GILLES CHRISTOL

Opération de Cartier et vecteurs de Witt

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 12 (1970-1971), exp. nº 13, p. 1-7

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

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
12e année, 1970/71, n° 13, 7 p.

22 février 1971

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

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

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

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

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

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

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

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

Enfin, nous noterons $\overline{}$ 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

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

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

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

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

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

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

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

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

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

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,

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

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

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

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

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

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

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

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

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

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

et, pour $n \geqslant h$, 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

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

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

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

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

D'après le théorème 1, si π est tel que $C(\overline{\pi}) - \overline{\pi} = \overline{0}$, il existe $\overline{a} \in k((x))$ qui vérifie $\overline{\pi} = d\overline{a}/\overline{a}$, et, par suite, il existe un élément a_0 , inversible dans A , tel que $\overline{a}_0 = \overline{a}$, 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

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

$\omega \in D$, et vérifie

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

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

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

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

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

il en résulte que

$$v(C(\omega) - \omega) \geqslant 1 \quad ,$$

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

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

ce qui s'écrit

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

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

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

nous avons donc démontré le lemme, avec

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

Pour aller plus loin, nous devons supposer $\pi \in D^+$. Cela entraîne en effet $a_0 = 1 + x(\ldots)$ (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 $b_n = 1 + x(\ldots)$. Dans ces conditions, le produit infini

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

existe, et vérifie

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

ce qui nous donne, pour tout n ,

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

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

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

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 $\alpha \in \underset{\sim}{Z}_p$.

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

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

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

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

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

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

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

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

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

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

est une série formelle de $\underset{\sim}{Z}_p((x))$. 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

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

4. Invariance de l'opération C .

Si y est un élément de D , tel que $y = x + \ldots$, 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 $n \in \mathbb{Z}$,

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

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

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

D'autre part, nous avons

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

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

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

ce qui donne

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

et, par suite, d'après (4),

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

c'est-à-dire

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

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

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

soit encore

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

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 $y = x + \dots$,

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

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 $a \in A$,

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

THÉORÈME 3. - <u>Pour tout</u> $\pi \in D$, $C_x(\pi) - C_y(\pi) \in B$.

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