GROUPE DE TRAVAIL
D'ANALYSE ULTRAMÉTRIQUE

GILLES CHRISTOL

Vecteurs de Witt et analyse p-adique

Groupe de travail d'analyse ultramétrique, tome 3, n° 1 (1975-1976), exp. n° 10, p. 1-5
<http://www.numdam.org/item?id=GAU_1975-1976__3_1_A6_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, P. ROBBA)
3e année, 1975/76, n° 10, 5 p.

26 janvier 1976

VECTEURS DE WITT ET ANALYSE p-ADIQUE

par Gilles CHRISTOL

Nous voulons montrer comment la technique des vecteurs de Witt permet de formaliser le passage de propriétés modulo p^h à des propriétés p-adiques pour les fonctions analytiques bornées à coefficients dans un corps de valuation discrète.

0. Rappels sur les vecteurs de Witt (voir [1] par exemple).

x désignant la suite de variable $(x_0 , \dots , x_n , \dots)$, nous posons

$$W_n(x) = W_n(x_0 , \dots , x_n) = x_0^{p^n} + p\, x_1^{p^{n-1}} + \dots + p^n x_n .$$

Il existe alors, pour chaque n , des polynômes P_n et S_n , à coefficients dans $\underset{\sim}{Z}$:

$$P_n(x , y) = P_n(x_0 , \dots , x_n ; y_0 , \dots , y_n)$$
$$S_n(x , y) = S_n(x_0 , \dots , x_n ; y_0 , \dots , y_n)$$

tels que, modulo p^{n+1} , on ait

$$W_n(P_0 , \dots , P_n) = W_n(x)\, W_n(y) \; ; \; W_n(S_0 , \dots , S_n) = W_n(x) + W_n(y) .$$

Par exemple, on vérifie immédiatement que

$$S_0 = x_0 + y_0 \; ; \; S_1 = x_1 + y_1 + \frac{(x_0 + y_0)^p - x_0^p - y_0^p}{p} .$$

On appelle vecteurs de Witt de l'anneau k l'anneau $W(k) = \underset{\sim}{k}^{N}$ muni des lois de composition :

$$(a_0 , \dots , a_n , \dots) + (b_0 , \dots , b_n , \dots) = (S_0(a_0 , b_0) , \dots , S_n(a , b) , \dots)$$
$$(a_0 , \dots , a_n , \dots) \times (b_0 , \dots , b_n , \dots) = (P_0(a_0 , b_0) , \dots , P_n(a , b) , \dots) .$$

Un calcul simple montre que

$$p(a_0 , \dots , a_n , \dots) = \underbrace{(a_0 , \dots) + \dots + (a_0 , \dots)}_{p \text{ fois}} = (0 , a_0^p , \dots , a_n^p , \dots)$$

Si k est un anneau parfait de caractéristique p , on peut définir un automorphisme σ (dit de Frobénius) de $W(k)$:

$$(a_0 , \dots , a_n , \dots)^\sigma = (a_0^p , \dots , a_n^p , \dots) .$$

$W(k)$ est muni de la valuation $v(a) = \inf(n \; ; \; a_n \neq 0)$ si bien que $v(a) \geqslant n$ est

équivalent à $a \in p^n W(k)$. Si $a_0 \in k$, alors

$$v[(a_0, a_1, \dots, a_n, \dots)^{p^h} - (a_0^{p^h}, 0, \dots, 0, \dots)] \geqslant h + 1$$

quels que soient les a_i ; on considèrera donc que $a_0^{p^h}$ est un élément de

$$W(k)/p^h W(k) .$$

On peut alors écrire la formule

$$W_n(a) = a^{\sigma^n} \pmod{p^{n+1}} .$$

1. Comparaison de $W(k[[x]])$ et de $W(k)[[x]]$.

Pour simplifier l'écriture, nous posons $A = W(k)$.

Un élément f de $A[[x]]$ sera noté $\sum f(n) x^n$, et $A[[x]]$ sera muni de la topologie de la convergence uniforme, c'est-à-dire de la valuation définie par

$$v(f) = \inf v(f(n)) .$$

Nous définissons, en outre, sur $A[[x]]$, les deux opérateurs

$$Uf = \sum f(np) x^n \quad ; \quad f^\sigma = \sum (f(n))^\sigma x^n .$$

LEMME. - *Si f appartient à $A[[x]]$, la suite $U^h(f^{p^h})^{\sigma^{-h}}$ converge, quand h tend vers l'infini, et sa limite ne dépend que de la valeur de f modulo p.*

On a vu que $v[(f(n))^p - (f(n))^\sigma] \geqslant 1$, c'est-à-dire $v[f^p(x) - f^\sigma(x^p)] \geqslant 1$, ce qui nous donne

$$v[f^{p^h}(x) - (f^\sigma)^{p^{h-1}}(x^p)] \geqslant h$$

puisque σ est un automorphisme. Enfin U et σ conservant les valuations, on obtient

$$v[U^h(f^{p^h})^{\sigma^h} - U^{h-1}(f^{p^{h-1}})^{\sigma^{-(h-1)}}] \geqslant h ,$$

ce qui démontre le lemme, puisque f^{p^h} ne dépend, modulo p^h, que de f modulo p.

On définit donc une application $\mathcal{P}$ de $k[[x]]$ dans $A[[x]]$ en posant, après avoir choisi un représentant quelconque de f dans $A[[x]]$,

$$\mathcal{P}(f) = \lim U^h(f^{p^h})^{\sigma^{-h}} .$$

LEMME. - *$\mathcal{P}$ se prolonge en une application A-linéaire de $W(k[[x]])$ dans $A[[x]]$ par*

$$\mathcal{P}[(f_0, \dots, f_n, \dots)] = \mathcal{P}(f_0) + p\, U\, \mathcal{P}(f_1)^{\sigma^{-1}} + \dots + p^n U^n \mathcal{P}(f_n)^{\sigma^{-n}} + \dots$$

D'après les définitions, on a

$$\mathcal{P}(f_0 , \dots) = U^h W_h(f)^{\sigma^{-h}} \pmod{p^{h+1}} .$$

Ce qui montre, pour a dans A (c'est-à-dire aussi dans $W(k[[x]])$) et f et g dans $W(k[[x]])$:

$$\begin{aligned}\mathcal{P}(af + g) &= U^h[W_h(a)\, W_h(f) + W_h(g)]^{\sigma^{-h}} \pmod{p^{h+1}} \\ &= W_h(a)^{\sigma^{-h}}\, U^h W_h(f)^{\sigma^{-h}} + U^h W_h(g)^{\sigma^{-h}} \pmod{p^{h+1}} \\ &= a\,\mathcal{P}(f) + \mathcal{P}(g) \pmod{p^{h+1}} .\end{aligned}$$

D'autre part, nous définissons une application A-linéaire $\mathfrak{L}$ de $A[[x]]$ dans $W(k[[x]])$ par

$\mathfrak{L}$ continue pour la topologie x-adique,

$\mathfrak{L}(a) = (a_0 , \dots , a_n , \dots)$ pour a dans A ,

$\mathfrak{L}(x) = (x , 0 , \dots , 0 , \dots)$.

LEMME. - On a $\mathcal{P} \circ \mathfrak{L} = I$.

Par définition, $W_h(\mathfrak{L}(f)) = \sum_n W_h(f\langle n\rangle)\, x^{np^h}$, ce qui donne bien

$$\mathcal{P} \circ \mathfrak{L}(f) = U^h[W_h(\mathfrak{L}(f))]^{\sigma^{-h}} = \sum_n W_h(f\langle n\rangle)^{\sigma^{-h}}\, x^n = \sum f\langle n\rangle\, x^n \pmod{p^{h+1}} .$$

Dans la suite, nous identifierons les éléments de $A[[x]]$ avec leur image, par $\mathfrak{L}$, dans $W(k[[x]])$.

PROPOSITION. - f est un élément analytique (resp. algébrique) si, et seulement si, les f_i sont rationnels (resp. algébriques).

Si f appartient à $k(x)$, il existe une fraction rationnelle à coefficients dans A , dont f est la réduction modulo p (il suffit de choisir un relèvement des éléments de k).

Comme l'opérateur U_h transforme une fraction rationnelle en fraction rationnelle, on voit que $\mathcal{P}(f)$ est encore une fraction rationnelle (de $A(x)$ cette fois). Par conséquent, si les f_i sont rationnels $\mathcal{P}(f)$ est limite uniforme de fractions rationnelles. Pour les élements algébriques, le raisonnement est le même : si k est parfait, toute fonction algébrique (sur $k(x)$) est diagonale d'une fraction rationnelle à 2 variables, et inversement, toute fraction rationnelle à 2 variables sur A a une diagonale qui est algébrique.

Inversement, si f est un élément analytique, il existe deux polynômes à coefficients dans A , tels que

$$Q(x)\, f(x) = P(x) \pmod{p^{h+1}} \quad \text{et} \quad Q(0) = 1 ,$$

ce qui donne

$$W_h(Q)\, W_h(f) = W_h(P) \pmod{p^{h+1}} ,$$

d'où on tire

$$f_h(x)\, Q_0(x) = \text{polynôme en } x , f_0 , \dots , f_{h-1} ,$$

ce qui montre, par récurrence, que f_h est une fraction rationnelle.

Pour les éléments algébriques, la réciproque est un cas particulier du théorème suivant $(h = 0)$.

THÉORÈME. - *Si* f *est un élément de* $A[[x]]$ *et* $P(x , y_0 , \dots , y_h)$ *un polynôme à coefficients dans* A *, tels que*

1 1° $P[x , f(x) , f^{\sigma}(x^p) , \dots , f^{\sigma^h}(x^{p^h})] = 0$,

2° $P(x , y , y^p , \dots , y^{p^h}) \not\equiv 0 \pmod{p}$,

3° *Il existe un polynôme* Q *à coefficients dans* A *, et deux entiers* k *et* i *tels que*

$$P(x , y_0 , \dots , y_h) = Q(x , y_0^{p^k} , \dots , y_h^{p^k})$$

$$\frac{\partial Q}{\partial y_i}[x , f^{p^k}(x) , f^{p^{k+1}}(x) , \dots , f^{p^{k+h}}(x)] \not\equiv 6 \pmod{p} .$$

Alors f *est un élément algébrique.*

Si $f = (f_0 , \dots , f_n , \dots)$, alors $f^{\sigma^h}(x^{p^h}) = (f_0^{p^h} , \dots , f_n^{p^h} , \dots)$, ce qui donne :

$$0 = W_n[P(x , f(x) , \dots , f^{\sigma^h}(x^{p^h})] \pmod{p^{n+1}}$$

$$= P[x^{p^n} , W_n(f_0 , \dots , f_n) , \dots , W_n(f_0^{p^h} , \dots , f_n^{p^h})] \pmod{p^{n+1}} ;$$

en particulier, on trouve

$$P(x , f_0 , \dots , f_0^{p^h}) = 0 \pmod{p} ,$$

ce qui montre, d'après la condition 2° que f_0 (qui appartient à $k[[x]]$) est algébrique sur $k(x)$.

La condition 3° permet d'écrire

$$P(x^{p^n} , y_0 + p^j z_0 , \dots , y_h + p^j z_0) = Q[x^{p^n} , (y_0 + p^j z_0)^{p^k} , \dots , (y_h + p^j z_h)^{p^k}]$$

$$= [Q + p^{j+k}(z_0 \frac{\partial Q}{\partial y_0} + \dots + z_h \frac{\partial Q}{\partial y_h})](x^{p^n} , y_0^{p^k} , \dots , y_h^{p^k}) \pmod{p^{j+k+1}}$$

ce qui donne, avec $j = n - k$,

$$P[x^{p^n}, W_n(f_0, \dots, f_n), \dots, W_n(f_0^{p^h}, \dots, f_n^{p^h})]$$

$$= P(x^{p^n}, f_0^{p^n} + \dots + p^{n-k-1} f_{n-k-1}^{p^{k+1}}, \dots, f_0^{p^{n+h}} + \dots + p^{n-k-1} f_{n-k-1}^{p^{k+h+1}})$$

$$+ p^n[[f_{n-k}^{p^k} \frac{\partial Q}{\partial y_0} + \dots + f_{n-k}^{p^{k+h}} \frac{\partial Q}{\partial y_h}](x^{p^n}, f_0^{p^{n+k}}, \dots, f_0^{p^{n+h+k}})] \pmod{p^{n+1}}.$$

par récurrence, on voit que le terme $P(\dots)$ doit être nul modulo p^n , et donc que f_{n-k} est zéro d'un polynôme à coefficients dans $k[[x]]$ dont le coefficient du terme de degré p^{k+i} est

$$[(\frac{\partial Q}{\partial y_i})^{\sigma^{-n}}(x, f_0^{p^k}, \dots, f_0^{p^{h+k}})]^{p^n},$$

c'est-à-dire n'est pas nul d'après l'hypothèse 3°, f_{n-k} est donc une fonction algébrique sur $k(x, f_0, \dots, f_{n-k-1})$ et, par récurrence, est algébrique sur $k(x)$.

Remarques. – La condition 3° n'est certainement pas la plus faible possible pour obtenir le résultat, on n'a en effet considéré que les termes linéaires de Q , mais les calculs deviennent très compliqués. La condition 2°, par contre, est indispensable ; on sait par exemple que la série théta : $\sum_{n=0} x^{n^2}$, est solution d'une équation du type

$$P(f(x), f(x^p), f(x^{p^2})) = 0 ,$$

telle que $P(y, y^p, y^{p^2}) = 0 \mod p$. Or, on peut démontrer que cette fonction n'est pas un élément algébrique.

BIBLIOGRAPHIE

[1] SERRE (J.-P.). – Corps locaux. – Paris, Hermann, 1962 (Act. scient. et ind., 1296 ; Publ. Inst. math. Univ. Nancago, 8).

(Texte reçu le 8 juillet 1976)

Gilles CHRISTOL
5 allée des Gradins
91350 GRIGNY