Available online at www.sciencedirect.com
SCIENCE DIRECT
C. R. Acad. Sci. Paris, Ser. I 339 (2004) 83–86
Comptes Rendus Mathematique

Logique/Algèbre

Fonctions rationnelles aux différences à valeurs entières 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 26 avril 2004 ; accepté le 27 avril 2004

Disponible sur Internet le 17 juin 2004

Présenté par Jean-Yves Girard

Résumé

On transpose les résultats de Kochen sur les fonctions rationnelles p-adiques à valeurs entières, aux fonctions rationnelles aux différences de l'automorphisme de Frobenius des vecteurs de Witt. ***Pour citer cet article : L. Bélair, C. R. Acad. Sci. Paris, Ser. I 339 (2004).***

Abstract

Integral valued difference rational functions over Witt vectors. We transpose Kochen's results on integral valued rational functions over the p-adic numbers to difference rational functions over the Witt vectors with their Frobenius. ***To cite this article: L. Bélair, C. R. Acad. Sci. Paris, Ser. I 339 (2004).***

1. Introduction

Dans son très bel article [5], Kochen donne un analogue p-adique du 17e problème de Hilbert en caractérisant les fonctions rationnelles p-adiques à valeurs dans les entiers p-adiques : ce sont les f qui satisfont une relation[1] de la forme $f^n + \sum_{i=0}^{n-1} a_i f^i = 0$, où $a_i = \frac{s_i}{1+pt_i}$, $s_i, t_i \in \mathbb{Z}[\gamma(\mathbb{Q}_p(x_1, \ldots, x_l))]$, $\gamma(x) = \frac{1}{p}\frac{x-x^p}{(x-x^p)^2-1}$. Dans l'analogue p-adique, le rôle du carré $x \mapsto x^2$ est joué par la fonction $\gamma(x)$, qui prend toutes ses valeurs dans les entiers p-adiques. Soit $W(k)$ le corps des vecteurs de Witt sur un corps parfait k de caractéristique $p > 0$, soit v_p sa valuation p-adique, et soit Frob le relèvement continu de l'automorphisme de Frobenius, $x \mapsto x^p$, de k à $W(k)$. Soit $\widetilde{\mathbb{F}}_p$ la clôture algébrique du corps premier $\mathbb{F}_p$. Les articles [1,2,8] indiquent que les modèles de la théorie élémentaire de $(W(\widetilde{\mathbb{F}}_p), \mathrm{Frob}, v_p)$ fournissent des domaines universels pour la théorie des p-jets de Buium [3]. Soit $\gamma_{\mathrm{Frob}}(x) = \frac{1}{p}\frac{\mathrm{Frob}(x)-x^p}{(\mathrm{Frob}(x)-x^p)^2-1}$. On sait que pour $x \in W(k)$ on a $v_p(\mathrm{Frob}(x)) = v_p(x)$ et on vérifie aussi que

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

[1] Pour le raffinement $n = 1$, qui rend l'analogie plus étroite encore, voir [7].

1631-073X/$ – see front matter
doi:10.1016/j.crma.2004.04.017

$v_p(\gamma_{\mathrm{Frob}}(x)) \geqslant 0$. A l'aide de γ_{Frob} et pour $k = \widetilde{\mathbb{F}}_p$, nous transposons les résultats de Kochen aux fonctions rationnelles aux différences de Frob (Théorème 3.5). Des résultats semblables s'obtiennent pour des corps aux différences valués (voir la définition ci-dessous) dont la théorie est modèle-complète (voir [2,8]) et avec un groupe de valuation discret.[2]

Un corps aux différences est un corps muni d'un automorphisme. Dans ce contexte on notera généralement l'automorphisme σ. Dans un corps aux différences (K, σ) on considère le sous-groupe multiplicatif $G_{\sigma,K} = \{\sigma(x)x^{-1} : x \in K^\times\}$. On note $\mathbf{x}$ le n-uplet $(x_1, \dots, x_n)$. Pour un corps valué (K, v), vK désigne son groupe de valuation, V_K son anneau de valuation, $resK$ son corps des restes et $max(V_K)$ l'idéal maximal de V_K. Un corps p-valué non ramifié est un corps valué de caractéristique 0 dont la valuation prolonge la valuation p-adique sur $\mathbb{Q}$ et où p engendre l'idéal maximal de la valuation. Un élément x est dit entier sur un anneau A s'il satisfait une relation de la forme $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$, avec $a_i \in A$. On note $\mathcal{M} \equiv \mathcal{N}$ le fait que $\mathcal{M}, \mathcal{N}$ sont élémentairement équivalents. Pour les éléments de théorie des modèles, on renvoie à [6].

2. Corps aux différences valués

Définition 2.1. (i) 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 [4]). On notera (K, σ, v) une telle structure.

(ii) Un corps aux différences valué sera dit *wittien* s'il est p-valué non ramifié et tel que $v(\sigma(x) - x^p) > 0$ pour tout x tel que $v(x) \geqslant 0$. Notons que $(\mathbb{Q}, \mathrm{id})$ est wittien pour la valuation p-adique.

(iii) Soit (k, σ, v) un corps aux différences valué wittien, et (K, σ) une extension de (k, σ). On dira que K est *formellement wittien sur* k s'il existe une valuation qui fait de (K, σ) un corps aux différences valué wittien et qui prolonge la valuation de k. On désignera par $W_{K/k}$ l'ensemble de ces valuations sur K. Un corps aux différences sera dit *formellement wittien* s'il est formellement wittien sur $\mathbb{Q}$.

(iv) Pour p fixé, on définit dans les corps aux différences la fonction

$$\gamma_\sigma(x) = \frac{1}{p} \frac{\sigma(x) - x^p}{(\sigma(x) - x^p)^2 - 1}.$$

Notons qu'une valuation v sur un corps aux différences (K, σ) en fait un corps aux différences valué si et seulement si le groupe multiplicatif $G_{\sigma,K}$ est tel que $v(G_{\sigma,K}) \geqslant 0$.

Lemme 2.2 [2]. *Tout corps wittien possède une extension qui est élémentairement équivalente à* $(W(\widetilde{\mathbb{F}}_p), \mathrm{Frob}, v_p)$.

Lemme 2.3. *Soit* (K, σ, v) *un corps aux différences valué de caractéristique* 0 *tel que* $v(p) > 0$. *Alors* (K, σ, v) *est wittien si et seulement si* $v(\gamma_\sigma(K)) \geqslant 0$.

Preuve. $(\Rightarrow)$. Si $v(x) \geqslant 0$: alors $v(\sigma(x) - x^p) > 0$ et $v(\gamma_\sigma(x)) = v(\sigma(x) - x^p) - v(p) \geqslant 0$. Si $v(x) < 0$: alors $v(\sigma(x) - x^p) = v(x^p) < 0$ et $v(\gamma_\sigma(x)) = -v(x^p) - v(p) \geqslant 0$. $(\Leftarrow)$. On a $v(p) > 0$. Soit $a \in K$ tel que $0 < v(a) \leqslant v(p)$. Puisque $v(a) > 0$ on obtient $v(\frac{\sigma(a)-a^p}{(\sigma(a)-a^p)^2-1}) = v(a) > 0$, d'où $v(\gamma_\sigma(a)) = v(a) - v(p) \geqslant 0$, et donc $v(a) = v(p)$. Ainsi $v(p)$ est le plus petit élément positif de vK. Vérifions que $v(x) \geqslant 0$ entraîne $v(\sigma(x) - x^p) > 0$. Si $v(x) > 0$, alors $v(\sigma(x) - x^p) = v(\sigma(x)) = v(x) > 0$. Si $v(x) = 0$, alors $v(\sigma(x) - x^p) \geqslant 0$; on ne peut avoir $v(\sigma(x) - x^p) = 0$ sinon on aurait $v(\gamma_\sigma(x)) < 0$, ce qui n'est pas le cas par hypothèse.

[2] Un autre cas remarquable, mais « direct », est celui où k est un corps fini. La modèle-complétude se déduit de *Fix*(Frob) $= \mathbb{Q}_p$ et $[W(k) : \mathbb{Q}_p] = [k : \mathbb{F}_p]$, et de celle de $\mathbb{Q}_p$.

Lemme 2.4 ([5], Lemme 3). *Soit K un corps valué, L/K une extension de K, A un sous-anneau de L tel que $V_K = A \cap K$. Soit $T = \{1 + ma\colon\ m \in \max(V_K), a \in A\}$. Alors la clôture intégrale du localisé A_T est égale à l'intersection de tous les anneaux de valuation V_L de L tels que $A \subseteq V_L$ et $V_K = V_L \cap K$.*

Kochen note que si K est p-valué non ramifié alors $T = 1 + pA$ et $\frac{1}{p} \in A_T$ entraîne $\frac{1}{p} \in A$, et aussi que si R est sous-anneau d'un corps k et $x \in R$, alors x^{-1} est entier sur R si et seulement si $x^{-1} \in R$. Dans la suite, si A est un anneau alors A_T désignera l'anneau de fractions $A[(1 + pA)^{-1}]$.

Proposition 2.5. *Soit (k, σ, v) wittien et (K, σ) une extension de (k, σ). Alors K est formellement wittien sur k si et seulement si $\frac{1}{p} \notin V_k[\gamma_\sigma(K), G_{\sigma,K}]$.*

Preuve. ($\Rightarrow$). Soit V_K un anneau de valuation qui rend (K, σ) wittien sur k. On a $\gamma_\sigma(K) \subseteq V_K$ par le lemme précédent et donc $V_k[\gamma_\sigma(K), G_{\sigma,K}] \subseteq V_K$. Comme $\frac{1}{p} \notin V_K$, on a $\frac{1}{p} \notin V_k[\gamma_\sigma(K), G_{\sigma,K}]$.

($\Leftarrow$). Supposons $\frac{1}{p} \notin V_k[\gamma_\sigma(K), G_{\sigma,K}]$, alors $V_k = V_k[\gamma_\sigma(K), G_{\sigma,K}] \cap k$ et par les remarques précédentes $\frac{1}{p}$ n'est pas entier sur $V_k[\gamma_\sigma(K), G_{\sigma,K}]_T$. Par le lemme de Kochen il existe un anneau de valuation V_K de K tel que $V_k[\gamma_\sigma(K), G_{\sigma,K}] \subseteq V_K$ et $p \in max(V_K)$. La valuation v de V_K est la valuation cherchée. En effet, $G_{\sigma,K} \subseteq V_K$ assure que (K, σ, v) est un corps aux différences valué, et (K, σ, v) est wittien par la proposition précédente.

Proposition 2.6. *Soit (K, σ, v) wittien, (L, σ) une extension de (K, σ) tel que $W_{L/K} \neq \emptyset$, soit $a \in L$ et $S \subseteq L \setminus K$. Alors $v(a) \geqslant 0$ pour tout $v \in W_{L/K}$ tel que $v(S) \geqslant 0$ si et seulement si a est entier sur $V_K[\gamma_\sigma(L), G_{\sigma,L}, S]_T$.*

Preuve. Par le lemme ci-dessus, a est entier sur $V_K[\gamma_\sigma(L), G_{\sigma,L}, S]_T$ ssi pour toute extension de la valuation de K à L telle que $V_K[\gamma_\sigma(L), G_{\sigma,L}, S]_T \subseteq V_L$ on ait $a \in V_L$. Or, par le Lemme 2.3, $V_K[\gamma_\sigma(L), G_{\sigma,L}, S]_T \subseteq V_L$ est équivalent à ce que la valuation sur L soit wittienne et $S \subseteq V_L$.

Lemme 2.7. *Si $(K, \sigma, v) \equiv (W(\widetilde{\mathbb{F}}_p), \mathrm{Frob}, v_p)$ alors $V_K = \gamma_\sigma(K)$.*

Preuve. Soit $a \in V_K$, l'équation $a = \gamma_\sigma(x)$ se ramène à $ap(\sigma(x) - x^p)^2 - (\sigma(x) - x^p) - ap = 0$. Posons $z = \sigma(x) - x^p$. L'équation $apz^2 - z - ap = 0$ a une solution ssi $1 + 4a^2p^2$ est un carré, ce qui est bien le cas, directement par le lemme de Hensel pour $p \neq 2$, et en allant mod 8 pour $p = 2$. Une des deux solutions z_1, z_2 doit être telle que $v(z_i) > 0$ car $v(z_1z_2) = v(-1) = 0$ et $v(z_1 + z_2) = v(pa^{-1}) < 0$. De là, l'équation $\sigma(x) - x^p = z_i$ a une solution par le lemme de Hensel pour les équations aux différences [4,1,8,2], et on a la solution cherchée.

Corollaire 2.8. *Soit $(K, \sigma, v) \equiv (W(\widetilde{\mathbb{F}}_p), \mathrm{Frob}, v_p)$, et (L, σ) une extension de (K, σ) tel que $W_{L/K} \neq \emptyset$, et soit $a \in L$. Alors $v(a) \geqslant 0$ pour tout $v \in W_{L/K}$ si et seulement si a est entier sur $\mathbb{Z}[\gamma_\sigma(L), G_{\sigma,L}]_T$.*

3. Fonctions rationnelles aux différences

Dans ce qui suit, $K[\mathbf{X}]_\sigma$ désigne l'anneau des polynômes aux différences en les indéterminées $X_1, \ldots, X_n$, et $K(\mathbf{X})_\sigma$ son corps des fractions. Par exemple, pour $n = 1$, $f(X) \in K[X]_\sigma$ est de la forme $f(X) = \sum a_{ij}(\sigma^i(X))^j$. Notons que si K est wittien alors $K(\mathbf{X})_\sigma$ est formellement wittien sur K, puisque par un argument de compacité, on peut aller à une extension élémentaire de K qui contienne des x_l tels que tous les $\sigma^i(x_l)$ soient algébriquement indépendants sur K.

Définition 3.1. Soit (K, σ, v) un corps aux différences valué, soit $r \in K(\mathbf{X})_\sigma$ et S une partie finie de $K(\mathbf{X})_\sigma$. On dit que r est à valeurs S-entières, si pour tout $a \in K^n$, ou bien $r(a)$ n'est pas défini ou bien $v(r(a)) \geqslant 0$ dès que pour chaque $s \in S$, $s(a)$ est ou bien non défini ou bien $v(s(a)) \geqslant 0$.

La proposition suivante découle du Lemme 2.2.

Proposition 3.2. *Soit (K,σ,v) wittien, et soit $r\in K(\mathbf{X})_\sigma$ et S une partie finie de $K(\mathbf{X})_\sigma$. Si r est à valeurs S-entières dans toute extension de (K,σ,v) qui est élémentairement équivalente à $(W(\widetilde{\mathbb{F}}_p),\mathrm{Frob},v_p)$, alors $v(r)\geqslant 0$ pour tout $v\in W_{K(\mathbf{X})_\sigma/K}$ tel que $v(S)\geqslant 0$.*

Comme la théorie du premier ordre de $(W(\widetilde{\mathbb{F}}_p),\mathrm{Frob},v_p)$ est modèle-complète [1,8,2] on obtient la proposition suivante.

Proposition 3.3. *Soit $(K,\sigma,v)\equiv(W(\widetilde{\mathbb{F}}_p),\mathrm{Frob},v_p)$, et soit $r\in K(\mathbf{X})_\sigma$ et S une partie finie de $K(\mathbf{X})_\sigma$. Alors r est à valeurs S-entières dans K si et seulement si r est à valeurs S-entières dans toute extension de (K,σ,v) qui est élémentairement équivalente à $(W(\widetilde{\mathbb{F}}_p),\mathrm{Frob},v_p)$.*

Des Propositions 2.6, 3.2, 3.3 et du Lemme 2.7, on déduit les résultats principaux de cette note.

Théorème 3.4. *Soit (K,σ,v) un sous-corps de $(W(\widetilde{\mathbb{F}}_p),\mathrm{Frob},v_p)$ tel que $\mathrm{res}\,K=\widetilde{\mathbb{F}}_p$. Soit $r\in K(\mathbf{X})_\sigma$ et S une partie finie de $K(\mathbf{X})_\sigma$. Alors r est à valeurs S-entières dans K si et seulement si r est entier sur $V_K[\gamma_\sigma(K(\mathbf{X})_\sigma),G_{\sigma,K(\mathbf{X})_\sigma},S]_T$.*

Preuve. On a que K est dense dans $W(\widetilde{\mathbb{F}}_p)$ et $(W(\widetilde{\mathbb{F}}_p),\mathrm{Frob},v_p)$ se plonge dans tout extension ω_1-saturée de (K,σ,v) qui est élémentairement équivalente à $(W(\widetilde{\mathbb{F}}_p),\mathrm{Frob},v_p)$ (voir [1,8,2]).

Théorème 3.5. *Soit $(K,\sigma,v)\equiv(W(\widetilde{\mathbb{F}}_p),\mathrm{Frob},v_p)$, et soit $r\in K(\mathbf{X})_\sigma$ et S une partie finie de $K(\mathbf{X})_\sigma$. Alors r est à valeurs S-entières dans K si et seulement si r est entier sur $\mathbb{Z}[\gamma_\sigma(K(\mathbf{X})_\sigma),G_{\sigma,K(\mathbf{X})_\sigma},S]_T$.*

Corollaire 3.6. *Soit $(K,\sigma,v)\equiv(W(\widetilde{\mathbb{F}}_p),\mathrm{Frob},v_p)$.*

(i) *$(S=\emptyset)$ r est à valeurs entières dans K si et seulement si r est entier sur $\mathbb{Z}[\gamma_\sigma(K(\mathbf{X})_\sigma),G_{\sigma,K(\mathbf{X})_\sigma}]_T$.*
(ii) *$(S=\{\mathbf{X}\})$ r est à valeurs entières sur V_K si et seulement si r est entier sur $\mathbb{Z}[\mathbf{X},\gamma_\sigma(K(\mathbf{X})_\sigma),G_{\sigma,K(\mathbf{X})_\sigma}]_T$.*

Remerciements

Je remercie l'Équipe de logique mathématique CNRS de l'Université Paris 7 pour son hospitalité, de septembre 2002 à juillet 2003.

Références

[1] L. Bélair, A. Macintyre, L'automorphisme de Frobenius des vecteurs de Witt, C. R. Acad. Sci. Paris, Sér. I 331 (2000) 1–4.
[2] L. Bélair, A. Macintyre, T. Scanlon, Model theory of Frobenius on Witt vectors, prépublication http://132.208.138.87//_belair/.
[3] A. Buium, Geometry of p-jets, Duke Math. J. 82 (1996) 349–367.
[4] A. Duval, Lemmes de Hensel et factorisation formelle pour les opérateurs aux différences, Funkcial. Ekvac. 26 (1983) 349–368.
[5] S. Kochen, Integral valued rational functions over the p-adic numbers: a p-adic analogue of the theory of real fields, in: Proc. Symposia Pure Maths XII, American Mathematical Society, 1969, pp. 57–73.
[6] D. Marker, Model Theory: An Introduction, Springer, 2002.
[7] A. Prestel, P. Roquette, Formally p-Adic Fields, Springer, 1984.
[8] T. Scanlon, Quantifier elimination for the relative Frobenius, in: F.-V. Kuhlmann, S. Kuhlmann, M. Marshall (Eds.), Valuation Theory and its Applications, vol. II, American Mathematical Society, 2003.