SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

GILLES CHRISTOL

Opération de Cartier et vecteurs de Witt

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 12 (1970-1971), exp. n° 13, p. 1-7

http://www.numdam.org/item?id=SDPP_1970-1971__12__A8_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1970-1971, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

OPÉRATION DE CARTIER ET VECTEURS DE WITT

par Gilles CHRISTOL

1. Introduction.

Si K est un corps de caractéristique p ($p \neq 0$), $D(K)$ le K -espace vectoriel des différentielles de K , et Z le sous-espace de $D(K)$ formé des éléments dont la différentielle est nulle, on peut définir l'opération de Cartier C de Z dans $D(K)$, et on sait que cette opération vérifie, pour tout $a \in K$ et tout π et $\pi' \in D(K)$:

- (i) $C(\pi + \pi') = C(\pi) + C(\pi')$, $C(a^p \pi) = aC(\pi)$;
- (ii) $C(da) = 0$;
- (iii) $C(da/a) = da/a$.

Ces propriétés peuvent d'ailleurs servir de définition à l'opération C .

Avec les notations ci-dessus, on démontre le théorème suivant :

THÉORÈME 1. - Soit $\pi \in D(K)$; pour qu'il existe $a \in K$, tel que $\pi = da/a$, il faut et il suffit que $\pi \in Z$ et que $C(\pi) = \pi$.

En particulier, si K est un corps de séries formelles à une variable sur un corps parfait k , de caractéristique p ($K = k((x))$), alors on a

$$C(\sum a(n) x^n (dx/x)) = \sum (a(np))^{1/p} x^n (dx/x) .$$

2. Définitions et notations.

Soit k un corps parfait, de caractéristique p ($p \neq 0$) ; $W(k)$ sera l'anneau des vecteurs de Witt de k , $A = W(k)((x))$ l'anneau des séries formelles à une variable sur $W(k)$, A^+ le sous-anneau de A des séries qui ne comprennent pas de puissances négatives de x , A^- l'anneau des polynômes en $1/x$, $D(A)$ (ou plus simplement D) le A -module des $W(k)$ -différentielles de A , et D^+ le sous-module $A^+ dx$. Nous noterons v la valuation de $W(k)$, nous munirons A de la valuation définie par

$$v(\sum a(n) x^n) = \inf(v(a(n))) ,$$

et la valuation d'un élément π de D sera donnée par

$$v(\pi) = v(b) , \quad \text{si } \pi = b dx ;$$

f désignera le frobénus de $W(k)$, et F l'endomorphisme de A défini par

$$F(\sum a(n) x^n) = \sum f(a(n)) x^{np} .$$

Enfin, nous noterons τ l'application canonique de $W(k)$ dans k (resp. de A dans $k((x))$, de D dans $D(k((x)))$).

Nous pouvons définir une opération C , de D dans D , par

$$C(\pi) = C(\sum \pi(n) x^n (dx/x)) = \sum f^{-1}(\pi(np)) x^n (dx/x) ,$$

et il est facile de vérifier, pour $a \in A$ et π et $\pi' \in D$, que

$$(1) \quad C(\pi + \pi') = C(\pi) + C(\pi') , \quad C(F(a)\pi) = aC(\pi) ,$$

$$(2) \quad v(C(\pi)) \geq v(\pi) ,$$

$$(3) \quad \overline{C(\pi)} = C(\overline{\pi}) ,$$

$$(4) \quad C(dF(a)) = p da ;$$

d'autre part, il est clair que C conserve l'espace D^+ .

3. Caractérisation des différentielles logarithmiques.

Nous nous proposons de généraliser le théorème 1 ; pour cela, nous noterons B l'ensemble des éléments de D qui sont de la forme $p da$.

LEMME 1. - $\pi \in B$, si, et seulement si, pour tout n , on a

$$v(C^n(\pi)) \geq n + 1 .$$

En effet, écrire $v(C^n(\pi)) \geq n + 1$ est équivalent à $v(f^{-n}(\pi(mp^n))) \geq n + 1$ pour tout m , c'est-à-dire, pour tout m et n , à $v(\pi(mp^n)) \geq n + 1$, ce qui s'exprime encore par il existe $a \in A$ tel que $\pi(mp^n) = p \cdot mp^n a(mp^n)$ pour tout n et tout m tel que $(m, p) = 1$, ce qui nous donne le lemme. En particulier, on aura $C(B) \subset p \cdot B$.

THÉORÈME 2. - $\pi \in D^+$ est de la forme da/a , avec $a \in A^*$ (ensemble des éléments inversibles de A^+), si, et seulement si,

$$\pi - C(\pi) \in B .$$

Pour la partie nécessaire, nous allons en fait démontrer que, si a est inversible dans A (et non dans A^+), alors $(da/a) - C(da/a) \in B$, c'est-à-dire, d'après le lemme,

$$(5) \quad v(C^{n+1}(da/a) - C^n(da/a)) \geq n + 1 .$$

Considérons d'abord le cas où $a = 1 + \alpha x^r$, pour lequel

$$da/a = r\alpha x^{r-1}/(1 + \alpha x^r) = r \sum_{m=1}^{\infty} \alpha^m x^{rm} (dx/x) ;$$

si, de plus, $(r, p) = 1$, alors

$$C^n(da/a) = r \sum_{m=1}^{\infty} f^{-n}(\alpha^{mp^n}) x^{rm} (dx/x) ;$$

comme f^{-1} conserve la valuation, nous pouvons appliquer la congruence $\alpha^{p^{n+1}} = f(\alpha^{p^n}) \pmod{p^{n+1}}$, ce qui donne

$$v(C^{n+1}(da/a) - C^n(da/a)) = \inf_m [v(f^{-n-1}(\alpha^{mp^{n+1}}) - f^{-n}(\alpha^{mp^n}))] \\ \geq n + 1 ;$$

si maintenant $r = r_0 p^h$, avec $(r_0, p) = 1$, on voit que $v(da/a) \geq h$; la relation (5) est donc évidente pour $n < h$, mais on a

$$C^h(da/a) = p^h r_0 \sum_{m=1}^{\infty} \alpha^m x^{r_0 m} (dx/x) ,$$

et, pour $n \geq h$, on est ramené au cas précédent. Si nous notons N l'ensemble des éléments de A qui vérifient la relation (5), nous avons donc prouvé que, pour tout $\alpha \in W(k)$ et tout r , $(1 + \alpha x^r) \in N$; il est facile de voir que N est fermé pour la multiplication, et pour le passage à la limite x -adique. Comme tout élément inversible dans A peut s'écrire sous la forme

$$a = a(h) x^h \prod_{r=1}^{\infty} (1 + \alpha_r x^r) ,$$

avec $a(h)$ inversible dans $W(k)$, $N = D$, ce qui achève la démonstration de la partie nécessaire du théorème.

LEMME 2. - Si $\pi \in D$ vérifie $C(\pi) - \pi \in B$, alors, pour tout n , il existe a_n , inversible dans A , tel que

$$(6) \quad v(C^n(\pi - (da_n/a_n))) \geq n + 1 .$$

D'après le théorème 1, si π est tel que $C(\bar{\pi}) - \bar{\pi} = \bar{0}$, il existe $\bar{a} \in k((x))$ qui vérifie $\bar{\pi} = d\bar{a}/\bar{a}$, et, par suite, il existe un élément a_0 , inversible dans A , tel que $\bar{a}_0 = \bar{a}$, qui donne (6) pour $n = 0$. Le lemme étant établi à l'ordre 0, nous le supposons vrai à l'ordre $n - 1$; nous posons

$$\omega = (1/p^n) C^n(\pi - (da_{n-1}/a_{n-1})) ,$$

$\omega \in D$, et vérifie

$$v(C(\omega) - \omega) = v[C^{n+1}(\pi - (da_{n-1}/a_{n-1})) - C^n(\pi - (da_{n-1}/a_{n-1}))] - n ;$$

or, d'après la partie suffisante, on sait que

$$v(C^{n+1}(da_{n-1}/a_{n-1}) - C^n(da_{n-1}/a_{n-1})) \geq n + 1 .$$

Comme, d'autre part, il résulte de l'hypothèse et du lemme 1 que

$$v(C^{n+1}(\pi) - C^n(\pi)) \geq n + 1 ,$$

il en résulte que

$$v(C(\omega) - \omega) \geq 1 ,$$

comme nous l'avons vu plus haut ; il existe donc b_n , inversible dans A , tel que

$$v(\omega - (db_n/b_n)) \geq 1 ,$$

ce qui s'écrit

$$v[C^n(\pi - (da_{n-1}/a_{n-1})) - p^n(db_n/b_n)] \geq n + 1 ;$$

or, d'après (1) et (4), nous savons que

$$C^n[dF^n(b_n)/F^n(b_n)] = p^n(db_n/b_n) ;$$

nous avons donc démontré le lemme, avec

$$a_n = a_{n-1} F^n(b_n) = a_0 \prod_{m=1}^n F^m(b_m) .$$

Pour aller plus loin, nous devons supposer $\pi \in D^+$. Cela entraîne en effet $a_0 = 1 + x(\dots)$ (puisque un premier terme en x^h entraînerait, dans π , des termes en $1/x$ par $dx^h/x^h = h/x$) ; de même ω , appartenant alors à D^+ , on choisira $b_n = 1 + x(\dots)$. Dans ces conditions, le produit infini

$$a = a_0 \prod_{m=1}^{\infty} F^m(b_m)$$

existe, et vérifie

$$v((da/a) - (da_n/a_n)) = v[\sum_{m=n+1}^{\infty} dF^m(b_m)/F^m(b_m)] = n + 1 ,$$

ce qui nous donne, pour tout n ,

$$v(C^n(\pi) - (da/a)) \geq n + 1 ,$$

c'est-à-dire qu'il existe, d'après le lemme 1, $b \in A$, tel que

$$\pi - (da/a) = p db .$$

Comme π et da/a appartiennent à D^+ , $b \in A^+$; par suite, on peut définir la série formelle $\exp pb$ (les limites étant prises au sens de la valuation v).

Comme

$$d(\exp pb)/(exp pb) = p db \quad ,$$

nous avons

$$\pi = da(\exp pb)/a(\exp pb) \quad ,$$

ce qui achève la démonstration du théorème 2.

Remarque. - Si nous supposons que $\pi \in D$ vérifie $\pi - C(\pi) \in B$, il est facile de constater que l'on a

$$\pi = p da^- + (\alpha/x) dx + (da^+/a^+) \quad ,$$

avec $a^- \in A^-$, $a^+ \in A^+$, et $\alpha \in \underline{Z}_p$.

Application. - Nous considérons la série formelle de $\underline{Z}_p((x))$,

$$y = x + x^p + \dots + x^{p^h} + \dots \quad ;$$

$\underline{Z}_p$ étant l'anneau des vecteurs de Witt sur F_p (corps à p éléments), on peut définir l'opération C sur $\underline{Z}_p((x))$, et on trouve

$$C(y(dx/x)) = y(dx/x) \quad ,$$

et par suite, en appliquant le théorème 2, on voit qu'il existe $z \in \underline{Z}_p((x))$, tel que

$$dz/z = y(dx/x) \quad ,$$

avec, en outre, $z = 1 + x(\dots)$. Or, dans $\underline{Q}_p((x))$, l'élément

$$z = \exp Y \quad , \quad \text{avec } dY = y(dx/x) \quad ,$$

est le seul à vérifier ces deux relations. Par suite,

$$z = \exp(x^p + (x^p/p) + \dots + (x^{p^h}/p^h) + \dots)$$

est une série formelle de $\underline{Z}_p((x))$. Remarquons qu'il est connu que

$$z = \sum_{n=0}^{\infty} (T(n)/n!) x^n \quad ,$$

où $T(n)$ est le nombre d'éléments du groupe des permutations dont l'ordre est une puissance de p (y compris $p^0 = 1$). Nous avons donc démontré que

$$v_p(T(n)) \geq v_p(n!) \quad .$$

4. Invariance de l'opération C .

Si y est un élément de D , tel que $y = x + \dots$, il existe un isomorphisme de $W(k)((y))$ dans A , continu pour les valuations x -adique et y -adique. L'opération

C , étant définie sur $W(k)((y))$ comme nous l'avons définie sur A , elle se transporte par cet isomorphisme en une opération de A , que nous noterons C_y (l'opération C étant donc l'opération C_x).

LEMME 3. - Pour tout y inversible dans A , on a, pour tout $n \in \mathbb{Z}$,

$$C(y^n(dy/y)) - y^{n/p}(dy/y) \in B,$$

avec la convention $y^{n/p} = 0$ si p ne divise pas n .

Si p ne divise pas n , il est en effet clair que

$$C(y^n(dy/y)) = C(dy^n/n) \in B.$$

D'autre part, nous avons

$$v(y^p - F(y)) \geq 1,$$

c'est-à-dire, puisque F est un automorphisme,

$$v(y^{p^{h+1}} - F(y^{p^h})) \geq h + 1,$$

ce qui donne

$$d(y^{p^{h+1}} - F(y^{p^h})) \in p^h B,$$

et, par suite, d'après (4),

$$C(p^{h+1} \cdot y^{p^{h+1}}(dy/y)) - p \cdot p^h y^{p^h}(dy/y) \in p^{h+1} B,$$

c'est-à-dire

$$C(y^{p^{h+1}}(dy/y)) - y^{p^h}(dy/y) \in B;$$

alors si $n = mp^h$, avec $(m; p) = 1$, nous aurons

$$C(y^{mp^h}(dy^m/y^m)) - y^{mp^{h-1}}(dy^m/y^m) \in B,$$

soit encore

$$m[C(y^n(dy/y)) - y^{n/p}(dy/y)] \in B,$$

et nous avons bien établi le lemme pour $n \neq 0$.

Le cas $n = 0$, ayant été traité dans le théorème 2, le lemme est démontré.

Nous avons donc, pour tout y de la forme $y = x + \dots$,

$$C_x(y^n(dy/y)) - C_y(y^n(dy/y)) \in B;$$

or C_x et C_y sont alors continus pour la valuation y -adique de A (qui est équivalente à la valuation x -adique). Comme B est fermé pour cette valuation, on

trouve, pour tout $a \in A$,

$$C_x(a(dx/x)) - C_y(a(dy/y)) \in B .$$

THÉOREME 3. - Pour tout $\pi \in D$, $C_x(\pi) - C_y(\pi) \in B$.

BIBLIOGRAPHIE

- [1] CARTIER (Pierre). - Questions de rationalité des diviseurs en géométrie algébrique, Bull. Soc. math. France, t. 86, 1958, p. 177-251 (Thèse Sc. math. Paris, 1958).

(Texte reçu le 21 juin 1971)

Gilles CHRISTOL
27 rue Charles Fourier
75 - PARIS 13