Séminaire Dubreil.
Algèbre et théorie
des nombres

Pierre Samuel

Classes de diviseurs et dérivées logarithmiques

Séminaire Dubreil. Algèbre et théorie des nombres, tome 16, n° 1 (1962-1963), exp. n° 3, p. 1-30

<http://www.numdam.org/item?id=SD_1962-1963__16_1_A3_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
16e année, 1962/63, n° 3

19 novembre 1962

CLASSES DE DIVISEURS ET DÉRIVÉES LOGARITHMIQUES

par Pierre SAMUEL

1. Classes de diviseurs d'un anneau de Krull.

Ce paragraphe est un rappel de résultats classiques. Cf. [2], [5] ou [9].

Soit A un anneau intègre. La relation $(A:b) = (A:b')$ entre idéaux (entiers ou fractionnaires) b, b' de A est une relation d'équivalence, dite "équivalence d'Artin" ou "Quasi-Gleichheit" ! Les classes d'équivalences s'appellent les diviseurs de A. La classe d'un idéal b admet un plus grand élément, à savoir $b' = A:(A:b)$ (autrement dit l'application $b \rightsquigarrow A:(A:b)$ est une opération de fermeture) ; les idéaux b' tels que $b' = A:(A:b')$ sont dits divisoriels ; les idéaux divisoriels sont donc en correspondance biunivoque avec les diviseurs ; on montre qu'ils ne sont autres que les intersections d'idéaux principaux.

La multiplication des idéaux donne aussitôt une multiplication des diviseurs (ou des idéaux divisoriels) : l'idéal divisoriel "produit" de deux idéaux divisoriels a, b est l'idéal divisoriel $A:(A:ab)$. Muni de cette loi et de la relation correspondant à l'inclusion, l'ensemble des diviseurs de A est un monoïde ordonné, que nous noterons $D(A)$; les éléments positifs de $D(A)$ correspondent aux idéaux entiers ; on utilise la notation additive. Pour que $D(A)$ soit un groupe, il faut et il suffit que l'anneau A soit complètement intégralement clos. Lorsque $D(A)$ est un groupe ordonné dont les éléments positifs vérifient la condition minimale, on dit que A est un anneau de Krull ; il s'ensuit aussitôt qu'un anneau noethérien intégralement clos est un anneau de Krull ; c'est d'ailleurs là l'exemple le plus important d'anneaux de Krull.

Soit A un anneau de Krull. La théorie élémentaire des groupes ordonnés montre que $D(A)$ est isomorphe à un groupe ordonné de la forme $\underset{\sim}{Z}^{(I)}$; la base de $D(A)$ correspondant à la base canonique de $\underset{\sim}{Z}^{(I)}$ est formée des diviseurs strictement positifs minimaux. On démontre :

a. les idéaux divisoriels p, correspondant à ces éléments de base, ne sont autres que les idéaux premiers de hauteur 1 de A (c'est-à-dire $p \neq (0)$, et p ne contient d'autre idéal premier que soi-même et (0)) ;

b. Pour un tel p, l'anneau de fractions A_p est l'anneau d'une valuation discrète normée v_p ;

c. A est l'intersection de ces A_p ;

d. Pour tout $x \neq 0$, les $v_p(x)$ sont presque tous nuls.

Notant $P(A)$ l'ensemble des idéaux premiers de hauteur 1 de A, et identifiant diviseurs et idéaux divisoriels, tout diviseur $\mathfrak{d}$ s'écrit, et de façon unique, sous la forme

$$\mathfrak{d} = \sum_{p \in P(A)} n(p) \cdot p \ , \tag{1}$$

où les $n(p)$ sont des entiers presque tous nuls.

Le diviseur correspondant à l'idéal principal Aa se note (a) et vaut

$$(a) = \sum_{p \in P(A)} v_p(a) \cdot p \ . \tag{2}$$

Les diviseurs correspondant aux idéaux principaux sont appelés les diviseurs principaux ; ils forment un sous-groupe, noté $F(A)$, de $D(A)$. Le groupe quotient $D(A)/F(A)$ est noté $C(A)$, et s'appelle le groupe des classes de diviseurs de A. Les anneaux factoriels sont les anneaux de Krull A tels que $C(A) = 0$.

Remarques.

1. Géométriquement le passage des idéaux aux diviseurs consiste à négliger les sous-variétés de codimension ≥ 2 (et donc à ne s'intéresser qu'à la codimension 1).

2. Considérons un anneau intègre A et une famille $(v_i)_{i \in I}$ de valuations discrètes du corps des fractions K de A telle que A soit l'intersection des anneaux des v_i, et que, pour tout $x \neq 0$, les $v_i(x)$ soient presque tous nuls. On montre alors que A est un anneau de Krull. Cette propriété est prise comme définition par plusieurs auteurs.

3. La famille des anneaux de Krull est stable pour les opérations suivantes : formation d'anneaux de fractions, formation d'anneaux de polynômes et de séries formelles, passage à la fermeture intégrale dans une extension finie du corps des fractions.

Soient maintenant A un anneau de Krull, et A' un sous-anneau de Krull de A : $A' \to A$. Pour tout $p \in P(A')$, les $\mathfrak{P} \in P(A)$ tels que $\mathfrak{P} \cap A' = p$ sont en nombre fini. La restriction de $v_{\mathfrak{P}}$ au corps des fractions K' de A' est alors une valuation équivalente à v_p ; notons $e(\mathfrak{P}.p)$ l'indice de ramification correspondant. Faisons correspondre à p le diviseur

$$(3) \qquad j(\dot{p}) = \sum_{\mathfrak{P} \cap A' = p} e(\mathfrak{P}.p).\mathfrak{P} \ .$$

Par linéarité j s'étend en un homomorphisme (noté encore j) de $D(A')$ dans $D(A)$. Supposons vérifiée la condition suivante :

(PDE) Pour tout $\mathfrak{P} \in P(A)$, l'idéal premier $\mathfrak{P} \cap A'$ est nul ou de hauteur 1.

On montre alors que, pour tout $x \in K'$ non nul, on a $j((x)_{A'}) = (x)_A$; ainsi j applique $F(A')$ dans $F(A)$, de sorte que, par passage aux quotients, on obtient un homomorphisme canonique $\overline{j}$ de $C(A')$ dans $C(A)$. La condition (PDE) est satisfaite dans les deux cas suivants :

1° A est entier sur A' (cela résulte en effet du "second théorème de Cohen-Seidenberg") ; nous allons en voir des exemples dans la suite de cet exposé ; ces exemples sont qualifiés (peut-être improprement) d'exemples "de descente" car nous déduirons certains renseignements sur $C(A')$ des propriétés du grand anneau A.

2° A est un A'-module plat. Contentons-nous de citer les résultats suivants (démonstrations et autres exemples dans [2] et [6]) :

THÉORÈME de Nagata. - Soient B un anneau de Krull et S une partie multiplicative de B. Alors $\overline{j} : C(B) \to C(S^{-1}B)$ est **surjectif**. Si, de plus, S est engendrée par des éléments premiers, alors $\overline{j}$ est bijectif.

THÉORÈME de Gauss. - Soient B un anneau de Krull et X une indéterminée. Alors $\overline{j} : C(B) \to C(B[X])$ est bijectif.

THÉORÈME de Mori. - Soit B un anneau de Zariski dont le complété $\hat{B}$ soit un anneau de Krull. Alors B est un anneau de Krull, et $\overline{j} : C(B) \to C(\hat{B})$ est injectif.

Nous laissons le soin au lecteur d'énoncer les corollaires de ces trois théorèmes relatifs aux anneaux factoriels.

2. La descente galoisienne.

Soient A un anneau de Krull, G un groupe cyclique fini d'automorphismes de A, s un générateur de G, et A' l'anneau des invariants de G ; on sait que A est entier sur A' (pour $a \in A$, le polynôme $\prod_{t\in G} (X - t(a))$ a ses coefficients dans A'). Le groupe G opère aussi sur le corps des fractions K de A ; ici on a un sous-corps d'invariants K' ; la théorie de Galois montre que $[K:K'] = \mathrm{card}(G)$; on a évidemment $A' = K' \cap A$, de sorte que (par le critère valuatif) A' est un anneau de Krull ; on voit aussitôt que K' est le corps des fractions de A'.

Nous allons étudier ici le noyau $\mathrm{Ker}(j)$ de l'homomorphisme canonique

$$\overline{j} : C(A') \to C(A) .$$

Dans de nombreux exemples, A sera factoriel, de sorte que $\mathrm{Ker}(\overline{j}) = C(A')$ et que nous déterminerons ainsi le groupe des classes de diviseurs de A'. Soit h l'homomorphisme de K^* dans K^* défini par $h(x) = s(x)/x$; écrivant $x = a/N(b)$ avec $a, b \in A$, on voit qu'on a $h(K^*) = h(A^*)$. Nous noterons U le groupe multiplicatif des unités (= éléments inversibles) de A.

Soit D_1 le groupe des diviseurs $\mathfrak{d}$ de A' tels que $j(\mathfrak{d})$ soit un diviseur principal de A ; on a $F(A') \subset D_1$, et le noyau de $\overline{j}$ est $D_1/F(A')$. Pour $\mathfrak{d} \in D_1$, on a $j(\mathfrak{d}) = (a)$ avec $a \in K$; comme $j(\mathfrak{d})$ est invariant par G, on a $(s(a)) = (a)$, c'est-à-dire $h(a) = s(a)/a \in U$, d'où $h(a) \in U \cap \mathrm{Im}(h)$. Or $U \cap \mathrm{Im}(h)$ contient évidemment $h(U)$. Pour $\mathfrak{d} \in D_1$, la classe de $h(a)$ modulo $h(U)$ est indépendante de l'élément a de A qu'on a choisi ; en effet, si $(a) = (a')$, on a $a' = au$ avec $u \in U$, d'où $h(a') = h(a)\, h(u)$; nous désignerons cette classe par $\varphi(\mathfrak{d})$.

Soient $\mathfrak{d} \in D_1$ et $a \in K$ tels que $j(\mathfrak{d}) = (a)$. On a les équivalences : $\varphi(\mathfrak{d}) = 1 \iff h(a) \in h(U) \iff$ il existe $u \in U$ tel que $s(a)/a = s(u)/u \iff$ il existe $u \in U$ tel que $a/u = s(a/u) \iff$ il existe $u \in U$ tel que $a/u \in A'$ (ici on utilise le fait que G est cyclique) $\iff \mathfrak{d} = (a/u)$ (dans A') $\iff \mathfrak{d}$ est principal.

Le noyau de φ est donc $F(A')$. D'où la première assertion du théorème suivant :

THÉORÈME 1. - Avec les hypothèses ci-dessus ("descente cyclique"), on définit un monomorphisme canonique

$$\bar{\varphi} : \mathrm{Ker}(\bar{j}) \to (U \cap \mathrm{Im}(h))/h(U) .$$

Si aucun diviseur premier de A n'est ramifié sur A', alors $\bar{\varphi}$ est un isomorphisme.

Il reste à démontrer l'assertion de surjectivité de $\bar{\varphi}$, c'est-à-dire : si un élément a de K est tel que $h(a) \in U$, alors le diviseur (a) est de la forme $j(b)$. L'hypothèse veut dire que (a) est invariant par G. Or, si p' est un diviseur premier de A', les diviseurs premiers distincts p_i $(i = 1, \dots, g(p'))$ de A au-dessus de p' (c'est-à-dire $p' = p_i \cap A'$) sont deux à deux conjugués par G, et l'hypothèse de non-ramification implique que $j(p') = p_1 + \dots + p_{g(p')}$. Comme (a) est invariant par G, deux diviseurs premiers conjugués y figurent avec le même coefficient, de sorte que (a) est une somme de diviseurs de la forme $j(p')$; donc (a) est de la forme $j(b)$.

C. Q. F. D.

Remarque 1. - Notons h' et N' les restrictions de h et de l'homomorphisme "norme" au groupe U. D'après le "théorème 90 de Hilbert", on a

$$U \cap \mathrm{Im}(h) = \mathrm{Ker}(N') ;$$

donc $\bar{\varphi}$ est un monomorphisme (resp. isomorphisme dans le cas "divisoriellement non-ramifié") de $\mathrm{Ker}(\bar{j})$ dans $\mathrm{Ker}(N')/\mathrm{Im}(h')$. Nous laissons aux cocyclistes le soin de dire ça en termes de cohomologie.

Remarque 2. - L'hypothèse de non-ramification est essentielle. Prenons pour A l'anneau $\underset{\sim}{Z}[i]$ des entiers de Gauss, pour G le groupe formé de l'identité et de la conjugaison s ; alors

$$A' = \underset{\sim}{Z} ;$$

on a

$$C(A) = C(A') = 0 ,$$

car A et A' sont des anneaux principaux ; d'où

$$\mathrm{Ker}(\overline{j}) = 0 .$$

Ici U est formé de 1 , -1 , i , $-i$; on a

$$h(U) = \{1 , -1\} ;$$

par contre $i \in U \cap \mathrm{Im}(h)$ puisque

$$h(1 - i) = (1 + i)/(1 - i) = i ,$$

d'où

$$U \cap \mathrm{Im}(h) = U .$$

On rappelle que le nombre premier 2 se ramifie dans A . Dans le cas général, il serait intéressant d'étudier comment la ramification divisorielle de A sur A' est décrite par le conoyau de $\overline{\varphi}$.

Remarque 3. - Dans le cas d'un groupe fini G quelconque d'automorphismes de A , on peut procéder comme suit. Posons

$$q = \mathrm{card}(G) .$$

Pour $x \in K^*$, posons

$$h(x) = (s(x)/x)_{s \in G} \in (K^*)^q .$$

Pour $\mathfrak{b} \in D_1$, soit $j(\mathfrak{b}) = (a)$ $(a \in K)$, on a

$$h(a) \in h(K^*) \cap U^q ,$$

et la classe $\theta(\mathfrak{b})$ de $h(a)$ modulo $h(U)$ est bien déterminée par $\mathfrak{b}$. Pour que $\theta(\mathfrak{b}) = 1$, il faut et il suffit qu'il existe $u \in U$ tel que $s(a)/a = s(u)/u$ pour tout $s \in G$, c'est-à-dire que a/u soit invariant par G . Autrement dit le noyau de θ est $F(A')$, d'où un monomorphisme

$$\overline{\theta} : \mathrm{Ker}(J) \to (h(K^*) \cap U^q)/h(U) .$$

Lorsqu'aucun diviseur premier de A n'est ramifié sur A' , on montre encore que $\overline{\theta}$ est un isomorphisme ; en effet, pour $a \in K$, la relation $h(a) \in U^q$ veut dire qu'on a $(s(a)) = (a)$ pour tout $s \in G$, c'est-à-dire que le diviseur (a)

est invariant par G ; comme dans le théorème 1, ceci implique que (a) est de la forme $j(b)$, vu la non-ramification.

Remarque 4. - Pour nous assurer, dans les exemples, de la non-ramification divisorielle de A sur A', nous utiliserons le résultat suivant : si p est un idéal premier ramifié de hauteur 1 de A, si x est un élément de A qui est élément primitif de K sur K', et si F est le polynôme minimal de x sur K', la dérivée $F'(x)$ appartient à p (voir [8] chap. III, ou [9] chap. V, § 11, corollaire du théorème 28 et théorème 29 ; ces auteurs travaillent avec des anneaux de Dedekind, mais, comme nous ne nous intéressons qu'aux idéaux divisoriels, nous nous ramenons à leur cas par localisation par rapport à $A' - (p \cap A')$).

Exemples polynomiaux.

1. Soient k un corps, A l'anneau de polynômes $k[x_1, \ldots, x_d]$ $(d \geqslant 2)$, n un entier étranger à l'exposant caractéristique de k, w une racine primitive n-ième de l'unité contenue dans k, s le k-automorphisme de A défini par $s(x_i) = wx_i$ pour tout i, et G le groupe cyclique d'ordre n engendré par s. L'anneau A' des invariants de G est engendré par les monômes de degré n en les x_i ; géométriquement c'est l'anneau de coordonnées homogènes du modèle n-uple de l'espace projectif. Pour $x = x_i$, la dérivée de la remarque 4 est nx_i^{n-1} ; aucun idéal premier de hauteur 1 ne contenant tous les nx_i^{n-1} (car $d \geqslant 2$), il n'y a pas de ramification divisorielle. Le groupe U des unités de A est k^* ; les unités de norme 1 (c'est-à-dire $U \cap \mathrm{Im}(h)$ vu le théorème 90 ; cf. remarque 1) sont les racines n-ièmes de l'unité, tandis que $h(U)$ est réduit à 1. Comme A est factoriel, on déduit du théorème 1 que $C(A')$ est un groupe cyclique d'ordre n.

2. Soient k un corps, A l'anneau de polynômes $k[x, y]$, n un entier étranger à l'exposant caractéristique de k, w une racine primitive n-ième de l'unité contenue dans k, s le k-automorphisme de A défini par $s(x) = wx$ et $s(y) = w^{-1}y$ et G le groupe cyclique d'ordre n qu'il engendre. L'anneau A' des invariants de G est engendré par les monômes x^n, y^n et xy, de sorte que c'est l'anneau de coordonnées affines de la surface $Z^n - XY = 0$. Les dérivées de la remarque 4 sont nx^{n-1} et ny^{n-1}, de sorte qu'il n'y a pas de ramification divisorielle. Comme dans l'exemple 1, on a $U = k^*$, et G opère trivialement dans U. On en déduit encore que $C(A')$ est un groupe cyclique d'ordre n.

3. Donnons maintenant un exemple du type "Artin-Schreier". Soient k un corps de caractéristique $p \neq 0$, $A = k[x, y]$ et s le k-automorphisme d'ordre p défini par $s(x) = x$ et $s(y) = y + x$. L'exemple est peu intéressant, car l'anneau A' des invariants est engendré par x et $N(y) = y^p - x^{p-1} y$, donc est factoriel. Le polynôme minimal $F(T)$ de y sur K' est $T^p - x^{p-1} T - N(y)$, d'où $F'(y) = -x^{p-1}$; ainsi seul l'idéal Ax pourrait être ramifié, mais il ne l'est pas car $x \in A'$ (de sorte que Ax est inerte) ; le théorème 1 peut donc s'appliquer. On constate que $U = k^*$; pour $a \in k$, on a $N(a) = a^p$, de sorte que 1 est la seule unité de norme 1 ; ainsi $U \cap \mathrm{Im}(h)$ et $h(U)$ sont réduits à 1, ce qui confirme la factorialité de A'.

Exemples en séries formelles. - Nous allons ici remplacer les anneaux de polynômes A des exemples 1 et 2 ci-dessus par les anneaux de séries formelles correspondants. Rien n'est changé pour la détermination des anneaux A', ni pour la non-ramification divisorielle. Par contre les unités de A sont ici les séries formelles d'ordre 0, ce qui rend un peu moins facile le calcul de $U \cap \mathrm{Im}(h)$ et $h(U)$. On utilise le lemme suivant :

LEMME. - Soient A un anneau local intègre, m son idéal maximal, et s un automorphisme de A d'ordre fini n étranger à l'exposant caractéristique de A/m. Tout élément u de $1 + m$ qui est de la forme $s(a)/a$ avec $a \in A$, est aussi de la forme $s(v)/v$ avec v inversible dans A.

En effet, comme dans le "théorème 90", on forme l'élément

$$v = 1 + u + u^{1+s} + \ldots + u^{1+s+\ldots+s^{n-2}} .$$

On a $v \equiv n.1 \pmod{m}$ de sorte que v est inversible (car $n.1 \notin m$). Comme $u = s(a)/a$, on a

$$u^{1+s+\ldots+s^{n-2}+s^{n-1}} = 1 ,$$

d'où facilement

$$u.v^s = v \quad \text{et} \quad u = v^{1-s} = v/s(v) .$$

C. Q. F. D.

Le lemme s'applique dans les analogues des exemples 1 et 2, et montre qu'il suffit de travailler dans $U/(1 + m) = k^*$. On obtient donc le même résultat que

pour les polynômes. Notons que, si A' est l'anneau des polynômes invariants, l'anneau des séries formelles invariantes est le complété $\hat{A}'$. Ainsi, dans les deux exemples, l'homomorphismes canonique $C(A') \to C(\hat{A}')$ est bijectif (cf. § 1) ; nous verrons qu'il n'en n'est pas de même dans certains exemples de descente p-radicielle.

Note. - On peut généraliser ainsi les exemples 1 et 2 : on prend $A = k[x_1, \dots, x_d]$ (ou $k[[x_1, \dots, x_d]]$) $(d \geqslant 2)$, n étranger à l'exposant caractéristique de k, et pour w une racine primitive n-ième de l'unité ; on définit l'automorphisme s par $s(x_i) = w^{n(i)} x_i$, n et les exposants $n(i)$ étant étrangers dans leur ensemble. Alors $C(A')$ est encore cyclique d'ordre n. Nous laissons au lecteur le soin de décrire l'anneau A' des invariants.

3. Théorie de la descente p-radicielle.

Les exemples de "descente" les plus intéressants sont des exemples de descente p-radicielle (= "pûrement inséparable") en caractéristique $p \neq 0$. Comme d'habitude les automorphismes y sont remplacés par des dérivations.

Soient A un anneau de Krull de caractéristique $p \neq 0$, K son corps des fractions, D une dérivation de K telle que $D(A) \subset A$, K' le sous-corps $\mathrm{Ker}(D)$, et A' l'anneau de Krull $K' \cap A$. On a $K^p \subset K'$ et $A^p \subset A'$, de sorte que A est entier sur A', et que l'homomorphisme canonique $\bar{j} : C(A') \to C(A)$ est défini (cf. § 1). Nous allons encore étudier le noyau $\mathrm{Ker}(\bar{j})$. Notons encore U le groupe des unités de A.

Soit D_1 le groupe des diviseurs $\mathfrak{d}$ de A' tels que $j(\mathfrak{d})$ soit principal ; on a $\mathrm{Ker}(\bar{j}) = D_1/F(A')$. Soient $\mathfrak{d} \in D_1$ et $a \in K$ tels que $j(\mathfrak{d}) = (a)$. Pour tout idéal premier p de hauteur 1 de A, il existe $a' \in K'$ tel que $v_p(a) = v_p(a')$; il existe donc un élément inversible x de l'anneau de valuation A_p tel que $a = xa'$, d'où $Da/a = Dx/x$, et $Da/a \in A_p$ car A_p est stable par D. Ceci ayant lieu pour tout p, on a $Da/a \in A$. Nous noterons $\underset{\sim}{D}$ le sous-groupe additif de A composé des éléments de la forme Dt/t avec $t \in K$ ("les dérivées logarithmiques") ; il contient le sous-groupe $\underset{\sim}{D}'$ des dérivées logarithmiques d'unités (c'est-à-dire des Du/u, où u parcourt U). La classe de Da/a modulo $\underset{\sim}{D}'$ ne dépend que du diviseur $\mathfrak{d}$ de A' ; nous la noterons $\varphi(\mathfrak{d})$. Ainsi φ est un homomorphisme de D_1 dans $\underset{\sim}{D}/\underset{\sim}{D}'$. Comme la relation $Da/a = Du/u$ $(a \in K,\ u \in U)$ équivaut à $D(a/u) = 0$, c'est-à-dire à $a/u \in K'$, le noyau de φ est $F(A')$. D'où la première assertion du théorème suivant :

THÉORÈME 2. - Avec les hypothèses et notations ci-dessus ("descente p-radicielle") on a un monomorphisme canonique $\overline{\varphi} : \mathrm{Ker}(\overline{j}) \to \underset{\sim}{D}/\underset{\sim}{D}'$ ($\underset{\sim}{D}$: dérivées logarithmiques qui se trouvent dans A ; $\underset{\sim}{D}'$: dérivées logarithmiques d'unités). Si, de plus, on a $[K:K'] = p$ et si $D.A$ n'est contenu dans aucun idéal premier de hauteur 1 de A, alors $\overline{\varphi}$ est un isomorphisme.

Les notations A, A', $\underset{\sim}{D}$, $\underset{\sim}{D}'$ seront utilisées sans avertissement dans la suite.

Démontrons l'assertion de surjectivité. Comme K est p-radiciel sur K', toute valuation de K' se prolonge de façon unique à K. Donc un diviseur $\sum_p n(p).p$ de A provient de A' si et seulement si, pour tout p, $n(p)$ est multiple de l'indice de ramification $e(p)$ de p sur K' (cf. § 1, (3)). Comme $[K:K'] = p$, on a, soit $e(p) = 1$ (et on dit que p est inerte), soit $e(p) = p$ (et on dit que p est ramifié). Soit alors $a \in K$ tel que $Da/a \in A$; il s'agit de montrer que, si $n = v_p(a)$ n'est pas multiple de p, alors p est inerte. Soit t une uniformisante pour p ; écrivons $a = ut^n$ où u est inversible dans A_p. On a

$$(Du/u) + n(Dt/t) = Da/a \in A \subset A_p ,$$

d'où

$$Dt/t \in A_p ,$$

de sorte que l'idéal maximal $tA_p = pA_p$ est stable pour D. Ainsi D définit, par passage au quotient, une dérivation $\overline{D}$ du corps résiduel $k = A_p/pA_p$. Comme il existe un élément b de A tel que $Db \notin p$, on a $\overline{D} \neq 0$. Soit k' le corps résiduel de la restriction de v_p à K' ; comme $\overline{D}(k') = 0$, on a $k' \neq k$. La formule " $ef \leqslant [K:K']$ " montre alors qu'on a $f = [k:k'] = p$ et $e = e(p) = 1$.

C. Q. F. D.

Remarque. - L'hypothèse sur l'image $D.A$ de A par D est peu restrictive : dans de nombreux exemples, A est factoriel, et il suffit de diviser D par un p. g. c. d. des éléments Db, où b parcourt A. L'hypothèse $[K:K'] = p$

est essentielle pour la surjectivité de $\overline{\varphi}$, comme le montre l'exemple suivant. Soient k un corps de caractéristique 2 , A l'anneau de polynômes $A = k[x , y , z]$ et D la k-dérivation définie par $Dx = y^4$, $Dy = x^2$, $Dz = xyz$. On a $Dz/z \in A$, et nous allons montrer que le diviseur (z) ne provient pas de $K' = \mathrm{Ker}(D)$, c'est-à-dire que l'idéal premier Az est ramifié. Supposons-le inerte. La valuation (z)-adique serait alors uniformisée par un élément de A' , nécessairement de la forme $a(x , y , z).z$, où a est un polynôme tel que $b = a(x , y , 0) \neq 0$. Comme $Dz/z = xy$ et que $D(az) = 0$, on a $Da/a = - xy$, d'où $Db/b = - xy$ en faisant $z = 0$ (noter que $k[x , y]$ est stable par D et que $Dz \in Az$). Or on a $D^2 t = 0$ pour tout $t \in k(x , y)$ (car D^2 est une dérivation en caractéristique 2) ; d'où

$$D(- xy) = D(Db/b) = - (Db/b)^2 = - x^2 y^2 .$$

C'est absurde, car

$$D(xy) = x.Dy + y.Dx = x^3 + y^5 .$$

Afin de traiter les exemples, nous aurons besoin de quelques formules sur les dérivées et dérivées logarithmiques en caractéristique p .

4. Formulaire des dérivées logarithmiques.

Soient K un corps de caractéristique $p \neq 0$ et D une dérivation de K . Nous utiliserons la formule de Barsotti-Cartier ([1], [3])

$$(4) \qquad D^{p-1}\left(\frac{Dx}{x}\right) = \frac{D^p(x)}{x} - \left(\frac{Dx}{x}\right)^p \qquad (x \in K)$$

et la formule de Hochschild ([4], [3])

$$(5) \qquad (tD)^p = t^p D^p + (tD)^{p-1}(t).D$$

($t \in K$; tD désigne la dérivation $x \rightsquigarrow t.Dx$) .

LEMME 1. - *Soient K un corps de caractéristique $p \neq 0$, D une dérivation de K , et K' le sous-corps $\mathrm{Ker}(D)$. Si $[K:K'] = p$, il existe $a \in K'$ tel que $D^p = aD$.*

En effet, on a $K = K'(x)$ avec $x \in K$ (et $x^p \in K'$). Une K'-dérivation de K étant entièrement déterminée par sa valeur en x, on a $D^p = aD$ avec $a \in K$. Pour montrer que $a \in K'$, prenons $t = 1/Dx$ dans la formule d'Hochschild ; comme tD est la dérivation par rapport à x, on a

$$(tD)^p = 0 ,$$

d'où

$$(tD)^{p-1}(y) \in K' \quad \text{pour tout} \quad y \in K ;$$

il vient donc

$$D^p = - t^{-p} . (tD)^{p-1}(t) . D ,$$

d'où

$$a \in K' .$$

LEMME 2. - Avec les mêmes hypothèses et notations, pour qu'un élément t de K soit une dérivée logarithmique, il faut et il suffit qu'on ait

$$D^{p-1}(t) - at + t^p = 0 .$$

La nécessité résulte aussitôt de la formule de Barsotti-Cartier. Supposons réciproquement qu'on ait

$$D^{p-1}(t) - at + t^p = 0 ,$$

et montrons que t est une dérivée logarithmique ; on peut supposer $t \neq 0$. Considérons la dérivation $E = t^{-1} D$, et appliquons la formule de Hochschild à t et E ; il vient

$$D^p = t^p E^p + D^{p-1}(t) . E = t^p E^p + (at - t^p) E ;$$

comme $D^p = aD = atE$, on en déduit $E^p = E$. Ceci s'écrit

$$E(E - I)(E - 2I)\dots(E - (p-1)\,I) = 0 \ ,$$

où I désigne l'application identique de K. Partons d'un élément y de K tel que $Ey \neq 0$, et formons

$$y_1 = Ey \ , \quad y_2 = (E - I)y_1 \ , \quad y_3 = (E - 2I)y_2 \ , \text{ etc.}$$

Il existe un indice j compris entre 1 et $p-1$ tel que $y_j \neq 0$ et que $y_{j+1} = 0$. On a alors $Ey_j = jy_j$. Soient n un inverse de j modulo p, et $x = y_j^n$. On a $Ex = x$, c'est-à-dire $t^{-1} Dx = x$ ou encore $t = Dx/x$.

C. Q. F. D.

On a aussi démontré que, pour que t soit une dérivée logarithmique pour D, il faut et il suffit que $(t^{-1} D)^p = t^{-1} D$.

Le résultat suivant a des chances d'être vrai, mais, pour l'instant, je ne l'ai démontré que dans des cas particuliers :

CONJECTURE. - Soient A un anneau intègre de caractéristique $p \neq 0$, et D une dérivation de A. Si une dérivée logarithmique t appartient à l'idéal q engendré par les Dx $(x \in A)$ alors t est la dérivée logarithmique d'une unité.

Comme on a $Du/u \in q$ quand u est une unité, la conjecture s'écrit

$$\underset{\sim}{D}' = \underset{\sim}{D} \cap q \ . \tag{6}$$

LEMME 3. - La conjecture est vraie sous les hypothèses suivantes : $p = 2$, A est local factoriel, on a $D^2 = aD$ avec $a \in \mathrm{Ker}(D)$ (cf. lemme 1), il existe deux éléments x, y de m tels que $q = (Dx , Dy)$.

Soit t une dérivée logarithmique de la forme $t = r.Dx + s.Dy$ $(r , s \in A)$. Divisant D et t par un p. g. c. d. de Dx et Dy, on voit qu'on peut supposer Dx et Dy étrangers. D'après le lemme 2 (ou par un calcul direct facile), on a $Dt + at + t^2 = 0$. En explicitant, ceci donne

$$(Dr + r^2\, Dx)\, Dx = (Ds + s^2\, Dy)\, Dy \ .$$

Il existe donc $b \in A$ tel que

$$Dr = r^2\,Dx + b\,Dy \quad \text{et} \quad Ds = s^2\,Dy + b\,Dx \ .$$

Par dérivations on voit que

$$Db.Dx = Db.Dy = 0 \ ,$$

de sorte que

$$Db = 0 \ .$$

Posons alors

$$u = 1 + rx + sy + (rs + b)\,xy \ ;$$

un calcul de trois lignes montre qu'on a $Du = +1$. Or, comme $u \in 1 + m$, u est une unité de A.

LEMME 4. - La conjecture est vraie sous les hypothèses suivantes : $p = 2$, 3 ou 5 (A est local), on a $D^p = D$, on a $q \subset m$.

Nous allons montrer que toute dérivée logarithmique t qui appartient à m est dérivée logarithmique d'une unité. Pour $p = 2$, on a

$$Dt = t^2 + t \qquad \text{(lemme 2)} \ ,$$

d'où

$$t = D(1 + t)/(1 + t) \ .$$

Pour $p = 3$, on a

$$D^2 t - t + t^3 = 0 \qquad \text{(lemme 2)} \ ,$$

d'où

$$D(Dt - t^2 + 1) = t(Dt - t^2 + 1) \ ;$$

comme $Dt \in m$, t est dérivée logarithmique de l'élément $1 + Dt - t^2$ de $1 + m$.

Enfin, pour $p = 5$, on a

$$D^4 t - t + t^5 = 0 .$$

Un calcul tout bête montre que, si on pose

$$v = 1 - t^4 + t^2 Dt + 2(Dt)^2 + tD^2 t + D^3 t ,$$

on a

$$Dv = tv .$$

Comme $v \in 1 + m$, notre assertion est démontrée.

5. Exemples polynomiaux de descente p-radicielle.

a. La surface $Z^p = XY$. - On prend pour A l'anneau de polynômes $A = k[x , y]$ sur un corps k de caractéristique p et pour D la k-dérivation définie par $Dx = x$, $Dy = - y$. On a $D(xy) = 0$, et, plus généralement,

$$D(x^a y^b) = (a - b) x^a y^b .$$

Les polynômes t tels que $Dt = 0$ sont donc ceux où ne figurent que des monômes $x^a y^b$ tels que $a \equiv b \pmod p$; il s'ensuit que $A' = k[x^p , y^p , xy]$; posant $X = x^p$, $Y = y^p$, $Z = xy$, on a $Z^p = XY$ (noter que cette surface est normale).

Soit u un polynôme. Les monômes qui figurent dans Du sont parmi ceux qui figurent dans u . Donc $d^0(Du) \leqslant d^0(u)$, de sorte que, si $Du/u \in A$, alors $Du/u \in k$. La formule $D(x^a y^b) = (a - b) x^a y^b$ montre qu'alors Du/u est de la forme $(a - b).1$, c'est-à-dire est un élément du corps premier $\underset{\sim}{F}_p$; elle montre aussi que tout élément de $\underset{\sim}{F}_p$ est une dérivée logarithmique. On a donc $\underset{\sim}{D} = \underset{\sim}{F}_p$. Comme les unités de A sont des constantes, on a $\underset{\sim}{D}' = 0$. Donc $C(A')$ est un groupe cyclique d'ordre p .

On obtient le même résultat que dans l'exemple galoisien correspondant (§ 2, ex. 2).

b. La surface $Z^p = X^i + Y^j$. - On prend encore pour A l'anneau de polynômes $k[x , y]$ sur un corps k de caractéristique p , et pour D la k-dérivation du corps des fractions K de A définie par $Dx = jy^{j-1}$ et $Dy = - ix^{i-1}$,

i et j étant des entiers positifs étrangers à p . Les élémetns $X = x^p$, $Y = y^p$ et $Z = x^i + y^j$ sont dans le noyau K' de D . Comme $[K:k(x^p , y^p)] = p^2$ et que $x^i + y^j \notin k(x^p , y^p)$, on a $[K:K'] = p$, de sorte que le § 3 est applicable et qu'on a $D^p = aD$ avec $a \in K'$ (§ 4, lemme 1). On a $X^i + Y^j - Z^p = 0$; comme ceci est l'équation d'une surface normale, l'anneau $k[X , Y , Z]$ est intégralement clos ; comme son corps des fractions est K' , cet anneau est $A' = K \cap A$; autrement dit, on a $A' = k[x^p , y^p , x^i + y^j]$.

Munissons x du poids j et y du poids i . Alors on voit que, si F est un polynôme isobare de poids q , DF est un polynôme isobare de poids $q + (ij - i - j)$; donc $D^{p-1}(F)$ et $D^p(F)$ sont isobares de poids respectifs $q + (p - 1)(ij - i - j)$ et $q + p(ij - i - j)$. Appliquant la formule $D^p F = a.DF$ à un polynôme isobare F tel que $DF = 0$ (par exemple $F = x$), on voit que l'élément a est isobare de poids $(p - 1)(ij - i - j)$. Donc, si F est isobare de poids q , $D^{p-1} F - aF$ est isobare de poids $q + (p - 1)(ij - i - j)$.

Considérons alors "l'équation des dérivées logarithmiques" (§ 4, lemme 2)

$$D^{p-1} F - aF = - F^p . \tag{1}$$

Décomposons F en composantes isobares non nulles ; appelons q (resp. q') le plus petit (resp. plus grand) de leurs poids. Les poids des composantes du second membre $- F^p$ s'échelonnent entre pq et pq' , effectivement atteints. Les poids des composantes du premier membre $D^{p-1} F - aF$ sont compris entre $q + (p - 1)(ij - i - j)$ et $q' + (p - 1)(ij - i - j)$ (les bornes pouvant n'être pas atteintes, à cause de composantes nulles). On a donc

$$q + (p - 1)(ij - i - j) \leqslant pq \quad \text{et} \quad q' + (p - 1)(ij - i - j) \geqslant pq'$$

(inégalités de sens inverses). Ces inégalités équivalent à $ij - i - j \leqslant q$ et $q' \leqslant ij - i - j$. Comme $q \leqslant q'$, une dérivée logarithmique F est nécessairement isobare de poids $q = q' = ij - i - j$.

Soit d le p. g. c. d. de i et j ; posons $i = dr$, $j = ds$ (où r et s sont étrangers). Un polynôme F isobare de poids $ij - i - j$ est combinaison linéaire de monômes $x^u y^v$ tels que $ju + iv = ij - i - j$, c'est-à-dire tels que $su + rv = drs - r - s$. On a $su \equiv - s \pmod r$, d'où $u \equiv - 1 \pmod r$. La plus petite valeur de u est donc $r - 1$ (correspondant à $v = (d - 1)s - 1$) ; de même la plus petite valeur de v est $s - 1$, correspondant à la plus grande

valeur $(d-1)r-1 = r-1+(d-2)r$ de u. Donc une dérivée logarithmique F est nécessairement de la forme

$$(2) \qquad F = \sum_{n=0}^{d-2} b_n x^{r-1+nr} y^{s-1+(d-2-n)s} \qquad (d-1 \text{ termes}).$$

On voit déjà que, si $d = 1$ (c'est-à-dire si i et j sont étrangers), alors F est nul, d'où $\underset{\sim}{D} = 0$. L'anneau $A' = k[X, Y, Z]$, où $Z^p = X^i + Y^j$, est donc factoriel lorsque i et j sont étrangers et étrangers à p.

On retrouve un cas particulier d'un résultat général de factorialité démontré dans [7] (et disant que l'équation $Z^n = X^i + Y^j$ donne un anneau factoriel lorsque n, i, j sont étrangers deux à deux.

Reste à déterminer les coefficients b_n. Les coefficients des monômes de F^p sont les b_n^p. Le coefficient correspondant de $aF - D^{p-1}F$ est une forme linéaire $L_n(b)$ en $b_0, \ldots, b_{d-2}$ (les coefficients de L_n sont dans le corps premier, comme ceux de D). Donc, tenant compte de (2), (1) implique le système d'équations

$$(3) \qquad b_n^p = L_n(b) \qquad (n = 0, 1, \ldots, d-2).$$

Or les équations (3), rendues homogènes, n'ont pas de solution à l'infini ; l'ensemble de leurs solutions est donc de dimension 0 ; d'après le théorème de Bezout, elles ont donc au plus p^{d-1} solutions dans une clôture algébrique de k. Comme $\underset{\sim}{D}$ est un sous-groupe additif de A, il a donc p^f éléments avec $f \leqslant d-1$. Les unités de A étant les constantes, on a $\underset{\sim}{D}' = 0$. D'où :

PROPOSITION 1. - Soient k un corps de caractéristique p, i et j deux entiers étrangers à p et d leur p. g. c. d. Le groupe $C(A')$ des classes de diviseurs de l'anneau $A' = k[X, Y, Z]$ où $Z^p = X^i + Y^j$ est un groupe fini de type $(p, p, \ldots, p)$, d'ordre p^f avec $f \leqslant d-1$. En particulier A' est factoriel si i et j sont étrangers.

Remarque. - Lorsque k est algébriquement clos, il est à présumer que $C(A')$ est exactement d'ordre p^{d-1}. Nous allons voir que c'est vrai si $p = 2$. Pour $p = 3$, c'est confirmé par les deux exemples :

1. $Z^3 = X^2 + Y^4$. On a $Dx = y^3$, $Dy = x$, $d = 2$, $r = 1$, $s = 2$, et $D^3 = 0$. Une dérivée logarithmique F est nécessairement de la forme by $(b \in k)$.

L'équation $D^2 F + F^3 = 0$ équivaut alors à $b + b^3 = 0$; les solutions de cette équation forment un groupe à trois éléments contenu dans $\underset{\sim}{F}_9$. L'anneau correspondant A' est factoriel si $k = \underset{\sim}{F}_3$, non-factoriel (avec $C(A')$ d'ordre 3) si $k \supset \underset{\sim}{F}_9$.

2. $Z^3 = X^4 + Y^8$. On a $Dx = y^7$, $Dy = x^3$, $D^3 = 0$, $d = 4$, $r = 1$, $s = 2$. Une dérivée logarithmique F est nécessairement de la forme $F = b_0 y^5 + b_1 xy^3 + b_2 x^2 y$. Un petit calcul montre que l'équation $D^2 F + F^3 = 0$ équivaut au système

$$b_2^3 = b_0 \ , \quad b_0^3 = b_2 \ , \quad b_1^3 + b_1 = 0 \ .$$

Les deux premières égalités donnent l'équation $b_0^9 = b_0$, dont les solutions forment le corps $\underset{\sim}{F}_9$; à chaque valeur de b_0 correspond une valeur de b_2 admissible ; d'autre part l'équation $b_1^3 + b_1 = 0$ a trois solutions (dans $\underset{\sim}{F}_9$). Donc, si k contient $\underset{\sim}{F}_9$, $C(A')$ est un groupe de type $(3 , 3 , 3)$, d'ordre $27 = 3^{d-1}$.

c. Compléments sur $Z^2 = X^i + Y^j$ en caractéristique 2 . — Nous gardons les notations précédentes. Les exposants i , j sont ici impairs, donc aussi d , r et s . Dans (2), il y a donc un nombre pair $2c$ de termes $(d = 2c + 1)$. L'équation (1) s'écrit ici $DF = F^2$ (car $D^2 = 0$). Considérons le terme

$$b_n x^{r-1+nr} y^{s-1+(d-2-n)s}$$

de F (cf. (2)). Si n est pair, le terme correspondant de DF est

$$b_n x^{r-1+nr+dr-1} y^{s-2+(d-2-n)s} \ ;$$

il doit être égal à un terme

$$b_m^2 x^{2(r-1)+2mr} y^{2(s-1)+2(d-2-m)s}$$

de F^2 , ce qui équivaut à

$$1 + 2m = n + d \quad \text{et} \quad b_m^2 = b_n \ ;$$

ceci équivaut à

$$b_m^2 = b_{2m+d+1} = b_{2(m-c)} \ ;$$

vu que m et n varient de 0 à $d-2 = 2c-1$, cette équation doit avoir lieu pour $m = c, c+1, \ldots, 2c-1$. Pour n impair on obtient de même la condition $b_m^2 = b_n$ avec $n = 2m+1$; d'où les équations $b_m^2 = b_{2m+1}$ pour $m = 0, 1, \ldots, c-1$.

Soit alors h la permutation de $(0, 1, \ldots, 2c-1)$ définie par

$$h(m) = 2m+1 \quad \text{pour} \quad m = 0, \ldots, c-1, \tag{4}$$
$$h(m) = 2(m-c) \quad \text{pour} \quad m = c, c+1, \ldots, 2c-1.$$

Pour F de la forme (2), l'équation $DF = F^2$ équivaut au système de $2c$ équations

$$b_m^2 = b_{h(m)} \qquad (m = 0, 1, \ldots, 2c-1). \tag{5}$$

Soient $U_1, \ldots, U_q$ les orbites du groupe engendré par h, $u(1), \ldots, u(q)$ leurs cardinaux respectifs ; on a $u(1) + \ldots + u(q) = 2c$. Celles des équations (5) où m (et $h(m)$) parcourent une orbite U_f équivalent à l'équation $b^{2^{u(f)}} = b$; les solutions de celle-ci sont les éléments de $k \cap \underset{\sim}{F}(2^{u(f)})$ (corps fini à $2^{u(f)}$ éléments). Nous voyons donc que le groupe $\underset{\sim}{D}$ des dérivées logarithmiques (donc $C(A')$) est isomorphe à

$$\prod_{f=1}^{q} (k \cap \underset{\sim}{F}(2^{u(f)})) \ . \tag{6}$$

PROPOSITION 2. - Soient k un corps de caractéristique 2, i et j deux entiers impairs, d leur p. g. c. d., A' l'anneau $k[X, Y, Z]$ où $Z^2 = X^i + Y^j$. Le groupe $C(A')$ des classes de diviseurs de A' est un groupe de type $(2, \ldots, 2)$, et d'ordre 2^v avec $v \leqslant d-1$. Si k contient la clôture algébrique de son corps premier, l'ordre de $C(A')$ est 2^{d-1}.

Remarques.

1. Lorsque k ne contient pas la clôture algébrique de son corps premier, la détermination de l'ordre de $C(A')$ demande qu'on connaisse la décomposition de $(0 , 1 , \dots , 2c-1)$ en orbites, c'est-à-dire le système $(u(1) , \dots , u(q))$. La table suivante donne ces systèmes pour $c = 1 , 2 , \dots , 13$; la loi de formation me paraît encore mystérieuse.

Valeurs de c	Système des cardinaux des orbites
1	(2)
2	(4)
3	(3 , 3)
4	(6 , 2)
5	(10)
6	(12)
7	(4 , 4 , 4 , 2)
8	(8 , 8)
9	(18)
10	(6 , 6 , 3 , 3 , 2)
11	(11 , 11)
12	(20 , 4)
13	(18 , 6 , 2) .

Il est facile de voir que, pour tout c , h n'admet pas de point fixe. Si $k = \underset{\sim}{F}_2$, l'ordre de $C(A')$ est $2^{(\text{nombre d'orbites})}$.

2. Les trois exemples de ce paragraphe sont "définis sur le corps premier $\underset{\sim}{F}_p$". Les calculs restent donc valables si on suppose seulement que k est un anneau factoriel de caractéristique p.

6. Exemples "formels" de descente p-radicielle.

a. La surface $Z^p = XY$ $(p = 2 , 3 , 5)$. - Nous prenons ici $A = k[[x , y]]$ et pour D la k-dérivation définie par $Dx = x$, $D_y = -y$. Comme au § 5, on a $A' = k[[x^p , y^p , xy]]$ et $D^p = D$. L'idéal engendré par Dx et Dy est l'idéal maximal m de A. D'après le lemme 4 du § 4, on a $\underset{\sim}{D}' = \underset{\sim}{D} \cap m$. Donc $\underset{\sim}{D}/\underset{\sim}{D}'$ est isomorphe au groupe additif des termes constants des dérivées logarithmiques. Or la formule $D(x^a y^b) = (a - b)x^a y^b$ montre que ce groupe est le corps

premier $\underset{\sim}{F}_p$. Ainsi $C(A')$ est cyclique d'ordre p , comme dans l'exemple polynomial correspondant.

b. La surface $Z^2 = X^{2i+1} + Y^{2j+1}$ en caractéristique 2 . - Soient k un corps de caractéristique 2 , A l'anneau de séries formelles $A = k[[x , y]]$ et D la k-dérivation définie par $Dx = y^{2j}$, $Dy = x^{2i}$. Comme dans le cas polynomial, on a

$$A' = k[[X , Y , Z]] \quad \text{avec} \quad X = x^2 , \quad Y = y^2 , \quad Z = x^{2i+1} + y^{2j+1}$$

$$\text{et} \quad Z^2 = X^{2i+1} + Y^{2j+1} .$$

(N. B. - Les entiers appelés i et j dans le cas polynomial s'appellent ici $2i + 1$ et $2j + 1$.)

On a $D^2 = 0$, de sorte que l'équation aux dérivées logarithmiques est

$$DF = F^2 . \tag{1}$$

Munissons x du poids $2j + 1$ et y du poids $2i + 1$. On constate que, si F_n est isobare de poids n , DF_n est isobare de poids $n + 4ij - 1$. Décomposons chaque série F en somme (infinie) de composantes isobares, $F = F_q + F_{q+1} + \dots$, et appelons ordre de F le poids de sa plus basse composante non nulle ; notation $o(F)$. Nous noterons $\underset{\sim}{D}_q$ le sous-groupe de $\underset{\sim}{D}$ formé des dérivées logarithmiques d'ordre $\geqslant q$; ainsi $(\underset{\sim}{D}_q)$ est une filtration de $\underset{\sim}{D}$; nous munissons $\underset{\sim}{D}'$ de la filtration induite $(\underset{\sim}{D}'_q) = (\underset{\sim}{D}_q \cap \underset{\sim}{D}')$, et le groupe quotient $\underset{\sim}{D}/\underset{\sim}{D}'$, que nous notons $\underset{\sim}{C}$, de la filtration quotient $(\underset{\sim}{C}_q)$; on a

$$\underset{\sim}{C}_q = (\underset{\sim}{D}' + \underset{\sim}{D}_q)/\underset{\sim}{D}' = \underset{\sim}{D}_q/\underset{\sim}{D}'_q .$$

Pour nous rassurer remarquons tout de suite que le lemme 3 du § 4 montre qu'on a $\underset{\sim}{D}_q = \underset{\sim}{D}'_q$ pour q assez grand, et donc $\underset{\sim}{C}_q = 0$. Nous allons déterminer les quotients successifs $\underset{\sim}{C}_q/\underset{\sim}{C}_{q+1}$. Comme $\underset{\sim}{D}$, ce sont des espaces vectoriels sur $\underset{\sim}{F}_2$; donc le problème d'extension des uns par les autres est trivial, de sorte que $\underset{\sim}{C}$ est isomorphe au groupe gradué associé $\sum_q \underset{\sim}{C}_q/\underset{\sim}{C}_{q+1}$.

Soit F une dérivée logarithmique non nulle. On a $o(F^2) = 2o(F)$ et $o(DF) \geqslant o(F) + 4ij - 1$, d'où $o(F) \geqslant 4ij - 1$ (par (1)). Si $o(F) = 4ij - 1$, et si G est la composante de poids $4ij - 1$ de F , on a $DG = G^2$, de sorte que G

est une dérivée logarithmique dont la forme a été déterminée dans le cas polynomial (cf. § 5, proposition 2). Celles-ci forment un sous-groupe fini $\underset{\sim}{E}$ de $\underset{\sim}{D}$, supplémentaire de $\underset{\sim}{D}_{4ij}$. D'autre part, on a $\underset{\sim}{D}' \subset \underset{\sim}{D}_{4ij}$; en effet, si H est une dérivée logarithmique d'unité, on a

$$H \in (Dx , Dy) = (y^{2j} , x^{2i}) ,$$

de sorte que, pour tout monôme $x^a y^b$ figurant dans H, on a $a \geqslant 2i$ ou $b \geqslant 2j$; dans tous les cas le poids $a(2j + 1) + b(2i + 1)$ d'un tel monôme est $\geqslant 4ij$. On pourra donc mettre de côté le facteur direct $\underset{\sim}{E}$ (facteur direct de $\underset{\sim}{D}$, et aussi de $\underset{\sim}{C} = \underset{\sim}{D}/\underset{\sim}{D}'$), et n'étudier $\underset{\sim}{D}_q$, D'_q et $\underset{\sim}{C}_q$ que pour $q \geqslant 4ij$.

Soit donc $q \geqslant 4ij$. Notons A_q l'ensemble des polynômes isobares de poids q. Soit φ l'homomorphisme de $\underset{\sim}{D}_q$ dans A_q qui, à toute

$$F = F_q + \dots + F_n + \dots \in \underset{\sim}{D}_q$$

fait correspondre sa composante F_q de poids q. Le noyau de φ est $\underset{\sim}{D}_{q+1}$. Pour $F \in \underset{\sim}{D}_q$ l'ordre de F^2 est $\geqslant 2q$, tandis que, si DF_q est non nul, il est d'ordre $q + 4ij - 1 < 2q$ (car $q \geqslant 4ij$) ; c'est impossible puisque $F^2 = DF$, de sorte qu'on a $DF_q = 0$. Ainsi l'image de φ est contenue dans $A' \cap A_q$. Donc $\varphi(\underset{\sim}{D}'_q) \subset \mathfrak{v} \cap A' \cap A_q$, où $\mathfrak{v}$ est l'idéal $(Dx , Dy) = (x^{2i} , y^{2i})$. Nous allons montrer qu'il y a surjectivité, plus précisément qu'on a les égalités

$$(2) \qquad \varphi(\underset{\sim}{D}_q) = A' \cap A_q , \qquad \varphi(\underset{\sim}{D}'_q) = \mathfrak{v} \cap A' \cap A_q .$$

En effet donnons-nous F_q dans $A' \cap A_q$ (resp. dans $\mathfrak{v} \cap A' \cap A_q$). Il s'agit de déterminer des polynômes isobares F_n $(n \geqslant q)$ (resp. des polynômes isobares F_n contenus dans l'idéal $\mathfrak{v} = (Dx , Dy)$; cf. lemme 3 du § 2) tels que, si on pose

$$F = F_q + \dots + F_n + \dots ,$$

on ait

$$DF = F^2 .$$

Comparant les composantes isobares, ceci s'écrit $F_n^2 = DF_{2n+1-4ij}$; comme $n \geqslant 4ij$, on a $2n + 1 - 4ij > n$, de sorte que chaque F_m devra âtre déterminé par "intégration" à partir d'un F_s^2 pour $s < n$; remarquons que, si m est pair, ou d'indice trop petit (i. e. $\frac{1}{2}(m + 4ij - 1) < q$), la condition sur F_m s'écrit $DF_m = 0$. En tous cas on a à déterminer un polynôme isobare F_m de poids m par une condition de la forme $DF_m = G^2$ où G est un polynôme isobare donné de poids $\geqslant q$. Par additivité de la dérivation et de l'élévation au carré, nous sommes ramenés au cas d'un monôme $G = x^a y^b$. Alors, si $2a \geqslant 2i$, on peut prendre

$$F_m = x^{2a-2i} y^{2b+1} \quad ;$$

si $2b \geqslant 2j$, on peut prendre

$$F_m = x^{2a+1} y^{2b-2j} \quad ;$$

on est dans au moins un de ces deux cas, car, sinon on aurait $a < i$, $b < j$, et G serait de poids $(2j + 1)a + (2i + 1)b < 4ij$, ce qui est impossible. De plus, si on suppose par récurrence qu'on a $G \in \mathfrak{p}$, on a $a \geqslant 2i$ ou $b \geqslant 2j$, d'où $2a - 2i \geqslant 2i$ ou $2b - 2j \geqslant 2j$, de sorte que F_m peut être pris dans $\mathfrak{p}$. Ceci démontre (2).

Il résulte de (2) qu'on a un isomorphisme canonique de $\underset{\sim}{C}_q/\underset{\sim}{C}_{q+1}$ sur $(A' \cap A_q)/(\mathfrak{p} \cap A' \cap A_q)$. Donc $\underset{\sim}{C}_q/\underset{\sim}{C}_{q+1}$ a une structure de k-espace vectoriel de dimension finie ; soit $n(q)$ celle-ci. Le facteur direct $\underset{\sim}{C}_{4ij}$ de $\underset{\sim}{C}(= C(A'))$ est ainsi un k-espace vectoriel de dimension finie

$$N(i , j) = \sum_{q \geqslant 4ij} n(q) \ .$$

Calculons finalement l'entier $N(i , j)$. Dans A , l'idéal $\mathfrak{p}$ admet un supplémentaire engendré par les monômes $x^a y^b$ tels que $a < 2i$ et $b < 2j$. Comme $x^{2i+1} + y^{2j+1} \in \mathfrak{p}$, un supplémentaire de $\mathfrak{p} \cap A'$ dans $A' = k[x^2 , y^2 , x^{2i+1} + y^{2j+1}]$ est engendré par les monômes $x^{2a} y^{2b}$ tels que $2a < 2i$ et $2b < 2j$. Ainsi $N(i , j)$ est égal au nombre de ceux de ces monômes qui sont de poids $\geqslant 4ij$. On a donc :

PROPOSITION 3. - Soient k un corps de caractéristique 2, i et j deux entiers, d le p. g. c. d. de $2i+1$ et $2j+1$, et A' l'anneau $k[[X, Y, Z]]$ où $Z^2 = X^{2i+1} + Y^{2j+1}$. Alors le groupe $C(A')$ des classes de diviseurs de A' est somme directe :

a. d'un groupe de type $(2, 2, \ldots, 2)$ et d'ordre 2^v où $v \leqslant d-1$; si k contient la clôture algébrique du corps premier F_2, cet ordre est 2^{d-1} ;

b. d'un espace vectoriel sur k, dont le dimension $N(i, j)$ est égale au nombre des couples d'entiers (a, b) tels que $0 \leqslant a < i$, $0 \leqslant b < j$, et $(2j+1)a + (2i+1)b \geqslant 2ij$.

Remarques.

1. L'entier $N(i, j)$ n'est égal à 0 que si, pour le "plus grand" couple $(a, b) = (i-1, j-1)$, l'inégalité $(2j+1)a + (2i+1)b \geqslant 2ij$ n'est pas satisfaite. Excluant les cas banaux où $i = 0$ ou $j = 0$, il reste les couples $(i, j) = (1, 1)$, $(1, 2)$ et $(2, 1)$; alors $(2i+1, 2j+1) = (3, 3)$, $(3, 5)$ et $(5, 3)$. Donc, à une permutation près, la seule équation donnant un anneau factoriel est $Z^2 = X^3 + Y^5$. Pour tous les autres couples $(2i+1, 2j+1)$ d'entiers impairs étrangers, les propositions 2 et 3 donnent des exemples d'anneaux factoriels dont les complétés ne sont pas factoriels.

2. Pour le plus grand couple $(a, b) = (i-1, j-1)$, le poids $(2j+1)a + (2i+1)b$ est égal à $4ij - i - j - 2$, nombre voisin du double de $2ij$. Donc environ la moitié des points (a, b) du rectangle $0 \leqslant a \leqslant i$, $0 \leqslant b \leqslant j$ vérifient l'inégalité $(2j+1)a + (2i+1)b \geqslant 2ij$. Ainsi, pour i et j grands, $N(i, j)$ est équivalent à $\frac{1}{2} ij$.

3. Désignons par $E(t)$ la partie entière du nombre réel t. En classifiant les couples (a, b) suivant la valeur de a, on voit sans difficulté que

$$N(i, j) = E\left(\frac{j}{2i+1}\right) + E\left(\frac{3j+1}{2i+1}\right) + \ldots + E\left(\frac{j + (i-1)(2j+1)}{2i+1}\right).$$

En particulier on a

$$N(1, j) = E\left(\frac{j}{3}\right), \quad N(2, j) = E\left(\frac{j}{5}\right) + E\left(\frac{3j+1}{5}\right), \text{ etc.}$$

c. Anneaux de séries formelles. - Soient k un corps de caractéristique 2, A l'anneau $k[x, y]$ (ou $k[[x, y]]$), R l'anneau de séries formelles $A[[T]]$, et D la k-dérivation de R définie par $Dx = y^{2j}$, $Dy = x^{2i}$ et $DT = 0$. Notons $\underset{\sim}{D}(A)$ le groupe des éléments de A qui sont des dérivées logarithmiques, et $\underset{\sim}{D}'(A)$ celui des dérivées logarithmiques d'unités ; idem pour $\underset{\sim}{D}(R)$ et $\underset{\sim}{D}'(R)$. Si A' est le noyau de la restriction de D à A, le noyau R' de D est $A'[[T]]$; rappelons que A' est défini par l'équation $Z^2 = X^{2i+1} + Y^{2j+1}$. On a $D^2 = 0$.

Pour qu'une série

$$\sum_{n\geqslant 0} a_n T^n \qquad (a_n \in A)$$

soit dans $\underset{\sim}{D}(R)$, il faut et il suffit qu'on ait

$$\sum_{n\geqslant 0} (Da_n) T^n = \sum_{n\geqslant 0} a_n^2 T^{2n} ,$$

ce qui se traduit par

$$Da_0 = a_0^2 \; ; \quad Da_{2n+1} = 0 , \quad Da_{2n} = a_n^2 . \tag{3}$$

La première égalité veut dire que $a_0 \in \underset{\sim}{D}(A)$. Ainsi $\underset{\sim}{D}(R)$ est somme directe de $\underset{\sim}{D}(A)$ et du sous-groupe $\underset{\sim}{D}_1(R)$ formé des séries formelles de $\underset{\sim}{D}(R)$ sans terme constant.

Une unité de R est une série dont le terme constant est une unité de A. Donc, si

$$\sum_{n\geqslant 0} a_n T^n \in \underset{\sim}{D}'(R) ,$$

on a

$$a_0 \in \underset{\sim}{D}'(A) .$$

Ainsi $\underset{\sim}{D}'(R)$ est somme directe de $\underset{\sim}{D}'(A)$ et du sous-groupe $\underset{\sim}{D}'_1(R)$ de $\underset{\sim}{D}'(R)$ formé des séries sans terme constant. Soit $\mathfrak{B}$ (resp. $\mathfrak{b}$) l'idéal de R (resp. A) engendré par Dx et Dy. On a

(4) $$\underset{\sim}{D}_1'(R) = \underset{\sim}{D}_1(R) \cap \mathfrak{D} \ .$$

En effet, si t est un élément du second membre, on lui applique le calcul du lemme 3 du § 3 : on a $t = rDx + sDy$, où r et s sont multiples de T ; l'élément b défini par $Dr = r^2 Dx + bDy$ est aussi multiple de T ; alors l'élément $u = 1 + rx + sy + (rs + b)\,xy$ tel que $Du = tu$ appartient à $1 + RT$ et est donc inversible.

Soit alors $\sum_{n \geqslant 1} a_n T^n$ un élément de $\underset{\sim}{D}_1(R)$. Munissons encore x du poids $2j + 1$ et y du poids $2i + 1$. Notons $q(n)$ le poids de la composante isobare non nulle de plus petit poids de a_n. Comme D élève les poids de $q = 4ij - 1$ unités, (3) montre qu'on a

$$q(2n) + q \leqslant 2q(n) \ ,$$

ce qui s'écrit

$$q(2n) - q \leqslant 2(q(n) - q) \ ;$$

on a donc

$$q(2^r n) \leqslant 2^r(q(n) - q) + q \ .$$

Comme $q(2^r n) \geqslant 0$, on doit avoir $q(n) \geqslant q = 4ij - 1$. Comme dans l'exemple précédent, on en déduit que la détermination de a_{2n} à partir de a_n au moyen de $Da_{2n} = a_n^2$ est possible, et que l'élément a_{2n} ainsi déterminé vérifie $q(2n) \geqslant q$. Notons encore A_q l'ensemble des éléments de A de poids $\geqslant q$. A chaque intégration s'introduit une "constante arbitraire", élément de $A_q \cap A'$; de sorte que $\underset{\sim}{D}_1(R)$ est isomorphe au produit d'une suite dénombrable de copies de $A_q \cap A'$. D'après (4), $\underset{\sim}{D}_1(R)/\underset{\sim}{D}_1'(R)$ est isomorphe au produit d'une suite dénombrable de copies de $(A_q \cap A')/(A_q \cap A' \cap \mathfrak{D})$. Ce quotient est un k-espace vectoriel dont la dimension est, comme dans l'exemple précédent, le nombre de couples $(a\ ,\ b)$ d'entiers tels que

$$0 \leqslant a < i \ , \quad 0 \leqslant b < j \ , \quad (2j + 1)2a + (2i + 1)2b \geqslant q = 4ij - 1 \ ;$$

cette dernière égalité équivaut à $(2j + 1)a + (2i + 1)b \geqslant 2ij$, de sorte que

ladite dimension est l'entier $N(i , j)$ de l'exemple précédent. D'où :

PROPOSITION 4. - Soient k un corps de caractéristique 2, i et j deux entiers, et A' l'anneau $k[X , Y , Z]$ (resp. $k[[X , Y , Z]]$) où $Z^2 = X^{2i+1} + Y^{2j+1}$. Alors le groupe $C(A'[[T]])$ est isomorphe à la somme directe de $C(A')$ (déterminé aux propositions 2 et 3), et du groupe $(k[[T]])^{N(i , j)}$ où l'entier $N(i , j)$ est celui défini dans la proposition 3.

Remarques.

1. Lorsque $A' = k[X , Y , Z]$, que $2i + 1$ et $2j + 1$ sont étrangers, et que $N(i , j) > 0$ (ce qui exclut seulement les couples d'exposants (3 , 5) et (5 , 3)), les propositions 2 et 4 fournissent des exemples d'anneaux factoriels A' tels que l'anneau de séries formelles $A'[[T]]$ ne soit pas factoriel. Voir [6] pour une autre méthode. Par contre, si A' est le seul anneau factoriel complet fourni par la proposition 3 (correspondant à l'équation $Z^2 = X^3 + Y^5$), on a $N(i , j) = 0$, et l'anneau de séries formelles $A'[[T]]$ est factoriel. Ceci laisse subsister la conjecture que, sur un anneau local factoriel et complet, l'anneau de séries formelles est factoriel.

2. Intervertissons les adjonctions "polynômes" et "séries formelles", et considérons $B' = k[[T]][X , Y , Z]$ où $Z^2 = X^{2i+1} + Y^{2j+1}$. La remarque (2) suivant la proposition 2 (§ 5) montre que $C(B')$ est un groupe fini de type $(2 , 2 , \ldots , 2)$, nul lorsque $2i + 1$ et $2j + 1$ sont étrangers. Donc, contrairement à $k[X , Y , Z][[T]]$, B' est souvent factoriel.

3. Soient A un anneau de caractéristique $p \neq 0$, D une dérivation de A ; prolongeons D à l'anneau de polynômes $A[T]$ au moyen de $DT = 0$. Raisonnant sur les degrés dans l'équation aux dérivées logarithmiques $D^{p-1} F - aF + F^p = 0$, on voit que les dérivées logarithmiques sont de degré 0 ; donc $\underset{\sim}{D}(A[T]) = \underset{\sim}{D}(A)$. Il est clair que $\underset{\sim}{D}'(A[T]) = \underset{\sim}{D}'(A)$. D'où, par descente radicielle à un anneau A', l'égalité $C(A'[T]) = C(A')$ (d'ailleurs vraie pour un anneau de Krull quelconque ; cf. § 1).

d. Un problème de Grothendieck. - A. GROTHENDIECK m'a posé la question suivante : soient A un anneau local noethérien factoriel, m son idéal maximal, $B = A[[T]]$ et $p = mB$; alors B_p est-il factoriel ? La proposition suivante, jointe aux exemples d'anneaux de séries formelles non factoriels fournis par la proposition 4, montre que la réponse est négative :

PROPOSITION 5. - Soient R un anneau local régulier de caractéristique 2, D une dérivation de R, et A son noyau. On suppose qu'on a $[R:A] = 2$, qu'il existe deux éléments x, y de $m(R)$ tel que l'idéal $q = R.DR$ soit engendré par Dx et Dy, et que R/q est complet (par exemple que q est ouvert). Posons $S = R[[T]]$, $B = A[[T]]$, $p = m(A).B$ et $\mathfrak{P} = m(R)S$. Alors l'homomorphisme canonique $C(B) \to C(B_p)$ est bijectif.

La surjectivité étant un fait général, il suffit de démontrer l'injectivité. Avec les notations habituelles, on a

$$C(B) = \underset{\sim}{D}(S)/\underset{\sim}{D}'(S) \quad \text{et} \quad C(B_p) = \underset{\sim}{D}(S_{\mathfrak{P}})/\underset{\sim}{D}'(S_{\mathfrak{P}})$$

car S est régulier donc factoriel (théorème 2 du § 3). D'après le lemme 3 du § 4 on a de même $\underset{\sim}{D}'(S) = \underset{\sim}{D}(S) \cap qS$ et $\underset{\sim}{D}'(S_{\mathfrak{P}}) = D(S_{\mathfrak{P}}) \cap qS_{\mathfrak{P}}$. Donc l'injectivité veut dire que, si un élément u de $\underset{\sim}{D}(S)$ appartient à $\underset{\sim}{D}'(S_{\mathfrak{P}})$, alors il appartient à $\underset{\sim}{D}'(S)$; autrement dit il s'agit de montrer qu'on a

$$\underset{\sim}{D}(S) \cap qS_{\mathfrak{P}} = \underset{\sim}{D}(S) \cap qS \text{, ou encore } S \cap qS_{\mathfrak{P}} = qS \text{.} \tag{5}$$

Or soit u un élément de $S \cap qS_{\mathfrak{P}}$. Il existe un élément w de $S - \mathfrak{P}$, c'est-à-dire une série formelle sur R dont au moins un coefficient est inversible, tel que $uw \in qS$. Notant u' et w' les séries obtenues à partir de u et w par réduction des coefficients modulo q, on obtient $u'w' = 0$. Comme R/q est complet, le théorème de préparation de Weierstrass montre que w' est associé à un polynôme distingué p' ; on a donc $u'p' = 0$. Comme un polynôme distingué n'est pas diviseur de zéro dans un anneau de séries formelles (voir lemme ci-dessous), on a $u' = 0$, d'où $u \in qS$.

C. Q. F. D.

Reste à rappeler la démonstration du lemme connu suivant :

LEMME. - Soient K un anneau local noethérien, m son idéal maximal,

$$m = m_0 + m_1 T + \dots + m_s T^s + T^{s+1} \qquad (m_i \in m)$$

un polynôme distingué, et $a = a_0 + \dots + a_n T^n + \dots$ une série formelle sur K telle que $ma = 0$. Alors $a = 0$.

En effet, pour tout $j \geqslant s+1$, on a

$$a_j + a_{j+1} m_s + \cdots + a_{j+s+1} m_0 = 0 . \tag{6}$$

On a donc $a_j \in m$ pour tout $j \geqslant s+1$. De $a_i \in m^q$ pour tout $i \geqslant s+1$ et de (6) on déduit qu'on a $a_j \in m^{q+1}$ pour tout $j \geqslant s+1$; d'où, par récurrence, $a_j \in m^n$ pour tout $j \geqslant s+1$ et tout n. Comme

$$\bigcap_{n=0}^{\infty} m^n = (0) ,$$

on a

$$a_j = 0 \quad \text{pour tout} \quad j \geqslant s+1 .$$

Donc a est un polynôme. De $ma = 0$, on déduit alors $a = 0$ en raisonnant sur les termes de plus haut degré.

C. Q. F. D.

Problèmes ouverts.

a. La conjecture du § 3 : soient A un anneau intègre, D une dérivation, q l'idéal $A.DA$. Toute dérivée logarithmique qui se trouve dans q est-elle dérivée logarithmique d'une unité ?

b. Problème analogue : un élément de q qui est la dérivée d'un élément de K (corps des fractions de A) est-il aussi la dérivée d'un élément de A ?

La solution de (a) et (b) permettrait de donner un analogue de la proposition 3 (§ 6) pour une caractéristique p quelconque.

c. A étant un anneau de polynômes ou de séries formelles sur un corps k, le groupe D/D' (dérivées logarithmiques dans A, modulo dérivées logarithmiques d'unités) est-il un groupe algébrique sur k ? La réponse est affirmative dans tous les exemples traités ici.

BIBLIOGRAPHIE

[1] BARSOTTI (Iacopo). - Repartitions on abelian varieties, Illinois J. of Math., t. 2, 1958, p. 43-70.

[2] BOURBAKI (Nicolas). - Algèbre commutative. Chap. 7 : Diviseurs. - Paris, Hermann, 1965 (Act. scient. et ind., 1314 ; Bourbaki, 31).

[3] 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).

[4] HOCHSCHILD (C.). - Simple algebras with purely inseparable splitting fields of exponent 1 , Trans. Amer. math. Soc., t. 79, 1955, p. 477-489.

[5] SAMUEL (Pierre). - Commutative algebra. - Ithaca (N. Y.), Cornell University, 1953 (Cours multigraphié).

[6] SAMUEL (Pierre). - Sur les anneaux factoriels, Bull. Soc. math. France, t. 89, 1961, p. 155-173.

[7] SAMUEL (Pierre). - Un exemple d'anneau factoriel, Bull. Soc. mat. Sao Paulo, t. 15, 1960, p. 1-4.

[8] SERRE (Jean-Pierre). - Corps locaux. - Paris, Hermann, 1962 (Act. scient. et ind., 1296 ; Publ. Inst. Math. Univ. Nancago, 8).

[9] ZARISKI (O.) and SAMUEL (P.). - Commutative algebra, Vol. 1 and 2. - Princeton, Toronto, London, D. Van Nostrand, 1958-1960.