polynômes? C'est en particulier la question qu'étudie R. Gilmer [10] lorsqu'il caractérise les parties S de $\mathbb{Z}$ telles que :

$$\mathbb{Z}[X]_{\text{sub}} = \{P(X) \in \mathbb{Q}[X] \; ; P(S) \subset \mathbb{Z}\}.$$

D'autre part, dans quelle mesure peut-on étendre l'ensemble dans lequel sont prises les valeurs des polynômes ? C'est en particulier la question étudiée dans la partie précédente lors de la caractérisation des anneaux de Dedekind A de caractéristique nulle tels que

$$A[X]_{\text{sub}} = \{P(X) \in K[X] \; ; P(\mathbb{Z}) \subset A\}.$$

Or, ces deux questions, qui en fait se recoupent, peuvent s'étudier sous des hypothèses très générales. Ainsi, nous obtenons des énoncés assez semblables à celui du Théorème 2.5 sans avoir à supposer A intégralement clos, ni même noethérien. L'anneau de base $\mathbb{Z}$ lui-même peut être remplacé par un anneau A_0 *a priori* quelconque. Les caractérisations sont intéressantes dans le cas où A_0 est un anneau principal, voire un anneau de Dedekind. Mais nous ne nous limiterons plus à la caractéristique nulle et pourrons prendre par exemple pour A_0 un anneau tel que $\mathbb{F}_q[T]$. Bien sûr les polynômes binomiaux $B_n(X)$ ne pourrons plus être considérés ; ce sont les analogues des polynômes $(X^p - X)/p$ qui joueront le rôle fondamental :

DEFINITION 4.1. A tout idéal premier principal pA_0 de A_0 de quotient de cardinal fini $N(p)$ associons le binôme de Fermat

$$F_p(X) = (X^{N(p)} - X)/p.$$

https://doi.org/10.4153/CJM-1993-002-8 Published online by Cambridge University Press

Notons que tout binôme de Fermat de l'anneau A_0 est un polynôme à valeurs entières sur A_0. En effet, l'image $\bar{a}$ de tout élément a de A_0 dans le corps fini A_0/pA_0 vérifie $\bar{a}^{N(p)} - \bar{a} = 0$ et donc $a^{N(p)} - a$ appartient à pA_0.

Posons-nous en toute généralité le problème de la substituabilité d'un anneau A_0 à un autre A :

HYPOTHESES ET NOTATIONS 4.2. Soient A_0 et A deux anneaux intègres tels que A_0 soit contenu dans A. Soient K_0 et K leurs corps des fractions respectifs.

DÉFINITION 4.3. Nous dirons que l'anneau A_0 est substituable à l'anneau A lorsque :

$$A[X]_{\text{sub}} = \{P(X) \in K[X] \; ; P(A_0) \subset A\}.$$

Si A_0 est substituable à A, alors tout binôme de Fermat relatif à l'anneau A_0 est à valeurs entières sur A. Nous allons voir dans quelle mesure cette condition est suffisante. Commençons par quelques assertions élémentaires.

PROPOSITION 4.4. *(i) Si A_0 est substituable à A, alors $A_0[X]_{\text{sub}}$ est inclus dans $A[X]_{\text{sub}}$.*

(ii) Si $A_0 \subset A_1 \subset A$ et si A_0 est substituable à A, alors A_1 est substituable à A.

(iii) Si K_1 est un corps compris entre K_0 et K et si A_0 est substituable à A, alors A_0 est substituable à $A_1 = A \cap K_1$.

(iv) Si A_0 est substituable à une famille d'anneaux A_j, alors A_0 est substituable à l'intersection A des anneaux A_j.

(v) Si A est la fermeture intégrale de A_0 dans K, pour que A_0 soit substituable à A il faut et il suffit que A_0 soit substituable à $A \cap K_0$ et que $A \cap K_0$ soit substituable à A.

DÉMONSTRATION. Toutes ces assertions sont de vérification immédiate. Seule la condition suffisante de l'assertion (v) nécessite une explication. Soit donc $P(X)$ dans $K[X]$ tel que $P(A_0)$ soit inclus dans A. Comme A est entier sur A_0, alors K est algébrique sur K_0, donc $P(X)$ est entier sur $K_0[X]$ et nous avons la relation :

$$P^n + Q_{n-1}P^{n-1} + \cdots + Q_1 P + Q_0 = 0.$$

Les $Q_\iota(X)$ sont des fonctions symétriques des conjugués de $P(X)$; par suite, pour tout élément a de A_0, les $Q_\iota(a)$ sont des fonctions symétriques des conjugués de $P(a)$ et donc appartiennent à $A \cap K_0$. Compte tenu des hypothèses, puisque $Q_\iota(A_0)$ est contenu dans $A \cap K_0$, $Q_\iota(A \cap K_0)$ est contenu dans $A \cap K_0$ et donc $Q_\iota(A)$ est contenu dans A. Ainsi, pour tout élément x de A, $P(x)$ est entier sur A c'est-à-dire appartient à A.

Pour effectuer une étude plus fine, ramenons nous au cas local à l'aide de :

PROPOSITION 4.5 (CAHEN ET CHABERT [5], § 3). *Pour toute partie multiplicative S de A_0, tout polynôme $P(X)$ appartenant à $K[X]$, tel que $P(A_0) \subset A$, vérifie aussi $P(S^{-1}A_0) \subset S^{-1}A$.*

COROLLAIRE 4.6. *Un anneau A_0 est substituable à tous ses localisés. Un anneau de Prüfer A_0 est substituable à tout anneau A compris entre A_0 et K_0.*

A cet effet, on notera que lorsque A_0 est de Prüfer, les anneaux A compris entre A_0 et K_0 sont tous des intersections de localisés de A_0.

Plus généralement ([5], § 3) : l'anneau A_0 est substituable à tout anneau A, compris entre A_0 et K_0, qui est plat sur A_0.

COROLLAIRE 4.7. *(i) Si, pour tout idéal maximal m de A_0, $(A_0)_m$ est substituable à A_m, alors A_0 est substituable à A.*

(ii) Si, pour tout idéal maximal M de A, $(A_0)_{M\cap A_0}$ est substituable à A_M, alors A_0 est substituable à A.

DÉMONSTRATION. Vérifions par exemple la première assertion. Soit $P(X)$ dans $K[X]$ tel que $P(A_0)$ soit inclus dans A. Alors, d'après la Proposition 4.5, pour tout idéal maximal m de A_0, $P\big((A_0)_m\big)$ est inclus dans A_m. Par suite, $P(A_m)$ est inclus dans A_m d'après l'hypothèse et donc $P(A)$ est inclus dans $A = \bigcap_m A_m$.

Pour énoncer une réciproque du Corollaire 4.7, nous devons introduire une hypothèse noethérienne :

PROPOSITION 4.8. *Supposons l'anneau A_0 noethérien. Si l'anneau A_0 est substituable à l'anneau A, alors :*

(i) pour tout idéal maximal m de A_0, $(A_0)_m$ est substituable à A_m.

(ii) pour tout idéal maximal M de A, $(A_0)_{M\cap A_0}$ est substituable à A_M.

DÉMONSTRATION. Montrons par exemple la première assertion. Soit $P(X)$ dans $K[X]$ tel que $P\big((A_0)_m\big)$ soit inclus dans A_m. Le A_0-module engendré par les valeurs de $P(X)$ sur A_0 est de type fini, puisqu'il est contenu dans le A_0-module engendré par les coefficients de $P(X)$. Il existe donc t dans $A_0 - m$ tel que $tP(A_0)$ soit inclus dans A. Par suite, avec l'hypothèse, $tP(A)$ est inclus dans A ; $P(A)$ est inclus dans A_m et finalement $P(A_m)$ est inclus dans A_m.

Ainsi le Corollaire 4.7 et la Proposition 4.8 ramènent notre étude au cas d'anneaux locaux.

5. **Étude locale.** Remarquons tout de suite qu'un corps infini est substituable à tout anneau qui le contient et que plus généralement :

PROPOSITION 5.1 (CAHEN ET CHABERT [5], § 2). *Un anneau local de corps résiduel infini est substituable à tout anneau qui le contient.*

Pour notre étude, nous pouvons donc supposer A_0 non seulement local, mais de corps résiduel fini.

HYPOTHESES ET NOTATIONS 5.2. L'anneau A_0 est un anneau intègre, de corps des fractions K_0, local, d'idéal maximal m et de corps résiduel de cardinal fini q. L'anneau A est un anneau intègre, contenant A_0, de corps des fractions K, local, d'idéal maximal M, dominant m.

PROPOSITION 5.3. *Supposons l'idéal maximal m de A_0 principal engendré par un élément p. Alors, les conditions suivantes sont équivalentes :*

(i) A_0 est substituable à A ;

(ii) le binôme de Fermat $F_p(X) = (X^q - X)/p$ appartient à $A[X]_{\text{sub}}$;

(iii) $mA = M$ et $A_0/m = A/M$.

DÉMONSTRATION. On sait que $F_p(X)$ est à valeurs entières sur A_0 et donc, si A_0 est substituable à A, $F_p(X)$ est aussi à valeurs entières sur A. D'où l'implication (i) $\Rightarrow$ (ii).

A présent, supposons vérifiée la condition (ii). Pour tout élément a de A, $(a^q - a)/p$ appartient à A, donc $a^q - a$ appartient à $pA = mA \subset M$. Ainsi, le cardinal de A/M est majoré par q ; comme A_0/m qui est de cardinal q s'y injecte, on a bien l'isomorphisme de (iii). Par ailleurs, si a appartient à M, $a^{q-1} - 1 = u$ est inversible dans A. Or, $ua = a^q - a$ appartient à pA, donc a appartient à pA, M est inclus dans pA et $M = pA$, ce qui achève de montrer (iii).

Pour montrer que (iii) implique (i), rappelons d'abord un résultat bien connu lorsque A est un anneau de valuation discrète :

LEMME 5.4 (CHABERT [6], III, § 5, n°4). *Supposons l'idéal maximal M de l'anneau local A principal et de corps résiduel de cardinal fini q. Soit p un générateur de M et soit $a_0, a_1, \ldots, a_{q-1}$ un système de représentants de A modulo M. Définissons alors des éléments a_r par :*

$$a_r = a_{r_0} + a_{r_1}p + \cdots + a_{r_k}p^k$$

où

$$r = r_0 + r_1 q + \cdots + r_k q^k$$

est l'écriture de l'entier r en base q. Pour qu'un polynôme $Q(X)$ de $K[X]$ appartienne à $A[X]_{\text{sub}}$ il faut et il suffit que $Q(a_r)$ appartienne à A pour tout $r \in \{0, 1, \ldots, \deg Q(X)\}$.

Supposons donc les conditions (iii) de la Proposition 5.3 réalisées. L'élément p et les représentants $a_0, a_1, \ldots, a_{q-1}$ peuvent être choisis dans A_0, les a_r construits sont alors des éléments de A_0. Par suite, $Q(A)$ est inclus dans A dès que $Q(A_0)$ est inclus dans A autrement dit A_0 est substituable à A, ce qui achève de montrer la proposition.

Dans le cas où A est supposé noethérien, cette réciproque résultera aussi de la proposition générale :

PROPOSITION 5.5 (CHABERT [6], III, § 5, n°1). *Supposons l'anneau A noethérien. Si $mA = M$ et $A_0/m = A/M$, alors A_0 est substituable à A.*

DÉMONSTRATION. Notons que les deux conditions de l'hypothèse peuvent se condenser en :

$$A = A_0 + mA.$$

Il est clair qu'elles impliquent cette égalité ; réciproquement, si $A = A_0 + mA$ alors, d'une part, nous avons *a fortiori* $A = A_0 + M$, d'où $A_0/m = A/M$ et, d'autre part,

$$M \subset (M \cap A_0) + mA = mA$$

d'où $mA = M$ puisqu'il est bien évident que $mA \subset M$.

Montrons, par récurrence sur n, que :

$$M^n = m^n + M^{n+1}.$$

Par hypothèse, $A = A_0 + M$ et la relation est vraie pour $n = 0$. Supposons-la vraie pour n. Alors :

$$M^{n+1} = mA.M^n = m.M^n = m.(m^n + M^{n+1}) = m^{n+1} + m.M^{n+1} = m^{n+1} + M^{n+2}.$$

Par suite :

$$A = A_0 + M = A_0 + M^2 = \cdots = A_0 + M^n = \cdots.$$

Soit $P(X)$ dans $K[X]$ tel que $P(A_0)$ soit inclus dans A et soit d un élément non nul de A tel que $dP(X)$ appartienne à $A[X]$. Fixons x dans A. Pour tout entier n, il existe a_n dans A_0 tel que $x - a_n$ appartienne à M^n. Ainsi, $d\big(P(x) - P(a_n)\big)$ appartient à M^n. Or, $P(a_n)$ appartient à A, donc $dP(x)$ appartient à $dA + M^n$. Ceci ayant lieu pour tout entier n,

$$dP(x) \in \bigcap_n (dA + M^n) = dA$$

puisque A est noethérien local d'idéal maximal M ([2], III, § 3). Ainsi, $P(x)$ appartient à A. Ceci ayant lieu pour tout x dans A, $P(X)$ est à valeurs entières sur A, ce qui achève la preuve.

Ainsi, pour tout entier naturel n, A_0 contient un système complet de représentants de A modulo M^n. Il s'agit de la condition de R. Gilmer sur sa partie S (*cf.* Proposition 6.2).

Nous retrouvons aussi le résultat connu suivant :

COROLLAIRE 5.6. *Si A_0 est noethérien, alors il est substituable à son complété pour la topologie m-adique (lorsque ce dernier est intègre).*

En effet, tout polynôme à valeurs entières sur un anneau noethérien A_0 est une fonction uniformément continue pour la topologie m-adique de A_0 dans A_0 [7].

EXEMPLE 5.7. Soient $A_0 = \mathbb{Z}[\sqrt{17}]$ et $A = \mathbb{Z}[(1 + \sqrt{17})/2]$. On sait que A est l'anneau des entiers de $\mathbb{Q}[\sqrt{17}]$, que l'idéal $2A$ y est décomposé en produit de deux idéaux maximaux M_1 et M_2 de norme 2, alors que le sous-anneau A_0 ne possède qu'un idéal maximal m au dessus de 2. L'anneau $\mathbb{Z}_{2\mathbb{Z}}$ est substituable à l'anneau $A_{2\mathbb{Z}}$ alors qu'il n'est pas substituable à l'anneau $(A_0)_{2\mathbb{Z}}$, car $2(A_0)_{2\mathbb{Z}}$ est distinct de $m(A_0)_{2\mathbb{Z}}$.

6. **Globalisation.** Les anneaux A_0 et A ne sont plus supposés locaux. Nous revenons aux notations générales du paragraphe 1.

PROPOSITION 6.1. *Supposons l'anneau A_0 de Dedekind. Pour que A_0 soit substituable à A il faut et il suffit que, pour tout idéal maximal m de A_0 de corps résiduel fini et tout idéal maximal M de A au-dessus de m, on ait :*

$$mA_M = MA_M \text{ et } A_0/m = A/M.$$

Cela résulte du Corollaire 4.7 et des Propositions 4.8, 5.1 et 5.3 : le corollaire et la première proposition ramènent le problème au cas local, la deuxième proposition au cas où A_0 a un corps résiduel fini et la troisième s'applique enfin puisque A_0 est alors principal.

A titre de comparaison, rappelons :

PROPOSITION 6.2 (GILMER [10], APPENDICE). *Supposons que A soit un anneau de Dedekind et soit S une partie de A. Alors $A[X]_{\mathrm{sub}} = \{P(X) \in K[X]\ ;\ P(S) \subset A\}$ si, et seulement si, pour tout idéal maximal M de A et pour tout entier naturel n, S contient un système complet de représentants de A modulo M^n.*

Lorsque A est un anneau noethérien, nous avons encore une condition suffisante :

PROPOSITION 6.3. *Supposons l'anneau A noethérien. Pour que A_0 soit substituable à A il suffit que, pour tout idéal maximal m de A_0 de corps résiduel fini et tout idéal maximal M de A au-dessus de m, on ait $mA_M = MA_M$ et $A_0/m = A/M$.*

Cela résulte du Corollaire 4.7 et des Propositions 5.1 et 5.5.

EXEMPLE 6.4. L'anneau $A_0 = \mathbb{Z}[\sqrt{17}]$ est substituable à l'anneau $A = \mathbb{Z}[(1+\sqrt{17})/2]$.

En effet, pour tout nombre premier impair p, $(A_0)_{p\mathbb{Z}} = A_{p\mathbb{Z}}$ et, pour $p = 2$, $(A_0)_{2\mathbb{Z}}$ est substituable à $A_{2\mathbb{Z}}$ d'après l'exemple 5.7.

La condition énoncée aux Propositions 6.1 et 6.3 possède des équivalents selon les hypothèses supplémentaires formulées sur A_0 ou sur A. Ainsi :

PROPOSITION 6.5. *Supposons l'anneau A noethérien de dimension 1. Soit m un idéal maximal de A_0 de norme q. Les assertions suivantes sont équivalentes :*

(i) pour tout idéal maximal M de A au-dessus de m, $mA_M = MA_M$ et $A_0/m = A/M$.

(ii) l'idéal mA est le produit des idéaux maximaux de A au-dessus de m et ceux-ci sont de norme q.

DÉMONSTRATION. Montrons l'implication (i) $\Rightarrow$ (ii) : puisque A est noethérien de dimension 1, les idéaux premiers de A contenant m sont en nombre fini ; soit $N = M_1 \cdots M_r$ l'idéal de A produit des idéaux maximaux de A au-dessus de m. Soit M un idéal maximal de A. Si M ne contient pas m, $mA_M = A_M = NA_M$. Si $M = M_j$, $mA_{M_j} = M_jA_{M_j} = NA_{M_j}$. Donc, $N = mA$.

Enfin, montrons l'implication (ii) $\Rightarrow$ (i) : par hypothèse $mA = M_1 \cdots M_r$ et, pour $j \in \{1, \ldots, r\}$, M_j a pour norme q. Ainsi, tout idéal maximal M de A au-dessus de m est un M_j, A/M a pour cardinal q, donc il est isomorphe à A_0/m puisque A_0/m s'injecte dans A/M et a déjà pour cardinal q. Enfin, la relation $mA_M = MA_M$ se déduit par localisation en M de la relation initiale.

THÉORÈME 6.6. *Supposons que l'anneau A_0 soit principal. Pour que A_0 soit substituable à A il faut et il suffit que, pour tout élément p irréductible dans A_0, de norme q et non inversible dans A, les assertions équivalentes suivantes soient vérifiées :*

(*i*) *tout idéal maximal* M *de* A *au-dessus de* pA_0 *est engendré par* p *dans* A_M *et a pour norme* q *;*

(*ii*) *le binôme de Fermat* $F_p(X) = (X^q - X)/p$ *est à valeurs entières sur* A.

Cela résulte du Corollaire 4.7 et des Propositions 4.8, 5.1 et 5.3.

7. **Substituabilité et binômes de Fermat généralisés.** En fait, le phénomène observé au Théorème 6. 6 a lieu dans un cadre un peu plus général que celui des anneaux principaux.

DÉFINITION 7.1 (PÓLYA [12], § 1). On dit que le A_0-module $A_0[X]_{\mathrm{sub}}$ possède une base régulière s'il possède une base formée de polynômes de degrés tous distincts.

On sait qu'il en est ainsi si et seulement si les idéaux fractionnaires $I_n(A_0)$ définis dans la première partie sont principaux ([12], § 2 et [3], § 2). En particulier :

PROPOSITION 7.2 (OSTROWSKI [11] ET CAHEN [4], V, § 2). *Lorsque* A_0 *est un anneau de Dedekind, le* A_0*-module* $A_0[X]_{\mathrm{sub}}$ *possède une base régulière si et seulement si le produit des idéaux maximaux de* A_0 *de même norme finie* q *est un idéal principal, quel que soit l'entier* $q > 1$.

De plus, si l'on note $s(q)$ un générateur de cet idéal principal, l'idéal fractionnaire principal $I_n(A_0)$ est de la forme $(1/a_n)A_0$ où $a_0 = a_1 = 1$ et, pour tout entier $n > 1$:

$$a_n = \prod_{1<q\leq n} s(q)^{w_q(n)} \quad (\textit{cf.}\ \text{Notation } 2.1).$$

Introduisons alors de nouveaux binômes de Fermat :

NOTATION 7.3. Si A_0 est un anneau de Dedekind tel que, quel que soit l'entier $q > 1$, le produit des idéaux maximaux de A_0 de norme q est un idéal principal engendré par un élément $s(q)$ alors nous associons à tout entier $q > 1$ le binôme de Fermat généralisé :

$$F_{s(q)}(X) = (X^q - X)/s(q).$$

Lorsque q n'est la norme d'aucun idéal maximal de A_0, on peut poser $s(q) = 1$ et $F_{s(q)}(X) = X^q - X$.

Ce polynôme est encore un polynôme à valeurs entières sur A_0. En effet, si $s(q)A_0 = m_1 \cdots m_r$ où les m_i sont les idéaux maximaux de A_0 de norme q, pour tout a dans A_0, $a^q - a$ appartient à tous les idéaux m_i, donc à leur produit, c'est-à-dire à $s(q)A_0$.

EXEMPLE 7.4. Lorsque $A_0 = \mathbb{Z}[\sqrt{-1}]$, les binômes de Fermat généralisés sont les polynômes $(X^2 - X)/(1 + \sqrt{-1})$ pour la norme 2, $(X^p - X)/p$ où p désigne un nombre premier congru à 1 modulo 4 et $(X^{p^2} - X)/p$ où p désigne un nombre premier congru à 3 modulo 4.

Lorsque A_0 est principal, le produit des idéaux maximaux de A_0 de norme q est bien sûr principal et pour caractériser la substituabilité, il suffit de considérer, pour tous les entiers $q > 1$, les binômes de Fermat généralisés correspondants. En effet :

https://doi.org/10.4153/CJM-1993-002-8 Published online by Cambridge University Press

PROPOSITION 7.5. *Supposons A_0 principal et soit un entier $q > 1$. Les propriétés suivantes sont équivalentes :*

(i) quel que soit l'élément irréductible p de A_0 de norme q, le binôme de Fermat $F_p(X) = (X^q - X)/p$ est à valeurs entières sur A ;

(ii) le binôme de Fermat généralisé $F_{s(q)}(X) = (X^q - X)/s(q)$ relatif à A_0 est à valeurs entières sur A.

DÉMONSTRATION. Notons $p_1A_0, p_2A_0, \ldots, p_rA_0$ les idéaux maximaux de A_0 de norme q : $s(q) = up_1p_2\cdots p_r$ où u est une unité de A_0. Supposons (i), alors, pour tout élément a de A, $a^q - a$ appartient à p_jA quel que soit j et, par conséquent :

$$a^q - a \in p_1A \cap p_2A \cap \cdots \cap p_rA = p_1A.p_2A\cdots p_rA = s(q)A,$$

car les éléments $p_1, p_2, \ldots, p_r$, étrangers deux à deux dans A_0, le sont encore dans A. Ainsi, le binôme de Fermat généralisé relatif à A_0, $F_{s(q)}(X) = (X^q - X)/s(q)$, est à valeurs entières sur A.

Réciproquement, supposons (ii) et soit p un élément irréductible de A_0 de norme q. Il est clair que p divise $s(q)$ et donc que, le binôme $F_{s(q)}(X) = (X^q - X)/s(q)$ étant à valeurs entières sur A, il en est de même du binôme $F_p(X) = (X^q - X)/p$.

Plus généralement :

PROPOSITION 7.6. *Supposons que A_0 soit un anneau de Dedekind tel que, pour tout entier $q > 1$, le produit des idéaux maximaux de norme q soit principal. Pour que A_0 soit substituable à A il faut et il suffit que les binômes de Fermat généralisés :*

$$F_{s(q)}(X) = (X^q - X)/s(q)$$

relatifs à A_0 soient à valeurs entières sur A.

DÉMONSTRATION. La condition est évidemment nécessaire puisque $F_{s(q)}(X)$ est à valeurs entières sur A_0. Réciproquement, soient m un idéal maximal de A_0 et M un idéal maximal de A au-dessus de m. Si A/m est infini, alors $(A_0)_m$ est substituable à A_M d'après la Proposition 5. 1. Supposons A/m de cardinal fini q. Le binôme de Fermat $(X^q - X)/s(q)$ est à valeurs entières sur A par hypothèse, donc aussi sur A_M d'après la Proposition 4.5. Par suite, $(A_0)_m$ est substituable à A_M d'après la Proposition 5.3 puisque $(A_0)_m$ est un anneau de valuation discrète d'uniformisante l'élément $s(q)$ de A_0. On conclut avec le Corollaire 4.7, la substituabilité ayant lieu localement.

Les Propositions 6.1, 6.3, 6.5, 7.6 et le Théorème 6.6 généralisent chacun à leur façon le Théorème 2.5. Donnons pour terminer un énoncé dans le cas particulier des couples d'anneaux de Dedekind de caractéristique quelconque, énoncé tout à fait calqué sur celui du Théorème 2.5.

THÉORÈME 7.7. *Supposons que A_0 et A soient deux anneaux de Dedekind et que le A_0-module $A_0[X]_{\mathrm{sub}}$ admette une base régulière. Alors les six propriétés suivantes sont équivalentes :*

(a) *l'anneau A_0 est substituable à l'anneau A c'est-à-dire*

$$A[X]_{\mathrm{sub}} = \{P(X) \in K[X] \; ; \; P(A_0) \subset A\} \; ;$$

(b) *quel que soit l'entier $n \geq 0$,*

$$I_n(A) = I_n(A_0).A \; ;$$

(c) *quel que soit l'entier $q > 1$, le produit des idéaux maximaux de A de norme q est l'idéal principal de A engendré par l'élément $s(q)$ de A_0 ;*

(d) *quel que soit l'entier $q > 1$, le binôme de Fermat généralisé $F_{s(q)}(X) = (X^q - X)/s(q)$ relatif à l'anneau A_0 est à valeurs entières sur A ;*

(e) *toute base régulière du A_0-module $A_0[X]_{\mathrm{sub}}$ est une base (régulière) du A-module $A[X]_{\mathrm{sub}}$;*

(f) *une base régulière du A_0-module $A_0[X]_{\mathrm{sub}}$ est une base (régulière) du A-module $A[X]_{\mathrm{sub}}$.*

DÉMONSTRATION. Nous allons montrer successivement l'équivalence des propriétés (b) et (c) puis la chaîne d'implications (a) $\Rightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (a), ce qui nous donnera l'équivalence des quatre propriétés (a), (b), (c) et (d), et enfin la chaine d'implications (b) $\Rightarrow$ (e) $\Rightarrow$ (f) $\Rightarrow$ (b), ce qui achèvera la démonstration.

Montrons l'implication (b) $\Rightarrow$ (c) par récurrence sur q. D'après la Proposition 2.2 :

$$I_q(A) = \prod_M M^{vM(Iq(A))} = \prod_M M^{-wN(M)(q)} = \prod_{2 \leq r \leq q} \Big[\prod_{N(M)=r} M\Big]^{-w_r(q)}$$

et, donc,

$$I_q(A) = \Big[\prod_{N(M)=q} M\Big]^{-1} \prod_{2 \leq r \leq q-1} \Big[\prod_{N(M)=r} M\Big]^{-w_r(q)}.$$

Pour $q = 2$:

$$\prod_{N(M)=2} M = I_2(A)^{-1} = a_2 A = s(2)A.$$

Supposons l'hypothèse de récurrence vérifiée pour $r = 2, \ldots, q-1$. Alors,

$$I_q(A) = \Big[\prod_{N(M)=q} M\Big]^{-1} . \prod_{2 \leq r \leq q-1} [s(r)A]^{-w_r(q)}.$$

Mais pour l'anneau A_0, nous avons :

$$I_q(A_0) = [s(q)A_0]^{-1} . \prod_{2 \leq r \leq q-1} [s(r)A_0]^{-w_r(q)}.$$

De l'égalité $I_q(A) = I_q(A_0).A$, nous déduisons finalement :

$$\prod_{N(M)=q} M = s(q)A.$$

L'implication (c) $\Rightarrow$ (b) résulte de ce que, sous l'hypothèse (c) et d'après la Proposition 7.2, le A-module $A[X]_{\mathrm{sub}}$ admet une base régulière et $I_n(A) = (1/a_n)A$ où

$$a_n = \prod_{1<q\leq n} s(q)^{w_q(n)}$$

est défini à partir des éléments $s(q)$ qui appartiennent à A_0.

Les propriétés (b) et (c) sont donc équivalentes.

Montrons l'implication (a) $\Rightarrow$ (c). Soit $q > 1$, alors $s(q)A_0 = m_1 \cdots m_r$ où $m_1, \ldots, m_r$ sont les idéaux maximaux de A_0 de norme q. D'après la Proposition 6.1, les idéaux maximaux de A de norme q sont nécessairement au-dessus des idéaux maximaux de A_0 de norme q et, d'après la Proposition 6.5, le produit des idéaux maximaux M de A au-dessus d'un idéal maximal fixé m de A_0 est égal à mA ; par suite, le produit des idéaux maximaux M de A de norme q est égal au produit $m_1A \cdots m_rA = s(q)A$.

L'implication (c) $\Rightarrow$ (d) résulte de ce que, sous l'hypothèse (c), le binôme de Fermat généralisé $F_{s(q)}(X)$ relatif à A_0 est aussi relatif à A, donc est à valeurs entières sur A.

Enfin, l'implication (d) $\Rightarrow$ (a) résulte de la Proposition 7.6.

Les propriétés (a), (b), (c) et (d) sont donc équivalentes.

Montrons, l'implication (b) $\Rightarrow$ (e). Soit $Q_0(X), Q_1(X), \ldots, Q_n(X), \ldots$ une base régulière de $A_0[X]_{\mathrm{sub}}$. Pour tout entier n, le polynôme $Q_n(X)$ est de degré n, il vérifie $Q_n(A_0) \subset A_0$ et son coefficient directeur engendre l'idéal $I_n(A_0)$ de A_0. D'après (a), qui est équivalent à (b), $Q_n(X)$ vérifie aussi $Q_n(A) \subset A$ et, d'après (b), son coefficient directeur engendre l'idéal $I_n(A)$ de A. La suite $Q_0(X), Q_1(X), \ldots, Q_n(X), \ldots$ est donc aussi une base régulière de $A[X]_{\mathrm{sub}}$.

L'implication (e) $\Rightarrow$ (f) est évidente.

Montrons, enfin, l'implication (f) $\Rightarrow$ (b). Soit $Q_0(X), Q_1(X), \ldots, Q_n(X), \ldots$ une base régulière de $A_0[X]_{\mathrm{sub}}$ qui est aussi une base régulière de $A[X]_{\mathrm{sub}}$. Pour tout entier n, d'après la Proposition 1.4, le coefficient directeur de $Q_n(X)$ engendre l'idéal $I_n(A_0)$ de A_0 et l'idéal $I_n(A)$ de A ; c'est donc que $I_n(A) = I_n(A_0).A$.

RÉFÉRENCES

1. Z I Borevitch et I R Chafarevitch, *Théorie des Nombres*, Gauthier-Villars, Paris, 1967

2. N Bourbaki, *Algèbre commutative*, Hermann, Paris, 1961

3. P-J Cahen, *Polynômes à valeurs entières*, Can J Math **24**(1972), 747–754

4. ———, *Polynômes à valeurs entières*, Thèse, Université Paris XI, Orsay, juin 1973

5. P-J Cahen et J -L Chabert, *Coefficients et valeurs d'un polynôme*, Bull Sci Math (2e) **95**(1971), 295–304

6. J -L Chabert, *Polynômes à valeurs entieres et extensions de Fatou*, Thèse, Université Paris XI, Orsay, mai 1973

7. ———, *Les idéaux premiers de l'anneau des polynômes a valeurs entières*, J reine angew Math **303/304**(1978), 366–378

8. G Gerboud, *Exemples d'anneaux A pour lesquels* $(\binom{X}{n})_{n\in N}$ *est une base du A-module des polynômes a valeurs entières sur A*, C R Acad Sci Paris (I) **307**(1988), 1–4

9. ———, *Construction, sur un anneau de Dedekind, d'une base régulière de polynômes à valeurs entieres*, Manuscripta Math **65**(1989), 167–179

10. R Gilmer, *Sets that determine integer-valued polynomials*, J Number Theory **33**(1989), 95–100

11. A Ostrowski, *Uber ganzwertige Polynome in algebraischen Zahlkorpern*, J reine angew Math **149**(1919), 117–124

https://doi.org/10.4153/CJM-1993-002-8 Published online by Cambridge University Press

12. G Polya, *Uber ganzwertige Polynome in algebraischen Zahlkorpern*, J reine angew Math **149**(1919), 97–116

13. P Samuel, *Theorie algebrique des Nombres*, Hermann, Paris, 1967

14. F Shibata, T Sugatani et K Yoshida, *Note on rings of integral valued polynomials*, C R Math rep Acad Sci Canada **8**(1986), 297–301

Institut Superieur des Sciences et Techniques
Universite de Picardie
48 rue Raspail
B P 422
02109 Saint Quentin Cedex
France

Institut Universitaire de Formation des Maîtres de l Academie d Amiens
51 boulevard de Châteaudun
80044 Amiens Cedex 1
France