RENDICONTI DEL CIRCOLO MATEMATICO DI PALERMO
Serie II, Tomo XLIII (1994), pp. 51-70

SUR LE THEOREME DE STONE-WEIERSTRASS EN ALGEBRE COMMUTATIVE

JEAN-LUC CHABERT

Résumé

Nous montrons que, dans la recherche d'une formulation du théorème d'approximation polynomiale de Weierstrass dans le cadre de l'Algèbre commutative, les conditions suffisantes obtenues par Cahen, Grazzini et Haouat s'avèrent essentiellement les plus générales possibles. Plus précisément, soient A un anneau nœthérien et I un idéal propre de A tel que A soit séparé pour la topologie I-adique. Notons $\hat{A}$ le complété de A et $C(\hat{A}, \hat{A})$ l'anneau des fonctions continues de $\hat{A}$ dans $\hat{A}$, muni de la topologie de la convergence uniforme. Les fonctions polynomiales constituent un sous-ensemble dense dans $C(\hat{A}, \hat{A})$ si et seulement si le radical de I est un idéal maximal m de A et le localisé A_m est un anneau de dimension 1, de corps résiduel fini et analytiquement irréductible.

Abstract

We show that the sufficient conditions given by Cahen, Grazzini and Haouat for a version of the Stone-Weierstrass theorem in commutative algebra are the widest. More precisely, let A be a Noetherian ring and I a proper ideal of A such that A is Hausdorff with respect to the I-adic topology. Note $\hat{A}$ the completion of A and $C(\hat{A}, \hat{A})$ the ring of continuous functions from $\hat{A}$ to $\hat{A}$ with uniform convergence topology. The subset of polynomial functions is dense in $C(\hat{A}, \hat{A})$ if and only if the radical of I is a maximal ideal m of A and the local ring A_m is a one-dimensional analytically irreducible domain with finite residue field.

1. Introduction.

Nous désirons donner une version générale du théorème de Stone-Weierstrass dans le cadre de l'algèbre commutative. Commençons par rappeler la version initiale du théorème de Stone-Weierstrass, c'est-à-dire le théorème d'approximation polynomiale:

PROPOSITION 1.1. (Weierstrass [15], prop. B). *L'anneau* $\mathbb{R}[X]$ *est dense dans l'anneau* $C([0,1],\mathbb{R})$ *muni de la topologie de la convergence uniforme.*

Rappelons aussi la traduction p-adique:

PROPOSITION 1.2. (Dieudonné [7]). *Toute fonction continue d'une partie compacte du complété* p*-adique* $\mathbb{Q}_p$ *de* $\mathbb{Q}$ *dans lui-même peut être approchée uniformément par des polynômes à coefficients dans* $\mathbb{Q}_p$.

On peut en particulier prendre pour partie compacte l'anneau $\mathbb{Z}_p$ des entiers p-adiques. Si l'on remplace le corps $\mathbb{Q}_p$ de l'ensemble d'arrivée par un anneau topologique, $\mathbb{Z}_p$ par exemple, on a l'énoncé:

PROPOSITION 1.3. (Malher [10]). *L'anneau des polynômes à valeurs entières sur* $\mathbb{Z}$ *est dense dans l'anneau* $C(\mathbb{Z}_p,\mathbb{Z}_p)$ *des fonctions continues de* $\mathbb{Z}_p$ *dans lui-même.*

Plus généralement:

PROPOSITION 1.4. (Kaplansky [9]). *Lorsque* A *est l'anneau d'une valuation discrète de corps résiduel fini, l'anneau des polynômes à valeurs entières sur* A *est dense dans l'anneau* $C(\hat{A},\hat{A})$ *des fonctions continues de* $\hat{A}$ *dans lui-même.*

Nous nous proposons ici de remplacer l'anneau de valuation par un anneau nœthérien A muni d'une topologie I-adique et de déterminer les conditions sous lesquelles il existe une approximation polynomiale des fonctions continues du complété $\hat{A}$ dans lui-même.

Notations 1.5. Soient A un anneau et I un idéal de A tels que A soit séparé pour la topologie I-adique. Notons $\hat{A}$ le complété de A pour la topologie I-adique et $C(\hat{A}, \hat{A})$ l'anneau des fonctions continues de $\hat{A}$ dans $\hat{A}$, muni de la topologie de la convergence uniforme.

A propos de l'énoncé que nous avons en vue notons tout d'abord le résultat négatif suivant:

PROPOSITION 1.6. *Les anneaux $A[X]$ et $\hat{A}[X]$ ne sont jamais denses dans $C(\hat{A}, \hat{A})$ sauf lorsque A est un corps fini.*

Démonstration. Supposons que $A[X]$ soit dense. L'idéal I est nul, sinon il existerait un élément non nul a de I et un entier k tel que a n'appartienne à pas à I^k; par suite, la fonction caractéristique de l'ouvert-fermé I^k ne pourrait être approchée à I près par des polynômes P de $A[X]$ puisque $P(a)$ appartient à I dès qu'il en est ainsi de $P(o)$. Ainsi la topologie de A doit être discrète et, dans ce cas, $A[X]$ dense dans $C(\hat{A}, \hat{A})$ signifie que toute application de A dans A est polynomiale. Soit alors c un élément non nul de A; s'il existe un polynôme P de $A[X]$ tel que $P(o) = o$ et $P(c) = 1$, alors c divisant $P(c) - P(o) = 1$ est nécessairement inversible dans A; ainsi, A doit être un corps. Enfin, lorsque A est un corps, toute application de A dans A est polynomiale si et seulement si ce corps est fini.

Nous disposons en revanche de la version p-adique du théorème de Stone-Weierstrass due à Kaplansky [8] et nous l'adapterons à notre problème au paragraphe 2 (proposition 2.6). Nous disposons aussi, lorsque l'anneau A est intègre de corps des fractions K, de l'anneau $\mathrm{Int}(A) = \{P \in K[X] | P(A) \subset A\}$ des polynômes à valeurs entières sur A et nous retrouverons au paragraphe 3 les conditions suffisantes obtenues, lorsque A est nœthérien, par Cahen, Grazzini et Haouat [5], pour que $\mathrm{Int}(A)$ soit dense dans $C(\hat{A}, \hat{A})$, à savoir que $\hat{A}$ soit intègre lui aussi (théorème 3.3). Mais il se pourrait qu'il existe un théorème analogue lorsque A n'est pas intègre, que l'on pourrait obtenir par exemple en utilisant des polynômes à coefficients dans l'anneau total des fractions de A (cf. proposition 3.1). C'est pourquoi nous introduisons au paragraphe 4 la notion générale de fonction polynomiale à valeurs entières sur A, dont l'ensemble constitue un A-module (proposition 4.6). Nous prouverons enfin au dernier paragraphe que, lorsque A est nœthérien, si les fonctions de $C(\hat{A}, \hat{A})$ qui sont polynomiales constituent un sous-ensemble dense alors en fait $\hat{A}$ est intègre (théorème 5.5).

2. Variantes du théorème de Stone-Weierstrass.

Rappelons l'une des versions initiales du théorème de Stone-Weierstrass:

PROPOSITION 2.1. (Stone [14], thm 1). *Soit X un espace compact et soit C une sous-algèbre de $C(X, \mathbb{R})$. Si C contient les fonctions constantes et sépare les points de X [c.-à-d., quels que soient x et y distincts dans X, il existe f dans C tel que $f(x) \neq f(y)$], alors C est dense dans $C(X, \mathbb{R})$.*

Il revient au même de dire: soit X un espace compact et soit B un sous-ensemble de $C(X, \mathbb{R})$ séparant les points de X. Alors, toute fonction numérique continue sur X peut être approchée uniformément par des expressions polynomiales en les éléments de B à coefficients réels.

Pour obtenir des conditions suffisantes d'approximation polynomiale, nous allons utiliser la version p-adique suivante du théorème de Stone-Weierstrass.

PROPOSITION 2.2. (Kaplansky [8]). *Soit X un espace compact totalement discontinu et soit R un anneau topologique possédant un système fondamental de voisinages de zéro formé d'idéaux. Notons $C(X, R)$ l'anneau des fonctions continues de X dans R muni de la topologie de la convergence uniforme. Un sous-anneau C de $C(X, R)$ vérifiant les conditions ci-dessous est dense dans $C(X, R)$: (i) C contient les constantes (c'est-à-dire les éléments de R en tant que fonctions constantes); (ii) C sépare les points de X au sens suivant:*

quels que soient x et y distincts dans X, il existe f dans C tel que $f(x) = o$ et $f(y) = 1$.

Remarque. Ces conditions peuvent aisément être remplacées par les conditions plus faibles suivantes: (i) C contient un sous-anneau R_o de R dense dans R; (ii) C sépare les points de X au sens suivant: quels que soient x et y distincts dans X, quel que soit le voisinage U de o dans R, il existe f dans C tel que $f(x)$ appartienne à U et $f(y)$ appartienne à $1 + U$.

Nous allons appliquer cet énoncé dans le cas où X et R sont tous deux le complété $\hat{A}$ d'un anneau nœthérien A muni d'une topologie I-adique pour laquelle il est séparé, I désignant un idéal de A. Pour que l'espace $\hat{A}$ soit compact, il est nécessaire que les espaces discrets quotients $\hat{A}/I^n\hat{A}$ isomorphes à A/I^n soient finis, c'est-à-dire en fait que le quotient A/I soit fini puisque A est supposé nœthérien. Cette hypothèse est alors suffisante pour que $\hat{A}$ soit compact et totalement discontinu puisque $\hat{A}$ est isomorphe à la limite projective des espaces finis discrets A/I^n. Enfin, sous cette hypothèse de finitude de A/I, les idéaux premiers contenant I sont en nombre fini et de corps résiduels finis, donc maximaux.

Notation 2.4. Pour tout sous-ensemble C de $C(\hat{A}, \hat{A})$ contenant A, tout idéal m de A contenant I et tout élément x de $\hat{A}$, considérons l'ensemble:

$$m_x(C) = \{f \in C | f(x) \in m\hat{A}\}.$$

Lorsque C est un A-module, $m_x(C)$ en est un sous-A-module maximal vérifiant $C/m_x(C) \cong A/m$. Lorsque C est un anneau, $m_x(C)$ en est un idéal maximal de corps résiduel isomorphe à A/m.

LEMME 2.5. *Si un sous-ensemble C de $C(\hat{A}, \hat{A})$ contenant A est dense dans $C(\hat{A}, \hat{A})$, alors, pour tout idéal m de A contenant I, les ensembles $m_x(C)$ sont distincts lorsque x décrit $\hat{A}$.*

Démonstration. Soient x et y dans A et soit k tel que $x - y$ n'appartienne pas à $I^k\hat{A}$. La fonction caractéristique de l'ouvert-fermé

$x + I^k\hat{A}$ étant approchée à $\hat{I}$ près par une fonction f de C, $f(x)$ et $f(y)$ appartiennent respectivement à $1 + \hat{I}$ et à $\hat{I}$ et, par suite, pour tout idéal maximal m contenant I, cette fonction f appartient à $m_y(C)$ sans appartenir à $m_x(C)$.

PROPOSITION 2.6. *Supposons A nœthérien et le quotient A/I fini. Soit C un anneau compris entre A et $\mathcal{C}(\hat{A}, \hat{A})$. Alors, les assertions suivantes sont équivalentes:*

(i) L'anneau C est dense dans $\mathcal{C}(\hat{A}, \hat{A})$.

(ii) Quels que soient x et y distincts dans $\hat{A}$ et quel que soit l'entier n, il existe f dans C tel que $f(x)$ et $f(y)$ appartiennent respectivement à $I^n\hat{A}$ et $1 + I^n\hat{A}$.

(iii) Quel que soit l'idéal maximal m de A contenant I, les idéaux $m_x(C) = \{f \in C | f(x) \in m\hat{A}\}$ sont distincts lorsque x décrit $\hat{A}$.

Démonstration. La proposition 2.2 et la remarque 2.3 montrent que (ii) implique (i) et le lemme 2.5 que (i) implique (iii). Montrons que (iii) implique (ii). Soient x et y distincts dans $\hat{A}$ et n un entier. Le quotient A/I étant fini, l'idéal I est contenu dans un nombre fini d'idéaux maximaux $m_1, \ldots, m_s$ et le radical $r\hat{A}$ de $I\hat{A}$ est l'intersection des idéaux $m_1\hat{A}, \ldots, m_s\hat{A}$. Selon (iii), pour tout $i = 1, \ldots, s$, il existe g_i dans C tel que $g_i(x)$ appartienne à $m_i\hat{A}$ et $g_i(y)$ n'y appartienne pas.

Soient encore, pour $i = 1, \ldots, s$, un élément b_i de A n'appartenant pas à m_i, mais appartenant aux autres m_j. Soit enfin $g = \Sigma_i b_i g_i$, alors g est dans C, $g(x)$ appartient à $r\hat{A}$ et $g(y)$ n'y appartient pas.

Soit k tel que r^k soit inclus dans I et soit $h = g^k$. Alors h est dans C, $h(x)$ appartient à $I\hat{A}$ et $h(y)$ est inversible dans $\hat{A}$. Soit donc u dans $\hat{A}$ tel que $uh(y) = 1$ et soit a dans A tel que u-a appartienne à $I^n\hat{A}$. Alors $f = (ah)^n$ est dans C, $f(x) = (ah(x))^n$ appartient à $I^n\hat{A}$ tandis que $f(y) - 1 = (ah(y))^n - (uh(y))^n = (a^n - u^n)h(y)^n$ appartient à l'idéal $(a - u)\hat{A}$ lui-même inclus dans $I^n\hat{A}$.

COROLLAIRE 2.7. *Soient C et D deux anneaux tels que $A \subset C \subset D \subset \mathcal{C}(\hat{A}, \hat{A})$. Supposons A nœthérien et le quotient A/I fini.*

Pour que C soit dense dans $C(\hat{A}, \hat{A})$, il faut et il suffit que D le soit et que, pour tout idéal maximal $\mathfrak{m}$ de A contenant I, l'application $\mathfrak{m}_I(D) \to \mathfrak{m}_I(D) \cap C = \mathfrak{m}_I(C)$ soit bijective.

Remarque 2.8. Bourbaki ([1], Chap. X, §4, ex. 24) donne un énoncé assez proche de celui de Kaplansky (proposition 2.2): si X est un espace compact totalement discontinu et R un anneau topologique possédant un système fondamental de voisinages de zéro formé d'idéaux, alors tout sous-anneau C de $C(X, R)$ contenant les constantes et séparant les points de X est dense dans $C(X, R)$. Mais ici séparer les points de X signifie selon Bourbaki ([1], Chap. IX, §1, déf. 5): quels que soient x et y distincts dans X, il existe f dans C tel que $f(x) \neq f(y)$. Sous cette forme, l'énoncé est manifestement en contradiction avec la proposition 1.6: appliqué au cas où $X = R = \hat{A}$, $\hat{A}$ désignant un anneau nœthérien local complet de corps résiduel fini, il prouverait que $\hat{A}[X]$ est dense dans $C(\hat{A}, \hat{A})$.

3. Conditions suffisantes.

Nous allons utiliser la proposition 2.6 dans le cas où C est un anneau de polynômes. Puisque C est contenu dans $C(\hat{A}, \hat{A})$, ces polynômes sont aussi des fonctions qui sur $\hat{A}$ prennent leurs valeurs dans $\hat{A}$ et qui de plus sont continues. A ce propos, lorsque A est un anneau intègre, on connaît les *polynômes à valeurs entières*, polynômes à coefficients dans le corps des fractions K de A, qui sur A prennent leurs valeurs dans A. Ils constituent un anneau:

$$\mathrm{Int}(A) = \{P \in K[X] | P(A) \subset A\}$$

On peut avoir l'idée d'élargir la notion en considérant, comme nous allons le faire dans un premier temps, l'anneau total des fractions T de l'anneau A et des polynômes $P \in T[X]$ tels que $P(A) \subset A$. Commençons par deux résultats préparatoires:

PROPOSITION. 3.1. *Supposons l'anneau A nœthérien et soit T*

l'anneau total des fractions de A. Tout polynôme $P \in T[X]$ tel que $P(A) \subset A$ appartient à l'anneau $C(\hat{A}, \hat{A})$.

Démonstration. Nous allons montrer qu'un tel polynôme P définit une application de A dans A uniformément continue pour la topologie I-adique, donc une application de $\hat{A}$ dans $\hat{A}$ uniformément continue.

Si d est un élément non diviseur de zéro dans A, le lemme d'Artin-Rees, appliqué au A-module A et à son sous-module dA, montre l'existence d'un entier k tel que, pour tout entier n, on ait:

$$I^{n+k} \cap dA = I^n(I^k \cap dA).$$

Par suite, pour tout entier naturel n et tout élément z de A, z appartient à I^n dès que dz appartient à I^{n+k}.

Soit donc $P(X) = \Sigma_i p_i X^i$ un polynôme à coefficients dans T tel que $P(A) \subset A$. Soit d un élément non diviseur de zéro dans A tel que $dP(X)$ appartienne à $A[X]$ et soit k l'entier correspondant décrit précédemment. Soient a et b deux éléments de A et n un entier naturel. Nous allons montrer que si $a - b$ appartient à I^{n+k}, alors $P(a) - P(b)$ appartient à I^n. Nous avons:

$$d(P(a) - P(b)) = \Sigma_{i>0}(dp_i)(a^i - b^i) = (a - b)\Sigma_{i>0}(dp_i)(a^i - b^i)/(a - b).$$

Or, dp_i et $(a^i - b^i)/(a - b)$ appartiennent à A; donc $d(P(a) - P(b))$ appartient à $(a - b)A$, qui est inclus dans I^{n+k}, et $P(a) - P(b)$ appartient à I^n.

LEMME 3.2. *Supposons l'anneau A nœthérien et intègre. Soit $S = \cap_i(A \setminus m_i)$ où m_i décrit l'ensemble des idéaux maximaux de A contenant I. Alors* $\mathrm{Int}(A)$ *est dense dans* $\mathrm{Int}(S^{-1}A)$.

Démonstration. L'inclusion de $\mathrm{Int}(A)$ dans $\mathrm{Int}(S^{-1}A)$ résulte de [4] sans hypothèse sur la partie multiplicative S (voir l'énoncé plus général rappelé en 4.9 ci-après). En fait, l'anneau A étant supposé nœthérien, on a $S^{-1}(\mathrm{Int}(A)) = \mathrm{Int}(S^{-1}A)$ et donc, pour tout idéal maximal m de A contenant I, $(\mathrm{Int}(A))_m = (\mathrm{Int}(S^{-1}A))_m$. Par suite, pour tout entier k, on a l'isomorphisme:

$$\mathrm{Int}(A)/I^k\mathrm{Int}(A) \cong \mathrm{Int}(S^{-1}A)/I^k\mathrm{Int}(S^{-1}A)$$

et donc:

$$\mathrm{Int}(S^{-1}A) = \mathrm{Int}(A) + I^k\mathrm{Int}(S^{-1}A).$$

THÉORÈME 3.3. *Soit A un anneau intègre nœthérien, séparé pour la topologie I-adique. Si A est un corps fini ou si le radical de I est un idéal maximal m de A tel que A_m, soit de dimension 1, à corps résiduel fini et analytiquement irréductible, alors l'anneau* Int(A) *des polynômes à valeurs entières sur A est dense dans $C(\hat{A}, \hat{A})$.*

Démonstration. Remarquons tout d'abord que Int(A) est bien contenu dans $C(\hat{A}, \hat{A})$ d'après la proposition 3.1 appliquée dans le cas où A est intègre. Si A est un corps fini, $I = (o)$ et l'affirmation du théorème est immédiate compte tenu des polynômes d'interpolation de Lagrange. Supposons donc A infini. L'idéal I ayant pour radical un idéal maximal m, on peut remplacer I par m puisque cela ne change rien au complété $\hat{A}$. Le lemme 3.2 permet de plus de supposer A local pour montrer la densité de Int(A) dans $C(\hat{A}, \hat{A})$. L'anneau local A est alors de dimension 1 et le théorème 3.3 résulte immédiatement de la proposition 3.4 ci-dessous énoncée par Cahen, Grazzini et Haouat [5] avec l'hypothèse supplémentaire que la clôture intégrale A' de A soit un A-module de type fini, mais ceci est automatique dès que $\hat{A}$ est réduit (cf. Nagata [11]). Nous en donnerons une démonstration basée sur la caractérisation suffisante de la proposition 2.6.

PROPOSITION 3.4. (Cahen, Grazzini et Haouat [5]). *Soit A un anneau intègre, nœthérien, local d'idéal maximal m, de corps résiduel fini et analytiquement irréductible. Alors l'anneau* Int(A) *est dense dans $C(\hat{A}, \hat{A})$ où $\hat{A}$ désigne le complété de A pour la topologie m-adique.*

Démonstration. Selon la proposition 2.6, il s'agit de montrer que les idéaux $m_x = m_x(\mathrm{Int}(A)) = \{P(X) \in \mathrm{Int}(A) | P(x) \in m\hat{A}\}$ de Int(A) sont distincts lorsque x décrit $\hat{A}$. L'anneau $\hat{A}$ étant intègre, la clôture intégrale A' de A est un anneau local (cf. Nagata [11]), d'idéal maximal m' et par suite est un anneau de valuation discrète. Etant aussi un A-module de type fini, A' a un corps résiduel extension finie de celui de A, donc fini. D'après la proposition 1.4, Int(A') est dense dans $C(\hat{A}', \hat{A}')$ où $\hat{A}'$ désigne le complété de l'anneau A' pour la topologie m'-adique (c'est aussi le complété du A-module A' pour la topologie mA'-adique).

Le conducteur de A' dans A est un idéal non nul de A' donc de la forme m'^e et est un idéal de A que l'on peut supposer contenu dans m (sinon $A' = A$ et il n'y aurait plus de question). Ainsi: $m'^e \subset m \subset m'$. Soient x et y distincts dans A et montrons qu'il existe Q dans Int(A) tel que Q appartienne à m_x et n'appartienne pas à m_y.

Soit k tel que $x - y$ n'appartienne pas à $m^k\hat{A}$. La propriété de densité relative à A' implique l'existence d'un polynôme Q de $K[X]$ tel que $Q(A') \subset A'$ et approchant à $m'^e\hat{A}$ près la fonction caractéristique de l'ouvert-fermé $y + m'^{ek}\hat{A}$ de $\hat{A}'$. Comme $m'^e\hat{A} \subset m\hat{A} \subset \hat{A}$ et $1 + m'^e\hat{A} \subset 1 + m\hat{A} \subset \hat{A}$, on voit qu'en fait $Q(A)$ est inclus dans $\hat{A} \cap K = A$ et donc Q appartient à Int(A). De plus, $Q(y)$ appartient à $1 + m'^e\hat{A} \subset 1 + m\hat{A}$ tandis que $Q(x)$ appartient à $m'^e\hat{A} \subset m\hat{A}$.

Plus brièvement, on peut retrouver cette condition suffisante de la proposition 3.4 avec la proposition suivante:

PROPOSITION 3.5. (Cahen [3]). *Si A est un anneau intègre nœthérien, de dimension 1, local, d'idéal maximal m et de corps résiduel fini et si la clôture intégrale A' de A est un anneau local d'idéal maximal m', alors l'application:*

$$x \to m_x = \{P(X) \in \mathrm{Int}(A) | P(x) \in m'\hat{A}'\}$$

est une bijection entre la fermeture topologique de A dans le complété $\hat{A}'$ de A' pour la topologie m'-adique et l'ensemble des idéaux premiers de Int(A) *au-dessus de m.*

En effet, on a dit, au cours de la démonstration de la proposition 3.4, que l'anneau A étant analytiquement irréductible, la topologie

m'-adique coïncide sur A avec la topologie m-adique et donc, dans la proposition 3.5, la fermeture topologique de A n'est autre que $\hat{A}$.

Exemples 3.6. a) L'anneau $A = \mathbb{F}_q[T^2, T^3]$, qui n'est pas un anneau de valuation, et l'idéal $I = (T^2)$ satisfont aux conditions du théorème 3.3.

b) Supposons que l'anneau A soit un ordre c'est-à-dire un sous-anneau d'un corps de nombres K de rang $n = [K : \mathbb{Q}]$ en tant que $\mathbb{Z}$-module. La clôture intégrale A' de A est l'anneau des entiers de K, c'est un $\mathbb{Z}$-module de rang n et a fortiori un A-module de type fini. Soit m un idéal maximal de A et $\hat{A}_m$ le complété de A pour la topologie m-adique. L'anneau A étant de dimension 1, pour que $\hat{A}_m$ soit intègre il faut et il suffit qu'il n'y ait qu'un idéal maximal de A' au-dessus de l'idéal maximal m de A (cf. [12]). En particulier:

Soit $A = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Soit m un idéal maximal de A et soit $\hat{A}_m$ le complété de A pour la topologie m-adique. L'anneau Int(A) est dense dans $C(\hat{A}_m, \hat{A}_m)$ sauf si m est au-dessus de 2 et $d \equiv 1 \pmod 8$.

En effet, si $d \equiv 2$ ou $3 \pmod 4$, $A = A'$. Supposons donc $d \equiv 1 \pmod 4$, alors $A' = \mathbb{Z} + (1 + \sqrt{d})/2\mathbb{Z}$. Soit p le nombre premier au-dessous de m. Si p n'est pas décomposé dans A' (c'est-à-dire n'est pas au-dessous de deux idéaux maximaux distincts de A'), il en est de même pour m. Par contre, si p est décomposé dans A', il s'agit de savoir si p est aussi au-dessous de deux idéaux maximaux distincts de A. Or, lorsque p est impair, A'/pA' est isomorphe à A/pA car $(1 + \sqrt{d})/2 \equiv (p+1)(1 + \sqrt{d})/2 \pmod{pA'}$ et $(p+1)(1+\sqrt{d})/2$ appartient à A. Ainsi, si p est décomposé dans A', il l'est aussi dans A. Il reste à envisager le cas où $p = 2$. On sait que si $d \equiv 5 \pmod 8$, alors 2 est inerte dans A' et donc non décomposé (cf. Samuel [13]), par contre, si $d \equiv 1 \pmod 8$, 2 est décomposé dans A' puisque $A'/2A' \cong \mathbb{F}_2[X]/X(X+1)$ tandis que 2 est au-dessous du seul idéal maximal m puisque $A/2A \cong \mathbb{F}_2[X]/(X+1)^2$ ($A/2A \cong \mathbb{Z}[X]/(2, X^2 - d) \cong \mathbb{F}_2[X]/(X^2 - d)$ et $X^2 - d \equiv X^2 - 1 \equiv (X+1)^2 \pmod 2$).

PROPOSITION 3.7. *Supposons A intègre, nœthérien, de dimension 1, local, de corps résiduel fini et analytiquement irréductible. Alors,* *pour tout entier naturel k, l'anneau $D^k = \{P \in K[X] | P^{(h)} \in \mathrm{Int}(A), o \leq h \leq k\}$, anneau des polynômes à valeurs entières sur A ainsi que leurs dérivées jusqu'à l'ordre k, est dense dans $C(\hat{A}, \hat{A})$. De plus, l'anneau $D = \cap_k D^k$, des polynômes à valeurs entières sur A ainsi que toutes leurs dérivées, est dense dans $C(\hat{A}, \hat{A})$ si et seulement si A est de caractéristique p non nulle.*

Démonstration. D'après [6], pour tout entier naturel k, l'anneau D^k vérifie la condition: pour tout Q dans $\mathrm{Int}(A)$, il existe un entier s tel que Q^s appartienne à D^k. Par suite l'application: $m_x \to m_x \cap D^k = m_x(D^k)$ est une bijection entre les idéaux maximaux de $\mathrm{Int}(A)$ et ceux de D^k au-dessus de m. Le lemme 2.5 et la proposition 3.4 montrent que D^k est dense dans $C(\hat{A}, \hat{A})$.

Si A est de caractéristique $p > o$, alors D vérifie la même propriété: pour tout Q dans $\mathrm{Int}(A)$, Q^p appartient à D puisque les dérivées de Q^p sont nulles. Par contre, si A est de caractéristique o, D ne peut être dense dans $C(\hat{A}, \hat{A})$. En effet, d'après [6], les idéaux m_x et m_y sont égaux dès que $x - y$ appartient à l'idéal $p\hat{A}$.

Remarque. La proposition précédente montre que, lorsque A est de caractéristique o, il n'existe pas de plus petit anneau compris entre $A[X]$ et $\mathrm{Int}(A)$ dense dans $C(\hat{A}, \hat{A})$ puisque les D^k sont denses et non leur intersection D.

4. Fonctions polynomiales à valeurs entières.

Nous allons regarder maintenant s'il est possible d'étendre le théorème 3.3 en ne se limitant plus au cas d'un anneau intègre A et en définissant une notion de polynome à valeurs entières la plus générale possible, plus générale que celle envisagée avec l'anneau total de fractions dans l'énoncé 3.1. Il faut d'abord préciser ce que l'on entend par fonction polynomiale sur un anneau A.

DÉFINITIONS 4.1.

(i) Une fonction f définie sur un anneau A et à valeurs dans un ensemble E est dite polynomiale s'il existe un A-module M contenant E et un polynôme $P(X) = m_0 + m_1X + \ldots + m_dX^d$ à coefficients dans le A-module M tels que:

$$f(a) = P(a) = m_o + a \cdot m_1 + a^2 \cdot m_2 + \cdots + a^d \cdot m_d.$$

On dira alors que f est représentable par le polynôme P

(ii) On dit qu'une fonction est à valeurs entières sur A si elle est définie sur A et prend ses valeurs dans A.

Notation 4.2. On notera Ent(A) l'ensemble des fonctions polynomiales à valeurs entières sur A.

A priori le A-module M de la définition 4.1.(i) est quelconque, cependant lorsque f est à valeurs entières sur A, on a:

PROPOSITION 4.3. *Toute fonction polynomiale à valeurs entières sur A est représentable par un polynôme à coefficients dans l'enveloppe injective E du A-module A.*

Démonstration. Soit f une fonction polynomiale à valeurs entières sur A. Elle est représentable par un polynôme à coefficients $m_0, m_1, \ldots, m_d$ dans un A-module M contenant A. L'enveloppe injective $E = E(A)$ du A-module A est contenue dans l'enveloppe injective $E(M)$ du A-module M; donc E est facteur direct de $E(M)$, c'est-à-dire $E(M) = E \oplus N$; par suite, pour $i = o, \ldots, d$, on a: $m_i = e_i + n_i$ où $e_i \in E$ et $n_i \in N$. Ainsi, pour tout élément a de A, on a:

$$f(a) = \Sigma_i a^i \cdot m_i = \Sigma_i a^i \cdot e_i + \Sigma_i a^i \cdot n_i.$$

Par hypothèse, $f(a)$ appartient à A, donc à E et on a: $f(a) = \Sigma_i a^i \cdot e_i$.

On va donc pouvoir se limiter aux polynômes à coefficients dans l'envelope injective E de A. Ceux-ci constituent clairement un A-module - et même un $A[X]$-module - isomorphe à $E \otimes A[X]$ que l'on peut noter $E[X]$. Pour tout élément a de A, l'application qui à un polynôme $P(X)$ associe sa valeur $P(a)$ en a est un homomorphisme du A-module $E[X]$ dans le A-module E.

DÉFINITION 4.4. *On appelle polynôme à valeurs entières sur un anneau A tout polynôme à coefficients dans l'enveloppe injective E de A qui sur A prend ses valeurs dans A.*

Notation. 4.5. On notera $\mathrm{Int}(A)$ l'ensemble des polynômes à valeurs entières sur A, autrement dit:

$$\mathrm{Int}(A) = \{P(X) \in E[X] | P(A) \subset A\}.$$

C'est un sous-A-module de $E[X]$.

Cette notation est en accord avec la terminologie antérieure relative au cas où A est un anneau intègre et où donc l'enveloppe injective de A est son corps des fractions (cf. [2], [3]).

PROPOSITION 4.6. *L'ensemble* $\mathrm{Ent}(A)$ *des fonctions polynomiales à valeurs entières sur A est un A-module et on a l'isomorphisme:*

$$\mathrm{Ent}(A) \cong \mathrm{Int}(A)/\{P(X) \in E[X] | P(A) = \{o\}\}.$$

Démonstration. Les définitions 4.1 ne permettaient pas de dire a priori que la somme de deux fonctions polynomiales à valeurs entières est encore une fonction polynomiale. Mais selon la proposition 4.3, les polynômes représentants de ces fonctions peuvent être choisis dans $E[X]$, si bien que la fonction somme des deux fonctions initiales sera représentable par le polynôme somme de ces deux représentants, somme qui elle est bien définie.

L'homomorphisme naturel de A-modules de $\mathrm{Int}(A)$ dans $\mathrm{Ent}(A)$, qui est surjectif d'après la proposition 4.3, a évidemment pour noyau l'ensemble des polynômes P de $\mathrm{Int}(A)$ ne prenant que la valeur o.

Lorsque A est un anneau intègre infini de corps des fractions K, le module $\{P(X) \in K[X] | P(A) = \{o\}\}$ est réduit à o et le A-module $\mathrm{Ent}(A)$ des fonctions polynomiales à valeurs entières sur A n'est autre que l'anneau $\mathrm{Int}(A)$ des polynômes à valeurs entières sur A.

Question. 4.7. A quelles conditions portant sur l'anneau A le A-module Ent(A) des fonctions polynomiales à valeurs entières sur A est-il un anneau?

PROPOSITION 4.8. *Soit S une partie multiplicative de l'anneau A. Il existe un homomorphisme naturel de A-modules de* Ent(A) *dans* Ent($S^{-1}A$), *module des fonctions polynomiales à valeurs entières sur* $S^{-1}A$.

Démonstration. Soit f un élément de Ent(A) et soit P un représentant de f dans Int(A). Notons P^* l'image de P dans $(E/A)[X]$. Puisque $P(A) \subset A$, on a $P^*(A) = \{o\}$, et donc, d'après le rappel 4.9 ci-dessous, l'image P_S^* de P^* dans le localisé $S^{-1}(E/A)[X]$ vérifie: $(P_S^*)(S^{-1}A) = \{o\}$. Comme $S^{-1}(E/A) = S^{-1}E/S^{-1}A$, l'image P_S de P dans $(S^{-1}E)[X]$ vérifie: $P_S(S^{-1}A) \subset S^{-1}A$. Ainsi P_S définit un élément f_S de Ent($S^{-1}A$).

Cet élément f_S ne dépend pas du choix du représentant P dans Int(A) car si $Q \in E[X]$ vérifie $Q(A) = \{o\}$, alors, toujours d'après le rappel 4.9, l'image Q_S de Q vérifie $Q_S(S^{-1}A) = \{o\}$.

Rappel 4.9. (Cahen et Chabert [4], Prop. 4). Soient M un A-module, P un polynôme à coefficients dans M et S une partie multiplicative de A. Si $P(A) = \{o\}$, alors l'image P_S de P dans $(S^{-1}M)[X]$ vérifie $P_S(S^{-1}A) = \{o\}$.

COROLLAIRE 4.10. *Supposons A nœthérien. Alors, pour toute partie multiplicative S de A, le $S^{-1}A$-module* S^{-1}Ent(A) = $S^{-1}A \otimes$ Ent(A) *s'injecte naturellement dans le $S^{-1}A$-module* Ent($S^{-1}A$).

Démonstration. L'homomorphisme de A-modules: $f \in$ Ent(A) $\rightarrow$ $f_S \in$ Ent($S^{-1}A$) induit, par tensorisation par $S^{-1}A$, un homomorphisme de $S^{-1}A$-modules: $S^{-1}A \otimes$ Ent(A) = S^{-1}Ent(A) $\rightarrow$ Ent($S^{-1}A$). Montrons que cet homomorphisme est injectif. Soit f dans Ent(A) tel que $f_S = 0$. Soit $P \in E[X]$ un représentant de f : $P(A) \subset A$ et $P_S(S^{-1}A) = \{o\}$. Le A-module N engendré par les valeurs de P sur A est de type fini puisqu'il est contenu dans le A-module engendré par les coefficients de P et que A est supposé nœthérien. Soient $a_1, a_2, \ldots, a_r$ dans A tels que $P(a_1), P(a_2), \ldots, P(a_r)$ engendrent le A-module N. Puisque $P_S(S^{-1}A) = \{o\}$, il existe en particulier $s_1, s_2, \ldots, s_r$ dans S tels que $s_i P(a_i) = o$ pour $i = 1, 2, \ldots, r$. Posons $s = s_1 s_2 \ldots s_r$. Le polynôme sP vérifie donc $(sP)(A) = \{o\}$, par suite il représente la fonction nulle sur A, autrement dit $sf = o$ et l'image de f dans $S^{-1}(\mathrm{Ent}(A))$ est nulle.

PROPOSITION 4.11. *Si q est un idéal premier de A de corps résiduel infini, alors:*

$$(\mathrm{Ent}(A))_q \cong (\mathrm{Int}(A))_q \cong \mathrm{Ent}(A_q) \cong \mathrm{Int}(A_q) = A_q[X].$$

Démonstration. Soit P un élément de $\mathrm{Int}(A)$. Selon la preuve de la proposition 4.8, l'image P_q de P dans $E_q[X]$ vérifie $P_q(A_q) \subset A_q$. Le rappel 4.12 ci-dessous, appliqué au A_q-module E_q et au polynôme P_q, montre que les coefficients de P_q appartiennent à A_q; donc $(\mathrm{Int}(A))_q = A_q[X]$. De plus, si un polynôme P_0 de $E[X]$ vérifie $P_o(A) = \{o\}$, alors $(P_o)_q(A_q) = \{o\}$ et, toujours d'après le rappel 4.12, $(P_o)_q = o$; d'où:

$$(\mathrm{Ent}(A))_q \cong (\mathrm{Int}(A))_q / \{P(X) \in E[X] | P(A) = \{o\}\}_q = (\mathrm{Int}(A))_q = A_q[X].$$

Rappel 4.12. (Cahen et Chabert [4], Prop. 3). Soient M un A-module et P un poynôme à coefficients dans M. Si tout idéal premier du support du A-module M a un corps résiduel infini, alors le A-module engendré par les coefficients de P est égal au A-module engendré par les valeurs de P sur A.

COROLLAIRE 4.13. *Si q est un idéal premier de A de corps résiduel infini, alors les coefficients de tout polynôme P dans* $\mathrm{Int}(A)$ *appartiennent au A-module: $A_{(q)} = \{e \in E|$ il existe $s \in A \backslash q$ tel que $se \in A\}$. Ainsi,* $\mathrm{Int}(A)$ *est inclus dans le A-module $A°[X]$ où $A°$ désigne le A-module $\cap A_{(q)}$ où q décrit l'ensemble des idéaux premiers de A de corps résiduel infini.*

En effet, d'après la proposition 4.11, les coefficients de P_q appartiennent à A_q; les coefficients de P sont donc des éléments e de E pour lesquels il existe $t \in A \backslash q$ tel que $e/t = a$ dans A_q, c'est-à-dire qu'il existe $s \in A \backslash q$ tel que l'on ait $s(e - ta) = o$, autrement dit tel que se appartienne à A.

5. Conditions nécessaires.

Nous allons chercher maintenant à quelles conditions il existe des ensembles de telles fonctions polynomiales denses dans $C(\hat{A}, \hat{A})$. Autrement dit, nous cherchons si l'ensemble $C = \mathrm{Ent}(\hat{A}) \cap C(\hat{A}, \hat{A})$ peut être dense dans $C(\hat{A}, \hat{A})$. Pour simplifier nous ferons dans toute la suite l'hypothèse suivante:

5.1. Hypothèse: l'anneau A est nœthérien.

Alors, A est un anneau de Zariski d'idéal de définition $\hat{I} = I\hat{A}$ et l'application $m \to m\hat{A}$ est une bijection de l'ensemble des idéaux maximaux de A contenant I sur l'ensemble des idéaux maximaux de $\hat{A}$.

Question 5.2. Les éléments de $\mathrm{Ent}(A)$ et ceux de $\mathrm{Ent}(\hat{A})$ appartiennent-ils tous à $C(\hat{A}, \hat{A})$? Lorsque A est intègre, $\mathrm{Ent}(A) = \mathrm{Int}(A)$ est contenu dans $C(\hat{A}, \hat{A})$. Dans le cas général, les fonctions à valeurs entières sur A représentables par des polynomes à coefficients dans l'anneau total des fractions de A appartiennent à $C(\hat{A}, \hat{A})$ (proposition 3. 1).

LEMME 5.3. *S'il existe un sous-ensemble de $C(\hat{A}, \hat{A})$ constitué de fonctions polynomiales qui est dense dans $C(\hat{A}, \hat{A})$, alors les idéaux premiers non nuls de $\hat{A}$ ont un corps résiduel fini.*

Démonstration. Supposons que q soit un idéal premier de $\hat{A}$ de corps résiduel infini. Soient a et b dans $\hat{A}$ tels que $a - b$ appartienne à q. Pour tout polynôme P de Int($\hat{A}$), P_q appartient à $\hat{A}_q[X]$ d'après la proposition 4.11. Donc, $P_q(a) - P_q(b)$ appartient à $(a-b)\hat{A}_q$ qui est contenu dans $q\hat{A}_q$ et l'élément $P(a) - P(b)$ de $\hat{A}$, dont l'image dans $\hat{A}_q$ appartient à $q\hat{A}_q$, est lui-même dans q. L'idéal q est contenu dans un idéal maximal et celui-ci est de la forme $m\hat{A}$ où m désigne un idéal maximal de A contenant I. Alors, $P(a) - P(b)$ appartient à $m\hat{A}$. De même, si f désigne un élément de Ent($\hat{A}$), $f(a) - f(b)$ appartient à $m\hat{A}$. Par suite, $m_a(\mathrm{Ent}(\hat{A})) = m_b(\mathrm{Ent}(\hat{A}))$ (cf. notation 2.4). A fortiori, $m_a(C) = m_b(C)$, si C désigne un sous-ensemble de $\mathrm{Ent}(\hat{A}) \cap C(\hat{A}, \hat{A})$. Or, si cet ensemble C est dense dans $C(\hat{A}, \hat{A})$, le lemme 2.5 impose que $a = b$ et donc que $q = (o)$.

LEMME 5.4. *S'il existe un élément non nul b de $\hat{A}$ tel que $b^2 = o$, alors les fonctions polynomiales ne peuvent être denses dans $C(\hat{A}, \hat{A})$.*

Démonstration. Soit b un élément de $\hat{A}$ de carré nul. Pour tout polynôme $P(X) = e_o + e_1X + e_2X^2 + \ldots + e_dX^d$ dans Int($\hat{A}$), on a: $P(b) - P(o) = b.e$ et $b.e$ appartient à $\hat{A}$. L'élément $b.e$ est lui aussi de carré nul, puisque $(b.e)(b.e) = [(b.e).b].e = [b.(b.e)].e = [(b.b).e].e = [o.e].e = o$. Soit m un idéal maximal de A contenant I, l'idéal $m\hat{A}$ contient $b.e$, par suite $P(b) - P(o)$ appartient à $m\hat{A}$. De même, si f désigne un élément de Ent($\hat{A}$), $f(b) - f(o)$ appartient à $m\hat{A}$. Par suite, $m_b(\mathrm{Ent}(A)) = m_o(\mathrm{Ent}(A))$. S'il existait un sous-ensemble C de fonctions polynomiales dense dans $C(\hat{A}, \hat{A})$, le lemme 2.5 imposerait encore $b = o$.

THÉORÈME 5.5. *Soit A un anneau nœthérien et I un idéal de A. On suppose A séparé pour la topologie I-adique et on note $\hat{A}$ le complété de A. S'il existe un ensemble de fonctions polynomiales dense dans l'anneau $C(\hat{A}, \hat{A})$ des fonctions continues de $\hat{A}$ dans $\hat{A}$ muni de la topologie de la convergence uniforme, alors ou bien A est un corps fini, ou bien le radical de I est un idéal maximal m et l'anneau local A_m est de dimension 1, à corps résiduel fini et analytiquement irréductible (c.-à-d. $\hat{A}$ intègre).*

Démonstration. Supposons qu'il existe un ensemble de fonctions polynomiales dense dans $C(\hat{A}, \hat{A})$ et que A ne soit pas un corps fini.

Le lemme 5.3 montre que les idéaux premiers de A contenant I ont un corps résiduel fini; ils sont donc nécessairement maximaux et l'anneau quotient A/I étant nœthérien et de dimension o est artinien et fini. L'idéal I n'est contenu que dans un nombre fini d'idéaux maximaux $m_1, \dots, m_s$. Le complété $\hat{A}$ de A pour la topologie I-adique est donc isomorphe au produit des complétés de A pour les topologies m_i-adiques ($i = 1, \dots, s$).

Par ailleurs, toujours d'après ce même lemme 5.3, les idéaux premiers non nuls de $\hat{A}$ ayant un corps résiduel fini sont tous maximaux et la dimension de A est 1 ou o selon que $\hat{A}$ est intègre ou non. Si $\hat{A}$ n'était pas intègre, il serait de dimension o, donc fini et il existerait un élément non nul b de $\hat{A}$ tel que $b^2 = o$, ce qu'exclut le lemme 5.4. Ainsi, $\hat{A}$ est intègre.

Or, un anneau intègre ne peut être un produit fini d'anneaux; c'est donc qu'il ne peut y avoir qu'un seul idéal maximal contenant I. Finalement, le radical de I est un idéal maximal m de A, $\hat{A}$ est aussi le complété de A pour la topologie m-adique et dire que $\hat{A}$ est intègre c'est dire que l'anneau A_m est analytiquement irréductible. De plus, comme on l'a vu, l'anneau intègre local A_m est nécessairement de dimension 1 et son corps résiduel est fini.

Les théorèmes 3.3 et 5.5 conduisent à la:

Conclusion 5.6. Soit A un anneau nœthérien et I un idéal de A tel que A soit séparé pour la topologie I-adique. Le sous-ensemble de $C(\hat{A}, \hat{A})$ formé des fonctions polynomiales est dense dans $C(\hat{A}, \hat{A})$ pour la topogie de la convergence uniforme si et seulement si, ou bien $I = (o)$ et A est un corps fini, ou bien $\sqrt{I} = m$ où m est un idéal maximal de A et A_m est de dimension 1, à corps résiduel fini et analytiquement irréductible.

Et, dans ce dernier cas, on sait que l'anneau $\mathrm{Int}(A)$ des polynomes à valeurs entières sur A est dense dans $C(\hat{A}, \hat{A})$.

BIBLIOGRAPHIE

[1] Bourbaki N., *Topologie générale*, Chap. V à X, nouvelle édition, Hermann, Paris, 1974.

[2] Brizolis D., *Hilbert rings of integral-valued polynomials*, Comm. Algebra, **3** (1975), 1051-1081.

[3] Cahen P.-J., *Integer-valued polynomials on a subset*, Proc. Amer. Math. Soc., **117** (1993), 919-929.

[4] Cahen P.-J., Chabert J.-L., *Coefficients et valeurs d'un polynôme*, Bull. Sc. math., 2e sér., **95** (1971), 295-304.

[5] Cahen P.-J., Grazzini F., Haouat Y., *Intégrité du complété et théorème de Stone-Weierstrass*, Ann. Sci. Univ. Clermont II, Sér. Math., **21** (1982), 47-58.

[6] Chabert J.-L., *Polynômes à valeurs entières ainsi que leurs dérivées*, Ann. Sci. Univ. Clermont II, Sér. Math., **18** (1979), 47-64.

[7] Dieudonné J., *Sur les fonctions continues p-adiques*, Bull. Sc. math., 2e série, **68** (1944), 79-95.

[8] Kaplansky I., *Topological rings*, Amer. J. Math., **69** (1947), 153-183.

[9] Kaplansky I., *The Weierstrass theorem in fields with valuations*, Proc. Amer. Math. soc., **1** (1950), 356-357.

[10] Mahler K., *An Interpolation Series for continuous Functions of a p-adic Variable*, J. reine angew. Math., **199** (1958), 23-34.

[11] Nagata M., *Local Rings*, Wiley, New-York, 1962.

[12] Northcott D. G., *A general theory of one dimensional local rings*, Proc. Glasgow math. Ass., **2** (1954/56), 159-169.

[13] Samuel P., *Théorie Algébrique des Nombres*, Hermann, Paris, 1967.

[14] Stone M. H., *The generalized Weierstrass approximation theorem*, Mathematics magazine, **21** (1948), 167-184.

[15] Weierstrass K., *Über die analytische Darstellbarkeit sogenannter willkurlicher Functionen reeller Argumente*, Sitzungsberichte der Konigl. Preuss. Akad. Wissenschaften Berlin (1885), 633-639.

Pervenuto il 11 marzo 1993.

Jean-Luc Chabert
Institut Supérieur des Sciences et Techniques
Université de Picardie
48, rue Raspail, 02109 St Quentin, France