C.R. Math. Rep. Acad. Sci. Canada - Vol. VII, No. 3, June 1985 juin

δ-ANNEAUX ET VECTEURS DE WITT

ANDRE JOYAL

Presented by P. Ribenboim, F.R.S.C.

Résumé

Nous donnons à la théorie des vecteurs de Witt une formulation nouvelle en utilisant les méthodes de l'algèbre universelle et de la théorie des catégories. On introduit une structure algébrique, celle de δ-anneau. Un δ-anneau est un anneau commutatif muni d'une opération unaire supplémentaire satisfaisant à des identités algébriques simples. Le résultat principal consiste à montrer que le foncteur oubliant de la catégorie des δ-anneaux vers celle des anneaux commutatifs possède un adjoint à droite W. Un calcul explicite permet l'identification de W(A) avec l'anneau des vecteurs de Witt sur A. On donne des démonstrations plus conceptuelles de plusieurs résultats de la théorie des vecteurs de Witt [7,2].

1- δ-anneaux

Fixons une fois pour toute un nombre premier p et une puissance $q = p^r$ $(r \geq 0)$.

DEFINITION 1 Un δ-anneau A est un anneau commutatif muni d'une opération unaire $\delta: A \to A$ satisfaisant aux identités suivantes:

$$\text{i)}\quad \delta(x+y) = \delta(x) + \delta(y) - \sum_{i=1}^{q-1} \frac{1}{p}\binom{q}{i} x^i y^{q-i}$$

$$\text{ii)}\quad \delta(xy) = x^q\delta(y) + \delta(x)y^q + p\delta(x)\delta(y)\ ,\ \delta(1) = 0$$

Nous dirons aussi que A est un δ-anneau relativement au couple (p,q).

Ces conditions entraînent que l'opération unaire $f(x) = x^q + p\delta(x)$ est un endomorphisme de l'anneau A:

$$f(x+y) = f(x) + f(y)$$
$$f(xy) = f(x)f(y)$$
$$f(1) = 1$$

Nous dirons que f est l'<u>endomorphisme</u> <u>de</u> <u>Frobenius</u>. Inversement, soit f un endomorphisme d'un anneau commutatif A sans p-torsion. Supposons que pour tout $x \in A$

$$f(x) \equiv x^q \mod pA$$

On obtient une structure de δ-anneau sur A en définissant δ comme suit:

$$\delta(x) = \frac{1}{p}(f(x) - x^q)$$

<u>Exemple 1</u>. L'anneau $\mathbb{Z}$ admet une seule structure de δ-anneau puisque le seul endomorphisme de $\mathbb{Z}$ est l'identité.

<u>Exemple 2</u> Soit L une extension galoisienne d'un corps K. Soit $B \subset L$ un anneau de valuation discrète et soit $A = B \cap K$. On suppose que $p = p \cdot 1$ est une uniformisante pour B et que $A/pA \simeq \mathbb{F}_q$. On sait montrer [1] l'existence d'une <u>substitution</u> <u>de</u> <u>Frobenius</u> $\sigma \in$ Galois (L/K) caractérisée par

i) $\sigma(B) = B$
ii) $\sigma(x) \equiv x^q \mod pB$

Un morphisme de δ-anneau est un homomorphisme d'anneaux qui préserve δ. Nous dirons aussi que c'est un δ-morphisme. On vérifie que l'endomorphisme de Frobenius est un δ-morphisme.

THEOREME 1 Soit $\mathbb{Z}[x_0,x_1,\ldots]$ l'anneau des polynômes sur une suite infinie d'indéterminés. Il y a une seule structure de δ-anneau sur $\mathbb{Z}[x_0,x_1,\ldots]$ pour laquelle $\delta(x_n) = x_{n+1}$ pour tout n. Muni de cette structure, $\mathbb{Z}[x_0,x_1\ldots]$ est un δ-anneau libre sur x_0.

Désignons par $\underline{A}$ la catégorie des anneaux et par $\delta\underline{A}$ celle des δ-anneaux.

THEOREME 2 Le foncteur oubliant $U\colon \delta\underline{A} \to \underline{A}$ possède un adjoint à droite $W\colon \underline{A} \to \delta\underline{A}$.

La théorie des catégorie [6] met en évidence l'équivalence entre le théorème précédent et le suivant:

THEOREME 3 Soient $A \to B$ et $A \to C$ des morphismes de δ-anneaux. Considérons le carré

$$\begin{array}{ccc} A & \to & C \\ \downarrow & & \downarrow i_2 \\ B & \underset{i_1}{\to} & B\otimes_A C \end{array}$$

Il y a sur $B\otimes_A C$ une seule structure de δ-anneaux pour laquelle i_1 et i_2 sont des δ-morphismes.

On peut donner une démonstration directe de ces théorèmes ou encore utiliser [8,9]. Comme conséquence, on a:

COROLLAIRE Le foncteur $W\colon \underline{A} \to \delta\underline{A}$ est représentable par l'anneau $\mathbb{Z}[x_0,x_1,\ldots]$. Il y a une bijection naturelle:

$$\gamma_A\colon W(A) \cong A^{\mathbb{N}}$$

La bijection γ_A s'explicite comme suit:

$$\begin{aligned} W(A) &\simeq \mathrm{Hom}_\delta(Z[x_0,x_1,\ldots], W(A)) \\ &\simeq \mathrm{Hom}\,(Z[x_0,x_1,\ldots], A) \\ &\simeq A^N \end{aligned}$$

2- Vecteurs de Witt

Pour voir que W(A) est isomorphe à l'anneau des vecteurs de Witt sur A, il suffira d'utiliser une description différente du δ-anneau libre sur un générateur. Cette description est basée sur le résultat suivant.

PROPOSITION 1 On peut définir dans la théorie des δ-anneaux une suite unique d'opérations unaires $\delta_0, \delta_1, \delta_2, \ldots$ vérifiant les identités

$$f^n(x) = \delta_0(x)^{q^n} + p\delta_1(x)^{q^{n-1}} + \ldots + p^n\delta_n(x) \qquad (n \geq 0)$$

Les deux premiers termes de la suite sont $\delta_0(x) = x$ et $\delta_1(x) = \delta(x)$.

PROPOSITION 2 Il y a sur $Z[Y_0,Y_1,Y_2,\ldots]$ une seule structure de δ-anneau pour laquelle $\delta_n(Y_0) = Y_n$ pour tout $n \geq 0$. Muni de cette structure, $Z[Y_0,Y_1,Y_2\ldots]$ est un δ-anneau libre sur Y_0.

THEOREME 4 Si q=p l'anneau W(A) s'identifie à l'anneau des vecteurs de Witt sur A.

A chaque élément $x \in W(A)$ correspondant un vecteur de Witt $\pi_A(x) \in A^N$. La description de π_A est semblable à celle de γ_A mais elle utilise plutôt le δ-anneau libre $Z[Y_0,Y_1,\ldots]$.

L'endofoncteur composé $\underline{A} \xrightarrow{W} \delta\underline{A} \xrightarrow{U} \underline{A}$ est une co-monade [6,3,2] sur $\underline{A}$. Pour simplifier, nous noterons encore ce foncteur par W. On a des transformations naturelles

$$W(A) \xrightarrow{\varepsilon_A} A \qquad W(A) \xrightarrow{E_A} W(W(A))$$

satisfaisant à des conditions d'associativité et d'unité. L'homomorphisme E_A est étroitement relié à l'exponentielle de Artin-Hasse [3]. Une structure de δ-anneau sur A équivaut à une structure de co-algèbre [6] $\underline{\delta}$: $A \to W(A)$. Celle-ci se décrit comme suit: pour tout $x \varepsilon A$ on a $\pi_A \underline{\delta}(x) = (\delta_0(x), \delta_1(x), \ldots)$.

Remarques

1) Soit A un anneau sans p-torsion muni d'un endomorphisme f tel que pour tout $x \varepsilon A$, $f(x) \equiv x^q \bmod pA$. Le lemme de Dieudonné-Cartier [4, page 508] affirme l'existence d'un homomorphisme s_f: $A \to W(A)$. Ce résultat s'interprète comme suit dans le contexte présent: les hypothèses entraînent l'existence d'une structure de δ-anneau sur A et on vérifie que $s_f = \underline{\delta}$.

2) Sous les hypothèses de la remarque précédente, on donne une description particulièrement simple de W(A) [5]. Posons

$$B = \{(a_n) \varepsilon A^N | a_{n+1} \equiv f(a_n) \bmod p^{n+1} \ \forall n\}$$

On vérifie que B est un sous-anneau de l'anneau produit A^N. L'opérateur de translation $t((a_n)) = (a_{n+1})$ est un endomorphisme de B et pour tout $x \varepsilon B$,

$$t(x) \equiv x^q \mod pB$$

Comme B est sans p-torsion, on a une structure de δ-anneau sur B pour laquelle t est l'endomorphisme de Frobenius. On vérifie ensuite directement qu'avec la projection $B \to A$, B devient le δ-anneau co-libre sur l'anneau A, donc que $B \simeq W(A)$.

Bibliographie

[1] Bourbaki. Algèbre, Chap. V, 11.

[2] Bourbaki. Algèbre, Chap. 8 et 9.

[3] M. Hazewinkel. Formal Groups and Applications. Academic Press Monographs 78, 1978.

[4] L. Illusie. Complexe de De Rham-Witt et cohomologie cristalline. Annales Scientifiques de l'Ecole Normale Supérieure. 4^o série, t12, 1979, p. 501 à 661.

[5] M. Lazard. Commutative Formal Groups. Lect. Notes in Math. 443, Springer-Verlag.

[6] S. MacLane. Category theory for the working Mathematician. Graduate text in Math. 5, Springer Verlag.

[7] P. Ribenboim. L'Arithmétique des corps. Hermann, Paris 1972.

[8] D.O. Tall, G.C. Wraith. Representable Functors and Operations on Rings. Proceedings of the London Mathematical Society (3) 20 (1970) p. 619-643.

[9] G.C. Wraith. Algebras over theories. Colloquium Mathematicum. vol. XXIII (1971) fasc 2.

Département de Mathématiques
et d'informatique
Université du Québec à Montréal

Received March 28, 1985