VECTEURS DE WITT

Luc Bélair

Résumé. Notre but était d'introduire les vecteurs de Witt et d'indiquer leur rôle dans la théorie des modèles des corps valués d'inégale caractéristique.

Plan. §1. Introduction
§2. Théorie des modèles des corps valués d'inégale caractéristique
§3. Vecteurs de Witt heuristiques
§4. Construction formelle

§1. INTRODUCTION

Les vecteurs de Witt furent introduits par Witt [Wi] en réponse à la question de la structure, et éventuellement la construction, de corps valués d'inégale caractéristique complet par rapport à une valuation discrète et ayant un corps des restes donné de caractéristique $p \neq 0$. En égale caractéristique on sait que pour un corps des restes donné k la réponse à la question analogue consiste en les séries de Laurent $k((T))$ sur le corps en question. En inégale caractéristique on peut distinguer les cas suivants. Soit k un corps de caractéristique $p \neq 0$ donné.

(1) <u>Cas non ramifié</u>. C'est-à-dire le cas où p est une uniformisante.

(1.1) <u>k parfait</u>. Alors pour chaque $m=1,2,\ldots$ on introduit une structure d'anneau sur le produit cartésien $k^{(m)}$ pour en faire un anneau noté $W_m(k)$ et appelé anneau des vecteurs de Witt de longueur m sur k . Les $W_m(k)$

forment un système projectif dont la limite est un anneau intègre de caractéristique zéro qui s'avère être l'anneau de valuation du corps valué complet voulu. On note $W(k)$ le corps des fractions de cette limite. C'est le corps des vecteurs de Witt sur k. Le corps k étant donné, tout corps valué d'inégale caractéristique complet par rapport à une valuation discrète non ramifiée et ayant un corps de restes isomorphe à k par un isomorphisme f, est isomorphe à $W(k)$ par un unique isomorphisme de corps valués induisant f au niveau des corps de restes.

Exemple. Soit $\mathbb{F}_p$ le corps premier de caractéristique p. Alors $W_m(F_p) = \mathbb{Z}/(p^m)$, $\varprojlim W_m(F_p) = \mathbb{Z}_p$, les entiers p-adiques, et $W(\mathbb{F}_p) = \mathbb{Q}_p$, les nombres p-adiques.

(1.2) k non parfait. (cf [Te]) Si k n'est pas parfait alors on le plonge dans une clôture parfaite $k^{p^{-\infty}}$, on passe à $W(k^{p^{-\infty}})$, et en relevant une p-base de k à $W(k^{p^{-\infty}})$ on arrive à construire le corps valué complet voulu à l'intérieur de $W(k^{p^{-\infty}})$. On le note aussi $W(k)$ et il possède la même propriété d'unicité que dans le cas parfait, à un choix de p-base près.

(2) Cas ramifié. Dans le cas où p n'est pas une uniformisante, le corps valué cherché s'avère être une extension totalement ramifiée du cas non ramifié. Plus précisément, tout corps valué d'inégale caractéristique complet par rapport à une valuation discrète ramifiée et de corps de restes donné k est isomorphe à une extension totalement ramifiée de $W(k)$ donnée par un polynôme d'Eisenstein i.e. de la forme $X^n+a_1X^{n-1}+\ldots+a_n$ où $p|a_i$ $(v(a_i)\geq v(p))$ mais $p^2\nmid a_n$ $(v(a_n)=v(p))$.

Witt (ibid.) utilisa les $W_m(k)$ en rapport avec la structure des extensions abéliennes d'ordre p^e d'un corps de caractéristique $p\neq 0$, en donnant un analogue de la théorie de Kummer. Pour plus de détails voir par exemple [Ja], [Ri].

§2. THEORIE DES MODELES DES CORPS VALUES D'INEGALE CARACTERISTIQUE

Il s'agit des corps valués de caractéristique 0 dont le corps de restes est de caractéristique $p \neq 0$. Notons cette théorie IN_p . Soit (K,v) un corps valué. On notera V_K l'anneau de valuation, val K le groupe de valuation, res K le corps des restes et $\bar{\ }$ l'application canonique de V_K dans res K . Pour fixer les idées on adopte le langage du premier ordre des corps valués contenant un prédicat unaire pour l'anneau de valuation.

Cas non-ramifié

On étudie ici le cas où il n'y a aucun élément entre 0 et $v(p)$ dans le groupe de valuation. Notons cette théorie INR_p . Soit k un corps de caractéristique $p \neq 0$.

Théorème. (Kochen, cf. [Ko]) Le principe d'Ax-Kochen-Ershov s'applique aux corps valués henséliens d'inégale caractéristique non-ramifié. En particulier $Th(W(k),v)$ est axiomatisée par les propriétés

$$INR_p + \text{hensélien} + \text{gr. de valuation } \mathbb{Z}\text{-groupe} + Th(k)$$

et si $Th(k)$ est modèle-complète alors $Th(W(k),v)$ l'est aussi.

Par exemple si $k=\mathbb{F}_p$ la théorie élémentaire de $W(\mathbb{F}_p)=\mathbb{Q}_p$ est celle des corps p-adiquement clos (de rang 1). Les vecteurs de Witt interviennent de la façon suivante. La méthode utilisée par Kochen est de montrer l'isomorphisme de modèles ω_1-saturés munis de section normalisée. On peut traduire ici en va-et-vient. Soit $HINR_p = INR_p$ + hensélien . Pour démontrer la complétude de la théorie $HINR_p + T_v + T_r$ où T_v, T_r sont respectivement des théories complètes pour le groupe de valuation et le corps de restes, on considère deux modèles ω_1-saturés avec section normalisée M_1 et M_2 tels que val M_1=val M_2 et res M_1=res M_2=k . Par saturation M_i contient un sous-corps valué complet pour une valuation discrète ayant un corps des restes égal à k . Ainsi $(W(k),v)$ se plonge dans M_1 et M_2 et fournit un isomorphisme partiel pour commencer un va-et vient. Plus précisément, Kochen met en évidence dans ce contexte le passage à la valuation quotient induite par le sous-groupe convexe $\mathbf{Z}.v(p)$ de val M $(M=M_i)$. A savoir, on considère la valuation composée $w: M \to$ val $M/\mathbf{Z}.v(p)$ et il appert que (M,w) est hensélien d'égale caractéristique 0 . Son corps des restes se relève donc en un sous-corps M' de M . Il s'ensuit que pour (M',v) , val $M'=\mathbf{Z}.v(p)$ et res M'=res $M=k$. Par saturation M contient un complété de (M',v) d'où un plongement de $W(k)$ dans M . Ainsi une théorie T_r de corps de restes étant donnée la classe des corps de vecteurs de Witt sur les modèles de T_r fournit des structures qui se plongent dans les modèles suffisamment saturés de $HINR_p + T_r$.

Dans le contexte de la modèle-complétude ou des extensions élémentaires on peut aussi se ramener à ce schéma. Cette fois on a deux modèles ω_1-saturés M_1 et M_2 , deux sous-modèles resp. N_1 et N_2 et un isomorphisme partiel f de N_1 sur N_2 et il s'agit de prolonger f en un va-et-vient entre M_1 et M_2 . Toujours dans la même notation , on a de nouveau un plongement de $W(k)$ dans M_i mais cette fois on procède à un amalgame de $W(k)$ et N_1 dans l'esprit de la Proposition 2.15 de [De] de façon à prolonger f tout en augmentant le corps des restes.

<u>Proposition</u>.([De],Prop.2.15) Soit $E \subseteq F$ des corps valués, $F_0 \subseteq F$ tels que le passage au reste $\bar{\ }$ induise un isomorphisme α entre F_0 et res F . Si $E_0 = \alpha^{-1}[\text{res } E]$ est contenu dans E , et K_0 est tel que $E_0 \subseteq K_0 \subseteq F_0$, alors

(i) E et F_0 sont linéairement disjoints au-dessus de E_0 .

(ii) Tout élément $x \in E[K_0]$ s'écrit $x = \Sigma_1^n e_i k_i$, avec $e_i \in E$, $k_i \in K$ et $v(e_i) < v(e_j)$ si $i < j$.

(iii) val EK_0 = val E et res EK_0 = res K_0 .

Cette technique s'applique aussi à l'élimination des quantificateurs. Ainsi on peut démontrer le cas d'inégale caractéristique du théorème d'élimination des quantificateurs de Cherlin-Dickmann [C-D] selon ce schéma. On remplace alors les sous-modèles N_i par des sous-structures et on utilise le même genre d'arguments que pour la modèle-complétude.

Notons que pour se ramener complètement au schéma du théorème de Kochen on doit introduire des sections normalisées. Ceci est possible moyennant un peu de théorie des modèles de base et des résultats auxiliaires de Kochen (ibid.).

Un dernier point à propos du théorème de Cherlin-Dickmann en rapport avec les vecteurs de Witt. Soit A l'anneau de valuation et U le groupe multiplicatif des éléments inversibles de A . L'hypothèse principale de ce théorème est que le sous-groupe U^n des puissances n-ièmes est d'indice fini pour tout n . Avec F.Delon nous avons remarqué que cette hypothèse implique que le corps des restes est fini. En effet soit k le corps des restes en question et supposons-le infini. Si k n'est pas parfait on montre directement que le sous-groupe multiplicatif des puissances p-ièmes $k^{\cdot p}$ (p=car k) est d'indice infini. Si k est parfait alors $A/(p^2)$ est isomorphe à l'anneau des vecteurs de Witt de longueur 2 sur k . A l'aide de notre connaissance explicite des opérations dans $W_2(k)$ on montre facilement que le sous-groupe multiplicatif des puissances p-ièmes est aussi d'indice infini.

Cas ramifié

Il existe aussi des résultats du type Ax-Kochen-Ershov dans le cas où il y a ramification i.e. des éléments entre 0 et $v(p)$. En rapport avec les vecteurs de Witt nous nous contenterons ici de dire que les résultats de Basarab [Ba] sur la ramification finie peuvent aussi être démontrés, moyennant un argument de compacité au départ, à l'intérieur du schéma que nous avons dégagé de l'article de Kochen.

En guise de conclusion nous soulignons dans cette approche le passage à la valuation quotient induite par le sous-groupe canonique discret mis en évidence par Kochen, et le rôle conceptuel de l'usage que fait F.Delon dans [De] de sa Proposition 2.15.

§3. VECTEURS DE WITT HEURISTIQUES

Nous présentons de façon heuristique la construction des anneaux $W_m(k)$. Soit k un corps parfait de caractéristique $p \neq 0$. On se place du point de vue de §1 . Rappelons que l'application canonique de l'anneau de valuation sur le corps de restes est notée $\bar{\ }$.

<u>Proposition</u>.(Teichmüller) Soit (K,v) un corps valué de caractéristique 0 non-ramifié complet par rapport à une valuation discrète de corps des restes égal à k . Soit V son anneau de valuation. Alors il existe $R \subseteq V$ un système de représentants canoniques pour k caractérisé par les propriétés suivantes: (1) Soit a_n t.q. $\bar{a}_n = \alpha^{p^{-n}}$ alors la suite $(a_n^{p^n})$ converge vers un élément $a \in R$ t.q. $\bar{a} = \alpha$.

(2) Tout élément de R possède une racine p-ième.

(3) Soit $a,b,c \in R$, $\bar{a}=\alpha, \bar{b}=\beta, \bar{c}=\gamma$. Alors $\alpha = \beta\gamma$ implique $a = bc$.

<u>Démonstration</u>. D'abord notons que (3)⇒(2) et qu'on a l'unicité de R par (1) et (2) . D'autre part soit $\alpha \in k$. On choisit a_n t.q. $\bar{a}_n = \alpha^{p^{-n}}$. Il s'ensuit que $a_{n+1} \equiv a_n \pmod p$ d'où $a_{n+1}^{p^{n+1}} \equiv a_n^{p^n} \pmod{p^n}$. La suite $(a_n^{p^n})$ est donc une suite de Cauchy et converge vers un élément $a \in V$. On vérifie que a est indépendant de la suite (a_n) choisie et on utilise ce fait pour montrer (3) par continuité. □

Il s'agit bien sûr des fameux représentants de Teichmüller.

<u>Exemple</u>. Si $K=\mathbb{Q}_p$ alors $R=\{0,\zeta_1,\ldots,\zeta_{p-1}\}$ où les ζ_i sont les racines $(p-1)$-ièmes de 1 (Lemme de Hensel).

<u>Lemme</u>. Soit K,R comme ci-dessus. Alors tout $x \in V$ s'écrit de façon unique $x = a_0 + a_1 p + a_2 p^2 + \ldots = \Sigma_0^\infty a_n p^n$, $a_i \in R$.

<u>Démonstration</u>. Soit $a_0 \in R$ t.q. $\bar{a}_0 = \bar{x}$ alors $p^{-1}(x-a_0) \in V$. Soit $a_1 \in R$ t.q. $\bar{a}_1 = \overline{p^{-1}(x-a_0)}$ alors $x \equiv a_0 + a_1 p \pmod{p^2}$ etc. □

Nous y allons maintenant de nos remarques heuristiques. Par approximation successive chaque élément du système canonique R est donné par ses racines p^n-ièmes modulo p . Partant d'un élément $x = a_0+a_1p+a_2p^2+\ldots$ comme dans le lemme on a

a_0 essentiellement donné par une suite $(\alpha_{00},\alpha_{01},\alpha_{02},\alpha_{03},\ldots)$
a_1 essentiellement donné par une suite $(\alpha_{10},\alpha_{11},\alpha_{12},\alpha_{13},\ldots)$
a_2 essentiellement donné par une suite $(\alpha_{20},\alpha_{21},\alpha_{22},\alpha_{23},\ldots)$
.... etc.

où par exemple $\alpha_{0i}^{p^i} = \alpha_{00} = \bar{a}_0$ et $\alpha_{0i+1}^p = \alpha_{0i}$.

Soit $k^{(m)}$ le produit cartésien de k m fois par lui-même. On peut considérer que la suite

$$(\alpha_{00}),(\alpha_{01},\alpha_{10}),(\alpha_{02},\alpha_{11},\alpha_{20}),(\alpha_{03},\alpha_{12},\alpha_{21},\alpha_{30}),\ \ldots$$

détermine essentiellement x . Ceci suggère un système projectif

$$k^{(1)} \longleftarrow k^{(2)} \longleftarrow k^{(3)} \longleftarrow k^{(4)} \longleftarrow \ \ldots$$

où par exemple $(\alpha_{01},\alpha_{10})$ est envoyé sur $\alpha_{01}^p = \alpha_{00}$. Faudrait-il encore mettre une structure d'anneau sur les $k^{(m)}$ de sorte que par exemple $(\alpha_{02},\alpha_{11},\alpha_{20})$

$$\delta(xy) = x^q\delta(y) + \delta(x)y^q + p\delta(x)\delta(y)$$
$$\delta(1) = 0 \quad .$$

Soit $\underline{A}$ la catégorie des anneaux unitaires commutatifs et $\underline{\delta A}$ celle des δ-anneaux. Il montre que le foncteur d'oubli $U: \underline{\delta A} \longrightarrow \underline{A}$ possède un adjoint à droite $W: \underline{A} \longrightarrow \underline{\delta A}$ et que dans le cas où $q=p$, $W(A)$ s'identifie à l'anneau des vecteurs de Witt sur A. Le lien entre les vecteurs de Witt et la structure de δ-anneau se fait au moyen de l'endomorphisme de Frobenius des vecteurs de Witt.

Références

[Ba] S.A.Basarab. "Some Model Theory of Henselian Fields", J. of Alg. 55 (1978),pp.191-212.

[C-D] G.Cherlin et M.Dickmann. "Anneaux réels clos et anneaux de fonctions continues", C.R.Acad.Sci. Paris, série A t.290, 9 janvier 1980.

[De] F.Delon. Quelques propriétés des corps valués en théorie des modèles. Thèse d'état, Université Paris VII, 1981.

[Ja] N.Jacobson. Basic Algebra II. W.H.Freeman & Co., San Francisco, 1980.

[Jo] A.Joyal. " δ-anneaux et vecteurs de Witt", C.R.Math.Acad.Sci Canada VII No 3, juin 1985.

[Ko] S.Kochen. "Model Theory of Local Fields", Logic Conference (Kiel 1974), Springer,(LNM,499), 1975.

[Ri] P.Ribenboim. L'arithmétique des corps. Hermann, Paris, 1972.

[Se] J.-P.Serre. Corps locaux. Hermann,Paris,1962.

[Te] O.Teichmüller."Diskret bewertete perfekte Körper mit unvollkommenen Restklassenkörper", Crelle 176 (1937),pp.141-152.

[Wi] E.Witt." Zyklische Körper und Algebren der Charakteristik p vom Grad p^n (Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p)", Crelle 176 (1937),pp.125-140.

L.Bélair
Equipe de logique mathématique
UER de mathématiques
Université Paris VII