C. R. Acad. Sci. Paris, t. 331, Série I, p. 1–4, 2000
Logique/*Logic*
(Algèbre/*Algebra*)

L'automorphisme de Frobenius des vecteurs de Witt

Luc BÉLAIR [a], Angus MACINTYRE [b]

[a] Département de mathématiques, Université du Québec, Montréal, Québec, H3C 3P8, Canada
Courriel : belair.luc@uqam.ca

[b] Department of mathematics and statistics, University of Edinburgh, Edinburgh, EH9 3JZ, Scotland, UK
Courriel : angus@maths.ed.ac.uk

(Reçu le 12 janvier 2000, accepté après révision le 17 avril 2000)

Résumé. On axiomatise la théorie du premier ordre de l'automorphisme de Frobenius du corps des vecteurs de Witt sur la clôture algébrique d'un corps fini. © 2000 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

The Frobenius automorphism of Witt vectors

Abstract. *We give an axiomatization of the first-order theory of the field of Witt vectors over the algebraic closure of a finite field, with the lifting of the Frobenius map.* © 2000 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

1. Introduction

La théorie du premier ordre du corps des vecteurs de Witt sur la clôture algébrique d'un corps fini de caractéristique p est bien connue depuis les travaux de Ax-Kochen et Ershov : la valuation p-adique se définit algébriquement par $v_p(x) \geqslant 0 \leftrightarrow \exists\, y\ (1 + px^{\varepsilon} = y^{\varepsilon})$, où ε est un entier premier avec p, et on obtient un système complet d'axiomes en disant qu'on a un corps p-valué non ramifié hensélien dont le corps des restes est un corps algébriquement clos de caractéristique p et le groupe de valuation un $\mathbf{Z}$-groupe. Désignons ces axiomes par W_p. Dans cette Note, on axiomatise la théorie du premier ordre obtenue en munissant les vecteurs de Witt du relèvement de l'automorphisme de Frobenius du corps des restes. On obtient une théorie décidable et modèle-complète. Il y a aussi une élimination des quantificateurs (*voir* ci-dessous). Ces résultats ont été obtenus indépendamment par T. Scanlon [6]. Les modèles de cette théorie devraient fournir les domaines universels dans la théorie des p-jets de Buium (*voir* [2]).

On note $\mathrm{W}(k)$ le corps des vecteurs de Witt sur un corps parfait k de caractéristique $p > 0$, v_p sa valuation p-adique, $\mathrm{W}[k]$ son anneau de valuation, $\overline{x} \in k$ le reste de $x \in \mathrm{W}[k]$, et Frob le relèvement continu de l'automorphisme de Frobenius $x \mapsto x^p$ de k à $\mathrm{W}(k)$. On utilise [3]. Pour $x \in \mathrm{W}[k]$, soit $\delta(x) = (\mathrm{Frob}\,(x) - x^p)/p$, alors on a les identités $\delta(1) = 0$, $\delta(x+y) = \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} x^i y^{p-i}$, $\delta(xy) = x^p\delta(y) + \delta(x)y^p + p\delta(x)\delta(y)$. Un δ-anneau est un anneau commutatif muni d'une opération unaire vérifiant ces identités. Le foncteur de construction des vecteurs de Witt est un adjoint à droite du foncteur d'oubli des δ-anneaux dans les anneaux commutatifs. Dans un δ-anneau, $f(x) = x^p + p\delta(x)$ est un endomorphisme. On peut définir dans la théorie des δ-anneaux une suite unique d'opérations unaires

Note présentée par Jacques TITS.

S0764-4442(00)00501-2/FLA

$\delta_0,\ \delta_1,\ \delta_2,\ldots$ vérifiant les identités $f^n(x)=\delta_0(x)^{p^n}+p\delta_1(x)^{p^{n-1}}+\cdots+p^n\delta_n(x)$. On a $\delta_0(x)=x$, $\delta_1(x)=\delta(x)$. Dans $\mathrm{W}[k]$, les δ_n donnent les *composantes* des vecteurs de Witt, à savoir, $x\in\mathrm{W}[k]$ s'identifie à $(\delta_0(x),\delta_1(x),\delta_2(x),\ldots)$.

Nous appellerons les corps munis d'un automorphisme σ, des σ-corps. Dans un σ-corps, $\mathrm{Fix}(\sigma)$ désigne le sous-corps des invariants de σ et $K(a)_\sigma$ le σ-corps engendré par $K(a)$. On note $\mathbf{x}$ le n-uplet $(x_1,\ldots,x_n)$. Pour un corps valué (K,v), vK désigne son groupe de valuation, V_K son anneau de valuation, $\mathrm{res}\,K$ son corps des restes et $\overline{x}$ le reste de x si $v(x)\geqslant 0$. Un corps p-valué non ramifié est un corps valué de caractéristique 0 dont la valuation prolonge la valuation p-adique sur $\mathbf{Q}$ et où p engendre l'idéal maximal de la valuation.

2. Corps valués munis d'un automorphisme

Nous appellerons *σ-corps valué* un corps valué muni d'un automorphisme σ tel que $v(\sigma(x))=v(x)$. Dans ces corps un schéma d'axiomes, noté σH^*, jouera le rôle du lemme de Hensel. Pour un polynôme $F(X,X_1,\ldots,X_n)$, soit $F(X)=F(X,\sigma(X),\ldots,\sigma^n(X))$ (on appellera *σ-polynôme* un tel polynôme) et les $D_{\mathbf{j}}$ définis par l'équation $F(X+h,X_1+h_1,\ldots,X_n+h_n)=\sum_{\mathbf{j}}D_{\mathbf{j}}F(\mathbf{X})\,\mathbf{h}^{\mathbf{j}}$. Alors le schéma σH^* exprime que, pour tout $F(X,X_1,\ldots,X_n)$, s'il existe α et γ tels que

$$v\big(F(\alpha,\sigma(\alpha),\ldots,\sigma^n(\alpha)\big)=\min_{1\leqslant j\leqslant n}v\left(\frac{\partial F}{\partial X_j}\big(\alpha,\sigma(\alpha),\ldots,\sigma^n(\alpha)\big)\right)+\gamma,$$

et si, pour tout $k>1$, on a $\min_{|\mathbf{j}|=k}\ v(D_{\mathbf{j}}F(\alpha))+k\gamma>\min_{|\mathbf{j}|=1}\ v(D_{\mathbf{j}}F(\alpha))+\gamma$, alors il existe α' tel que $F(\alpha')=0$ et $v(\alpha'-\alpha)=\gamma$.

LEMME 2.1. – (i) *Soient (L_1,v,σ), (L_2,v,σ) des σ-corps valués henséliens, $(K_i,v,\sigma)\subseteq(L_i,v,\sigma)$, $i=1,2$, et $f:(K_1,v,\sigma)\to(K_2,v,\sigma)$ un σ-isomorphisme de corps valués. Alors les hensélisés K_i^h sont clos par rapport à σ et f se prolonge en un σ-isomorphisme de corps valués $f^h:(K_1^h,v,\sigma)\to(K_2^h,v,\sigma)$.*

(ii) *Soit (K,v,σ) un σ-corps valué satisfaisant le schéma σH^*, Δ un sous-groupe convexe de vK et $\dot v$ la valuation sur K induite par Δ. Alors $(K,\dot v,\sigma)$ satisfait aussi le schéma σH^*.*

(iii) *Soit (K,v,σ) un σ-corps valué satisfaisant le schéma σH^* et avec un corps des restes de caractéristique 0. Alors il existe un sous-corps $K_0\subset K$ tel que $\sigma(K_0)=K_0$, $v(\sigma(K_0))=0$ et l'application de passage au reste induit un isomorphisme de K_0 sur le corps des restes.*

Voici le résultat clef pour adapter les méthodes habituelles.

PROPOSITION 2.2. – *Soit (K,v,σ) un σ-corps p-valué non ramifié tel que σ relève l'application $x\mapsto x^p$ du corps des restes, $v(\mathrm{Fix}(\sigma))=vK$ et $\mathrm{res}\,K$ est infini. Soit $(a_\rho)\in K$ une suite pseudoconvergente qui converge vers une pseudolimite α dans une extension immédiate (L,v,σ) de K. Soient $F_1(X),\ldots,F_t(X)$ des σ-polynômes sur K. Alors il existe une suite pseudoconvergente $(a'_\rho)\in K$ telle que $a'_\rho\to\alpha$, $F_i(a'_\rho)\to F_i(\alpha)$, $i=1,\ldots,t$, et (a'_ρ) possède les mêmes pseudolimites que (a_ρ).*

Démonstration. – On traite le cas d'un seul $F(X)$. Soit $v(a_\rho-\alpha)=\gamma_\rho=v(\theta_\rho)$, où (γ_ρ) est asymptotiquement croissante et $\theta_\rho\in\mathrm{Fix}(\sigma)$. Posons $a'_\rho=a_\rho+\theta_\rho d_\rho$, où d_ρ est à déterminer tel que $v(d_\rho)=0$. Considérons

$$\begin{aligned}F(a'_\rho)-F(\alpha)&=\sum_{\mathbf{j}}c_{\mathbf{j}}(a'_\rho-\alpha)^{j_0}\cdots\sigma^n(a'_\rho-\alpha)^{j_n}\\&=\sum_m\sum_{|\mathbf{j}|=m}c_{\mathbf{j}}(a_\rho-\alpha+\theta_\rho d_\rho)^{j_0}\cdots\sigma^n(a_\rho-\alpha+\theta_\rho d_\rho)^{j_n}.\end{aligned}$$

Posons $a_\rho-\alpha=\theta_\rho e_\rho$, $v(e_\rho)=0$, et soit $c_{\mathbf{j}_m}$ tel que $v(c_{\mathbf{j}_m})=\min_{|\mathbf{j}|=m}v(c_{\mathbf{j}})$. On obtient

$$F(a'_\rho)-F(\alpha)=\sum_m c_{\mathbf{j}_m}\left[\sum_{|\mathbf{j}|=m}c'_{\mathbf{j}}(e_\rho+d_\rho)^{j_0}\cdots\sigma^n(e_\rho+d_\rho)^{j_n}\right]\theta_\rho^m,$$

où $v(c'_{\mathbf{j}}) \geqslant 0$ et $v(c'_{\mathbf{j}}) = 0$ au moins une fois. Considérons le σ-polynôme $F_m(Z) = \sum_{|\mathbf{j}|=m} c'_{\mathbf{j}} Z^{j_0} \cdots \sigma^n(Z)^{j_n}$. En utilisant les identités $\sigma^i(Z) = Z^{p^i} + p\delta_1(Z)^{p^{i-1}} + \cdots + p^i\delta_i(Z)$, on obtient $F_m(Z) = G_m(Z, \delta_1(Z), \ldots, \delta_n(Z))$, où $G_m(Z, Z_1, \ldots, Z_n)$ est un polynôme sur V_L, non nul si F_m n'est pas nul (*cf.* [3], proposition 2). Soit c_m un coefficient de G_m de valuation minimum, alors on a $G_m(Z, \delta_1(Z), \ldots, \delta_n(Z)) = c_m H_m(Z, \delta_1(Z), \ldots, \delta_n(Z))$, où le polynôme $\overline{H}_m(Z, Z_1, \ldots, Z_n)$ sur $\operatorname{res} K$, obtenu par passage aux restes, est non nul. Puisque $\operatorname{res} K$ est infini il existe $x_0, \ldots, x_n \in \operatorname{res} K$ tels que $x_0 \neq 0$ et $\overline{H}_m(x_0, x_1, \ldots, x_n) \neq 0$, pour tout m. Notons qu'il existe $x \in V_K$ tel que $\overline{\delta_0(x)} = x_0, \ldots, \overline{\delta_n(x)} = x_n$. Considérons les équations suivantes en d_ρ : $\overline{\delta_0(e_\rho + d_\rho)} = x_0, \ldots, \overline{\delta_n(e_\rho + d_\rho)} = x_n$. Via la structure des vecteurs de Witt, il existe des polynômes Q_i sur $\operatorname{res} K$ tels que $\overline{\delta_i(e_\rho + d_\rho)} = Q_i(\overline{\delta_0(e_\rho)}, \ldots, \overline{\delta_n(e_\rho)}, \overline{\delta_0(d_\rho)}, \ldots, \overline{\delta_n(d_\rho)})$. On obtient le système d'équations en les $\overline{\delta_i(d_\rho)}$ à coefficients dans $\operatorname{res} K$:

$$x_i = Q_i\big(\overline{\delta_0(e_\rho)}, \ldots, \overline{\delta_n(e_\rho)}, \overline{\delta_0(d_\rho)}, \ldots, \overline{\delta_n(d_\rho)}\big), \quad i = 0, \ldots, n.$$

Ce système est cohérent puisqu'il a la solution $y_{i,\rho} = \overline{\delta_i(x - e_\rho)}$ pour tout x comme ci-dessus. Soit $d_\rho \in V_K$ tel que $\overline{\delta_i(d_\rho)} = y_{i,\rho}$, $i = 1, \ldots, n$. Alors on a $\overline{\delta_i(e_\rho + d_\rho)} = x_i$ et $v(F_m(e_\rho + d_\rho)) = v(c_m)$ et notons que $a'_\rho = a_\rho + \theta_\rho d_\rho \in K$ et $v(d_\rho + e_\rho) = 0$. On a $v(a'_\rho - \alpha) = v(\theta\rho) + v(d_\rho + e_\rho) = \gamma_\rho$, de sorte que $a'_\rho \to \alpha$ et que (a'_ρ) possède les mêmes pseudolimites que (a_ρ). D'autre part, on a $F(a'_\rho) - F(\alpha) = \sum_m c_{\mathbf{j}_m} F_m(e_\rho + d_\rho){\theta_\rho}^m$, où $v(c_{\mathbf{j}_m} F_m(e_\rho + d_\rho)) = v(c_{\mathbf{j}_m}) + v(c_m)$ ne dépend pas de ρ. On peut alors appliquer les arguments de [4] (p. 399) pour conclure que $F(a'_\rho) \to F(\alpha)$.

Soit (K, v, σ) un σ-corps valué. Une suite pseudoconvergente $(a_\rho) \in K$ sera dite *de type σ-algébrique sur K* s'il existe une suite pseudoconvergente $(a'_\rho) \in K$ avec les mêmes pseudolimites que (a_ρ) et un σ-polynôme non nul $F(X)$ sur K tel que $F(a'_\rho) \to 0$ et que les $D_{\mathbf{j}}F(a'_\rho)$ soient des suites pseudoconvergentes pour tout multi-indice $\mathbf{j}$ (*cf.* ci-dessus). Sinon, la suite (a_ρ) sera dite *de type σ-transcendant sur K*. On vérifie qu'une pseudolimite d'une suite pseudoconvergente de type σ-transcendant sur K est un élément σ-transcendant sur K.

3. Les axiomes

Nous allons utiliser le langage des σ-corps valués, avec un symbole σ pour un automorphisme et un prédicat pour l'anneau de valuation. Nous formulerons les arguments en utilisant les applications de valuation et de passage au reste. Puisque la valuation p-adique est définissable algébriquement dans les vecteurs de Witt, les résultats se traduisent en conséquence.

Soit $\mathrm{W}F_p$ la théorie de σ-corps valués obtenue en ajoutant à la théorie W_p les axiomes suivants : 1. $v(\sigma(x)) = v(x)$, 2. $v(x) \geqslant 0 \to v(\sigma(x) - x^p) > 0$, 3. $\forall x \exists y\, (\sigma(y) = y \wedge v(x) = v(y))$, 4. $\mathrm{Fix}\,(\sigma)$ est p-adiquement clos, 5. le schéma d'axiomes σH^*.

Le corps $\mathrm{W}(\widetilde{\mathbf{F}}_p)$ des vecteurs de Witt sur la clôture algébrique du corps à p éléments avec l'automorphisme Frob vérifie clairement les axiomes 1-2-3. On a $\mathrm{Fix}(\mathrm{Frob}) = \mathbf{Q}_p$, les nombres p-adiques, ce qui vérifie l'axiome 4. Pour le schéma σH^*, vérifions d'abord que tous les polynômes *σ-linéaires* $F(X) = a_n\sigma^n(X) + \cdots + a_1\sigma(X) + a_0X + b$, où $v_p(a_i) \geqslant 0$ avec au moins un a_i de valuation nulle, possède une racine (c'est un cas particulier de σH^*). Modulo p, cette équation devient $\overline{a}_n X^{p^n} + \cdots + \overline{a}_1 X^p + \overline{a}_0 X + \overline{b} = 0$ et elle a une solution dans $\widetilde{\mathbf{F}}_p$, disons $\overline{x}_0$. Soit $v_p(F(x_0)) = m > 0$; considérons $F(x_0 + p^m y) = F(x_0) + p^m \sum a_i\sigma^i(y)$. L'équation $F(x_0)p^{-m} + \sum a_i\sigma^i(y) = 0$ a aussi, comme ci-dessus, une solution en y modulo p. On obtient alors $x_1 = x_0 + p^m y$ tel que $v_p(F(x_1)) > v_p(F(x_0))$ et $v_p(x_0 - x_1) = m$, et on peut continuer pour obtenir une suite de Cauchy dont la limite fournit la solution cherchée. L'existence de solutions pour ces équations σ-linéaires permet d'adapter l'argument ci-dessus à la vérification du schéma σH^* (analogue au cas habituel d'un simple polynôme, qui est une version du lemme de Hensel classique).

Pour montrer que $\mathrm{W}F_p$ est une théorie complète on construit un va-et-vient entre deux modèles ω_1-saturés quelconques (M_1, σ), (M_2, σ). On peut supposer $\operatorname{res} M_1 = \operatorname{res} M_2$, $vM_1 = vM_2$. Appelons *bonne sous-structure* de M_i, une sous-structure $(K, v, \sigma) \subset (M_i, v, \sigma)$, où vK est dénombrable et pur dans vM_i,

$v(\mathrm{Fix}\,(\sigma) \cap K) = vK$ et $\mathrm{res}\,K = \mathrm{res}\,M_i$. Les isomorphismes partiels du va-et-vient se font entre bonnes sous-structures. On utilise le lemme 3.1 pour amorcer le va-et-vient, puis les propositions 3.2, 3.3, 3.4 l'une après l'autre comme dans [4]. Notons qu'un corps stable par σ est linéairement disjoint de $\mathrm{Fix}(\sigma)$ au-dessus de leur intersection. La proposition 2.2 (et des variantes mineures) apparaît dans la preuve des propositions 3.3, 3.4.

LEMME 3.1. – *Il existe de bonnes sous-structures* $(N_i, v, \sigma) \subset (M_i, v, \sigma)$ *telles que* $(N_i, v, \sigma) \simeq (\mathrm{W}(\mathrm{res}\,M_i), v_p, \mathrm{Frob})$.

PROPOSITION 3.2. – *Soient* $(K_i, v, \sigma) \subset (M_i, v, \sigma)$ *de bonnes sous-structures telles que* (K_i, v) *soit hensélien et* K_i *contienne un relèvement du corps des restes de* M_i *pour la valuation induite par le sous-groupe convexe* $\mathbf{Z}v(p)$. *Soit* $f : (K_1, v, \sigma) \to (K_2, v, \sigma)$ *un* σ*-isomorphisme de corps valués qui respecte les relèvements ci-dessus, et* $a \in M_1$ *tel que* $vK_1(a) \neq vK_1$. *Alors* f *se prolonge en un* σ*-isomorphisme de corps valués* $f_1 : (E_1, v, \sigma) \to (E_2, v, \sigma)$, *où* (E_i, v, σ) *est une bonne sous-structure de* M_i, $(K_i, v, \sigma) \subset (E_i, v, \sigma)$; (E_1, v) *est hensélien et* $vE_1(a) = vE_1$.

PROPOSITION 3.3. – *Soient* $(K_i, v, \sigma) \subset (M_i, v, \sigma)$ *de bonnes sous-structures et* $f : (K_1, v, \sigma) \to (K_2, v, \sigma)$ *un* σ*-isomorphisme de corps valués. Soit* $a \in M_1$ *tel que* $K_1(a)_\sigma / K_1$ *soit une extension immédiate et* a *soit* σ*-algébrique sur* K_1. *Alors* f *se prolonge en un* σ*-isomorphisme de corps valués* $f_1 : (E_1, v, \sigma) \to (E_2, v, \sigma)$, *où* (E_i, v, σ) *est une bonne sous-structure de* M_i, $(K_i, v, \sigma) \subset (E_i, v, \sigma)$, $a \in E_1$ *et* E_1/K_1 *est une extension immédiate,* σ*-algébrique.*

PROPOSITION 3.4. – *Soient* $(K_i, v, \sigma) \subset (M_i, v, \sigma)$ *de bonnes sous-structures et* $f : (K_1, v, \sigma) \to (K_2, v, \sigma)$ *un* σ*-isomorphisme de corps valués. Soit* $a \in M_1$ *tel que* $K_1(a)_\sigma / K_1$ *soit une extension immédiate et* a *soit* σ*-transcendant sur* K_1. *Alors* f *se prolonge en un* σ*-isomorphisme de corps valués* $f_1 : (E_1, v, \sigma) \to (E_2, v, \sigma)$, *où* (E_i, v, σ) *est une bonne sous-structure de* M_i, $(K_i, v, \sigma) \subset (E_i, v, \sigma)$, *et* $a \in E_1$.

La théorie WF_p est aussi modèle-complète. Pour construire un va-et-vient entre deux modèles $M_1,\ M_2$, déjà extensions d'un modèle M, on peut encore utiliser le lemme 3.1 car on peut obtenir une copie de $\mathrm{W}(\mathrm{res}\,M_i)$ qui soit linéairement disjointe de M sur un sous-corps commun (comme le cas classique, *cf.* par exemple [1]). On procède alors comme-ci-dessus.

On peut montrer que WF_p est la modèle-compagne de la théorie des σ-corps p-valués non ramifiés, où le groupe de valuation est égal à $v(\mathrm{Fix}(\sigma))$. On peut aussi obtenir une élimination des quantificateurs en passant à un langage multisorte et en ajoutant, pour chaque n, un symbole pour une *composante angulaire d'ordre* n (*cf.* [5], théorème 3.7).

Ces derniers points et des résultats plus généraux seront exposés dans un article détaillé.

Références bibliographiques

[1] Bélair L., Vecteurs de Witt, in: Séminaire sur les structures algébriques ordonnées II, Publications mathématiques de l'Université Paris-7, 1990.
[2] Buium A., Geometry of p-jets, Duke Math. J. 82 (1996) 349–367.
[3] Joyal A., δ-anneaux et vecteurs de Witt, C. R. Math.- Math. Rep. Acad. Sci. Canada 7 (1985) 177–182.
[4] Kochen S., The model theory of local fields, in: Logic Conference, Kiel 1974, Lect. Notes in Math. 499, Springer-Verlag, 1975.
[5] Pas J., Cell decomposition and local zeta functions in a tower of unramified extensions of a p-adic field, Proc. London Math. Soc. 65 (1990) 37–67.
[6] Scanlon T., Quantifier Elimination for the Relative Frobenius, Prépublication, 1999.