Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 340 (2005) 99–102
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Théorie des nombres

Équations aux différences dans les vecteurs de Witt

Luc Bélair

Département de mathématiques, université du Québec – UQAM, C.P. 8888 succ. Centre-ville, Montréal, Québec, H3C 3P8, Canada

Reçu le 10 septembre 2004 ; accepté le 30 novembre 2004

Présenté par Jean-Pierre Serre

Résumé

On montre une propriété d'approximation analogue à celle de Greenberg [Publ. Math. IHES 31 (1966) 59–64], mais pour les équations aux différences de l'automorphisme de Frobenius des vecteurs de Witt. ***Pour citer cet article : L. Bélair, C. R. Acad. Sci. Paris, Ser. I 340 (2005).***

Abstract

Difference equations in Witt vectors. We prove an approximation property for Frobenius difference equations in the Witt vectors, analog to a theorem of Greenberg [Publ. Math. IHES 31 (1966) 59–64]. ***To cite this article: L. Bélair, C. R. Acad. Sci. Paris, Ser. I 340 (2005).***

1. Introduction

Dans [8], Greenberg montre une propriété d'approximation pour les solutions des systèmes d'équations algébriques dans les anneaux de valuation discrète henséliens excellents.[1] Considérons des équations algébriques où apparaîtraient aussi un automorphisme et ses itérés, dites *équations aux différences*. Dans cette Note, on considère un résultat analogue à celui de Greenberg (Théorème 3.2) pour les équations aux différences dans un anneau de valuation discrète de caractéristique 0 qui satisfait un lemme de Hensel approprié, en particulier l'anneau des vecteurs de Witt sur un corps algébriquement clos avec son Frobenius. Un cas particulier avait été traité dans [5]. Essentiellement, nous transposons au nouveau contexte les preuves de [14,1] du théorème de Greenberg qui utilisent la théorie des modèles (de base) et les ultraproduits. Je ne connais pas de preuve « purement algébrique ».

Adresse e-mail : belair.luc@uqam.ca (L. Bélair).

[1] Pour toute cette théorie, voir [13].

1631-073X/$ – see front matter
doi:10.1016/j.crma.2004.12.001

On montre d'abord un résultat plus faible sur l'anneau des vecteurs de Witt (Théorème 2.1), inspiré de [14], qui a l'avantage de faire appel directement à un résultat connu. On donne finalement une application à un théorème des zéros pour les équations aux différences dans les vecteurs de Witt (Théorème 4.4). Les preuves et des résultats supplémentaires seront exposés dans un article détaillé.

Dans cette Note, les anneaux sont commutatifs unifères. On note $\mathbf{x}$ le n-uplet $(x_1, \ldots, x_n)$, et on abusera parfois de cette notation vectorielle. Un anneau aux différences est un anneau muni d'un automorphisme (voir [6]). Dans ce contexte on notera généralement l'automorphisme σ et on désignera une telle structure par (A, σ), où A est l'anneau sous-jacent. Pour un tel (A, σ), $A[\mathbf{X}]_\sigma$ désigne l'anneau des polynômes aux différences sur A en les indéterminées $X_1, \ldots, X_n$, c'est-à-dire, l'anneau des polynômes habituels sur A en les variables $\sigma^j(X_i)$, $j \in \mathbb{Z}$, $1 \leqslant i \leqslant n$.[2] Pour un corps valué[3] (K, v), V_K désigne son anneau de valuation et K_v son corps résiduel. Comme dans [2] on appellera *corps aux différences valué* un corps K muni d'un automorphisme σ et d'une valuation v tels que $v(\sigma(x)) = v(x)$ (voir [7]). On notera (K, σ, v) une telle structure. Si A, B sont deux sous-anneaux, $A \cdot B$ est le sous-anneau engendré.

Une sous-structure $\mathcal{M}$ d'une structure $\mathcal{N}$ est dite *sous-structure élémentaire,* si pour tout énoncé φ de la logique du premier ordre, formulé en termes des opérations et relations de base de $\mathcal{M}$ et $\mathcal{N}$ *et de paramètres dans* $\mathcal{M}$, on a que φ est vrai dans $\mathcal{N}$ ssi φ est vrai dans $\mathcal{M}$. En particulier, tout système d'équations et inéquations à paramètres dans $\mathcal{M}$ qui a une solution dans $\mathcal{N}$ a déjà une solution dans $\mathcal{M}$. Un exemple est fourni par une extension de corps algébriquement clos $\mathcal{M} \subset \mathcal{N}$. Une théorie du premier ordre est *modèle-complète* si tout modèle $\mathcal{M}$ qui est une sous-structure d'un autre modèle $\mathcal{N}$, en est automatiquement une sous-structure élémentaire. Un exemple est fourni par la théorie des corps algébriquement clos. Soit D un ultrafiltre non principal construit sur $\mathbb{N}$, on désignera par $(\quad)^*$ le foncteur « ultrapuissance modulo D », qui associe à tout ensemble E l'ensemble des suites $(e_n)_{n\in\mathbb{N}}$, $e_n \in E$, modulo la relation d'équivalence de coïncider sur un ensemble d'indices appartenant à D. On a un plongement naturel $E \hookrightarrow E^*$ par les suites constantes. Pour plus de précision sur les éléments de théorie des modèles on renvoie à [12], et sur les ultraproduits, à [1].

2. Le Frobenius des vecteurs de Witt

Soit $W[\widetilde{\mathbb{F}}_p]$ l'anneau des vecteurs de Witt sur la clôture algébrique $\widetilde{\mathbb{F}}_p$ du corps premier de caractéristique $p > 0$. Soit $W(\widetilde{\mathbb{F}}_p)$ le corps des fractions de $W[\widetilde{\mathbb{F}}_p]$ et v_p sa valuation p-adique. Soit $\rho : \widetilde{\mathbb{F}}_p \to W[\widetilde{\mathbb{F}}_p]$ le système de représentants qui commute aux puissances p-ièmes. Tout $x \in W[\widetilde{\mathbb{F}}_p]$ a une représentation unique $x = \sum_{i=0}^{\infty} \rho(\alpha_i) p^i$, et on a l'automorphisme $\sigma_p : W[\widetilde{\mathbb{F}}_p] \to W[\widetilde{\mathbb{F}}_p]$ défini par $\sigma_p(\sum_{i=0}^{\infty} \rho(\alpha_i) p^i) = \sum_{i=0}^{\infty} \rho(\alpha_i)^p p^i$. On notera aussi σ_p le prolongement à $W(\widetilde{\mathbb{F}}_p)$. Soient $f_1, \ldots, f_m \in W[\widetilde{\mathbb{F}}_p][X_1, \ldots, X_n]_\sigma$ et désignons par S le système d'équations $f_1 = 0, \ldots, f_m = 0$.

Théorème 2.1. *Si, pour tout entier $N \geqslant 1$, il existe $\mathbf{y} \in W[\widetilde{\mathbb{F}}_p]$ tel que $f_i(\mathbf{y}) \equiv 0 \bmod p^N$, $i = 1, \ldots, m$, alors il existe $\mathbf{x} \in W[\widetilde{\mathbb{F}}_p]$ tel que $f_i(\mathbf{x}) = 0$, $i = 1, \ldots, m$.*

Démonstration. Soit (K, σ, v) une extension élémentaire de $(W(\widetilde{\mathbb{F}}_p), \sigma_p, v_p)$ qui soit assez saturée, par exemple une ultrapuissance $(W(\widetilde{\mathbb{F}}_p), \sigma_p, v_p)^*$. Alors il existe $\mathbf{b} \in K$ tel que $v(\mathbf{b}) \geqslant 0$ et $v(f_i(\mathbf{b})) > v(p^n)$ pour tout $n \geqslant 0$, $v(p)$ est le plus petit élément du groupe de valuation de (K, v), le corps résiduel K_v est un corps algébriquement clos de caractéristique p, et σ induit $x \mapsto x^p$ sur K_v (cf. [1], §1). Soit $\dot{v}$ la valuation de K induite par le sous-groupe convexe $\mathbb{Z}v(p)$ et $\dot{V}_K$ l'anneau de cette valuation. On a l'inclusion $W(\widetilde{\mathbb{F}}_p) \subset \dot{V}_K$. On a la valuation naturelle induite par v sur le corps résiduel $K_{\dot{v}}$, son groupe de valuation est $\mathbb{Z}v(p)$ et son corps des restes s'identifie canoniquement avec K_v. L'application naturelle $\dot{V}_K \to K_{\dot{v}}$ induit un plongement de corps valués $W(\widetilde{\mathbb{F}}_p) \hookrightarrow K_{\dot{v}}$, qui est

[2] N.B. L'automorphisme σ de A se prolonge en un automorphisme de $A[\mathbf{X}]_\sigma$, de la façon suggérée par le nom des variables.

[3] Les valuations seront en général des valuations de Krull.

compatible avec l'inclusion $\widetilde{\mathbb{F}}_p \hookrightarrow K_v$. Les applications naturelles ci-dessus sont compatibles avec σ, de sorte que σ induit un automorphisme $\bar{\sigma}$ de $K_{\dot{v}}$ tel que $v(\bar{\sigma}(x)) = v(x)$. Par saturation, $(K_{\dot{v}}, v)$ est un corps valué complet et est donc isomorphe au corps $W(K_v)$ des vecteurs de Witt sur le corps K_v (voir par ex. [11]). Par la propriété universelle des vecteurs de Witt, $W(\widetilde{\mathbb{F}}_p) \hookrightarrow K_{\dot{v}}$ est l'unique plongement de corps valués induit par l'inclusion $\widetilde{\mathbb{F}}_p \hookrightarrow K_v$ et ce plongement est compatible avec σ_p. On a donc le plongement $(W(\widetilde{\mathbb{F}}_p), \sigma_p, v_p) \hookrightarrow (K_{\dot{v}}, \bar{\sigma}, v)$. La construction donne précisément que pour le reste $\bar{\mathbf{b}}$ de $\mathbf{b}$ dans $K_{\dot{v}}$ on a $f_i(\bar{\mathbf{b}}) = 0$ dans $K_{\dot{v}}$, c'est-à-dire $\bar{\mathbf{b}}$ est une solution du système S telle que $v(\bar{\mathbf{b}}) \geqslant 0$. Or, par [3,15,4], $(K_{\dot{v}}, \bar{\sigma}, v)$ est un modèle de la théorie du premier ordre de $(W(\widetilde{\mathbb{F}}_p), \sigma_p, v_p)$, qui est modèle-complète. Ainsi, $(W(\widetilde{\mathbb{F}}_p), \sigma_p, v_p) \hookrightarrow (K_{\dot{v}}, \bar{\sigma}, v)$ donne une extension élémentaire, et le système S doit déjà posséder une solution dans $W[\widetilde{\mathbb{F}}_p]$, tel que voulu. □

3. Le cas général

Le résultat principal, le Théorème 3.2, s'obtient en transposant les arguments du Théorème 2.1 de [1] à l'aide du Lemme 3.3 ci-dessous. Pour le lemme on peut raisonner comme dans le Théorème 4.7 de [4] (voir [3], Lemme 2.1(iii)). Dans le cas classique c'est essentiellement l'observation qu'en caractéristique résiduelle nulle on peut relever le corps résiduel d'un anneau hensélien.

Définition 3.1 [4]. Soit (A, σ) un anneau aux différences qui soit un anneau de valuation. Notons que σ envoie l'idéal maximal des éléments non inversibles sur lui-même et induit un automorphisme du corps résiduel. On dit que (A, σ) est *σ-hensélien,* si pour tout $f \in A[X]_\sigma$, donné par $f(X_0, X_1, \ldots, X_n) \in A[X_0, \ldots, X_n]$ i.e. $f(X) = f(X, \sigma(X), \ldots, \sigma^n(X))$, et pour tout $y \in A$ tel que $f(y)$ est non inversible mais $\frac{\partial f}{\partial X_i}(y, \sigma(y), \ldots, \sigma^n(y))$ est inversible pour au moins un i, il existe alors $x \in A$ tel que $f(x) = 0$ et $x - y$ est non inversible.

L'anneau $(W[\widetilde{\mathbb{F}}_p], \sigma_p)$ est σ-hensélien [3,15,4]. En pratique, pour vérifier cette propriété, on a besoin de la propriété supplémentaire que tout élément de A soit de la forme ub où u est inversible et $\sigma(b) = b$.

Théorème 3.2. *Soit (A, σ) un anneau aux différences qui soit un anneau de valuation discrète de caractéristique nulle σ-hensélien. Soit t une uniformisante de A, soient $f_1, \ldots, f_m \in A[\mathbf{X}]_\sigma$, et $\mathbf{f} = (f_1, \ldots, f_m)$. Alors il existe un entier $N \in \mathbb{N}$, qui dépend de $\mathbf{f}$, tel que pour tout $\alpha \in \mathbb{N}, \alpha > 0$, et pour tout $\mathbf{x} \in A$ tel que $\mathbf{f}(\mathbf{x}) \equiv 0 \mod t^{\alpha N}$, il existe $\mathbf{y} \in A$ tel que $\mathbf{f}(\mathbf{y}) = 0$ et $\mathbf{y} \equiv \mathbf{x} \mod t^\alpha$.*

Considérons la valuation v associée à A, dont le groupe de valuation est $\mathbb{Z}$, et posons $k = A/(t)$ son corps résiduel.

Lemme 3.3 (cf. [1], Lemme 2.2). *Soit D un ultrafiltre non principal construit sur $\mathbb{N}$ et appliquons le foncteur $(\quad)^*$ pour obtenir l'anneau de valuation σ-hensélien A^* avec la valuation associée v^* dont le groupe de valuation est $\mathbb{Z}^*$ et le corps résiduel est $k^* = A^*/(t)$. Soit H un sous-groupe convexe de $\mathbb{Z}^*$ qui contient $\mathbb{Z}$, et soit $I_H = \{x \in A^*\colon\ v^*(x) \notin H\}$, $A^H = A^*/I_H$, et $A^* \xrightarrow{\pi} A^H$, $A \xrightarrow{i} A^*$ les applications naturelles. Alors A^H se relève en un sous-anneau aux différences de A^*, i.e. il existe un homomorphisme d'anneaux aux différences $A^H \xrightarrow{\psi} A^*$ tel que $\pi\psi = \mathrm{id}_{A^H}$ et $\psi|_A = i$.*

Par les mêmes méthodes on obtient un analogue de [9] (cf. [1]). Dans tous ces résultats, les mêmes remarques que dans [1] sur l'existence de bornes théoriquement calculables s'appliquent.

[4] Cette version [15] est équivalente à celle de [3,4].

4. Application à un théorème des zéros

On utilise la notation de [2]. Dans un corps aux différences (K,σ) on considère le sous-groupe multiplicatif $G_{\sigma,K}=\{\sigma(x)x^{-1}\colon x\in K^\times\}$ et la fonction $\gamma_\sigma(x)=\frac{1}{p}\frac{\sigma(x)-x^p}{(\sigma(x)-x^p)^2-1}$, où p est un nombre premier fixé. Pour un corps K, $K(\mathbf{X})_\sigma$ désigne le corps des fractions de $K[\mathbf{X}]_\sigma$.

Définition 4.1 (cf. [10]). Soit (K,σ,v) un corps aux différences valué et $r\in K(\mathbf{X})_\sigma$. On dit que r est *régulière sur* V_K s'il existe $\lambda\in K^\times$ tel que $v(r(\mathbf{a}))\geqslant v(\lambda)$, pour tout $\mathbf{a}\in V_K$ tel que $r(\mathbf{a})$ est défini.

Proposition 4.2. *Soit*[5] $(K,\sigma,v)=(W(\widetilde{\mathbb{F}}_p),\sigma_p,v_p)$, *soient* $r\in K(\mathbf{X})_\sigma$, $A=\mathbb{Z}[\mathbf{X},\gamma_\sigma(K(\mathbf{X})_\sigma),G_{\sigma,K(\mathbf{X})_\sigma}]$ *et l'anneau de fractions* $R=A[(1+pA)^{-1}]$. *Alors* r *est régulière sur* V_K *si et seulement si* r *est entier sur l'anneau* $R\cdot K$.

Par [2], $v(\lambda^{-1}r(\mathbf{a}))\geqslant 0$, pour tout $\mathbf{a}\in V_K$ tel que $r(\mathbf{a})$ est défini, si et seulement si $\lambda^{-1}r$ est entier sur l'anneau R, d'où le résultat. Le lemme suivant découle immédiatement du Théorème 2.1. On raisonne alors comme dans le Lemme 5 de [10] pour déduire un théorème des zéros analogue.

Lemme 4.3. *Soit* (K,σ,v) *comme dans la proposition et* $h\in K[\mathbf{X}]_\sigma$. *Alors* h *n'a aucun zéro dans* V_K *si et seulement si* h^{-1} *est régulière sur* V_K.

Théorème 4.4 (Théorème des zéros). *Soient* K *et* R *comme dans la proposition précédente et soient* $f_1,\dots,f_m\in K[\mathbf{X}]_\sigma$. *Si* $f_1,\dots,f_m$ *n'ont aucun zéro commun dans* V_K, *alors* $(f_1,\dots,f_m)_{R\cdot K[\mathbf{X}]_\sigma}=R\cdot K[\mathbf{X}]_\sigma$, *où* $(f_1,\dots,f_m)_{R\cdot K[\mathbf{X}]_\sigma}$ *désigne l'idéal engendré par les* f_i *dans l'anneau* $R\cdot K[\mathbf{X}]_\sigma$.

Démonstration. Posons $f=\sum_{i=1}^m p^{i-1}f_i^m$, alors $f(\mathbf{a})=0$ ssi $f_1(\mathbf{a})=0,\dots,f_m(\mathbf{a})=0$. Ainsi f n'a aucun zéro dans V_K et f^{-1} est entier sur l'anneau $R\cdot K$. Mais alors f^{-1} doit déjà appartenir à $R\cdot K[\mathbf{X}]_\sigma$, car f^{-1} est dans le corps des fractions de $R\cdot K[\mathbf{X}]_\sigma$ (cf. [10]). Il existe donc $g\in R\cdot K[\mathbf{X}]_\sigma$ tel que $gf=1$, c.-à-d. $\sum_{i=1}^m gp^{i-1}f_i^{m-1}f_i=1$. Mais $gp^{i-1}f_i^{m-1}\in R\cdot K[\mathbf{X}]_\sigma$, d'où le résultat. □

Références

[1] J. Becker, J. Denef, L. Lipshitz, L. van den Dries, Ultraproducts and approximation in local rings I, Invent. Math. 51 (1979) 189–203.
[2] L. Bélair, Fonctions rationnelles aux différences à valeurs entières dans les vecteurs de Witt, C. R. Acad. Sci. Paris, Ser. I 339 (2004) 83–86.
[3] L. Bélair, A. Macintyre, L'automorphisme de Frobenius des vecteurs de Witt, C. R. Acad. Sci. Paris, Ser. I 331 (2000) 1–4.
[4] L. Bélair, A. Macintyre, T. Scanlon, Model theory of Frobenius on Witt vectors, prépublication, http://132.208.138.87//_belair/.
[5] A. Buium, An approximation property for Teichmüller points, Math. Res. Lett. 3 (1996) 453–457.
[6] R.M. Cohn, Difference Algebra, Wiley, 1965.
[7] A. Duval, Lemmes de Hensel et factorisation formelle pour les opérateurs aux différences, Funkcial. Ekvac. 26 (1983) 349–368.
[8] M. Greenberg, Rational points in henselian discrete valuation rings, Publ. Math. IHES 31 (1966) 59–64.
[9] M. Greenberg, Strictly local solutions of Diophantine equations, Pacific J. Math. 51 (1974) 143–153.
[10] S. Kochen, Integral valued rational functions over the p-adic numbers: a p-adic analogue of the theory of real fields, in: Proc. Sympos. Pure Math., vol. XII, American Mathematical Society, 1969, pp. 57–73.
[11] S. Kochen, The model theory of local fields, in: Logic Conference, Kiel, 1974, in: Lecture Notes in Math., vol. 499, Springer, 1975, pp. 384–425.
[12] D. Marker, Model Theory: An Introduction, Springer, 2002.
[13] D. Popescu, Artin approximation, in: M. Hazewinkel (Ed.), Handbook of Algebra, vol. 2, Elsevier, 2003, pp. 321–356.
[14] A. Robinson, Elementary embeddings of fields of power series, J. Number Theory 2 (1970) 237–247.
[15] T. Scanlon, Quantifier elimination for the relative Frobenius, in: F.-V. Kuhlmann, et al. (Eds.), Valuation Theory and its Applications, vol. II (Saskatoon, SK, 1999), American Mathematical Society, 2003, pp. 323–352.

[5] Ou encore (K,σ,v) *élémentairement équivalent* à $(W(\widetilde{\mathbb{F}}_p),\sigma_p,v_p)$, i.e. modèle de la théorie du premier ordre de $(W(\widetilde{\mathbb{F}}_p),\sigma_p,v_p)$.