MÉMOIRES DE LA S. M. F.

N. ZINN-JUSTIN

Dérivations dans les corps et anneaux de caractéristique p

Mémoires de la S. M. F., tome 10 (1967)

<http://www.numdam.org/item?id=MSMF_1967__10__3_0>

Bull. Soc. Math. France
Mémoire 10, 1967, 79 p.

DERIVATIONS DANS LES CORPS ET ANNEAUX DE CARACTERISTIQUE p

par Nicole ZINN-JUSTIN (1)

TABLE DES MATIERES

INTRODUCTION 5

PARTIE I

CHAPITRE I : Résultats relatifs à la théorie de la descente p-radicielle 7

A. - Quelques rappels 7
B. - Etude de quelques cas particuliers 8
C. - Généralisation du théorème 0 et interprétation par les groupes de cohomologie 11

CHAPITRE II : Application à l'étude de la factorialité de certains anneaux 14

A. - Lien avec la théorie de la descente p-radicielle 14
B. - Résolution dans l'anneau A de l'équation $F^2 = DF$ 17
C. - Conclusion 24

APPENDICE 29

PARTIE II

INTRODUCTION 36

CHAPITRE I : Préliminaires 38

A. - Rappels concernant la notion de p-base 38
B. - Quelques lemmes concernant les dérivations 40

(1) Thèse Sc. Math., Paris, 1967.

CHAPITRE II : Notion de bonnes dérivations 45

A. - Définition de bonnes dérivations 45
B. - Existence de bonnes dérivations 49
C. - Problème réciproque 54
D. - Problèmes d'extension de bonnes dérivations 55

CHAPITRE III : Etude détaillée d'une bonne dérivation 58

A. - Le corps K est de degré fini sur k 59
B. - Le corps K est de degré infini dénombrable sur k 61

CHAPITRE IV : Etude de toutes les dérivations de K de noyau k lorsque $[K : k]$ est fini 65

A. - Caractérisations des dérivations de K de noyau k 65
B. - Caractérisation des dérivées logarithmiques pour une dérivation de noyau k 70

BIBLIOGRAPHIE 79

INTRODUCTION

Le présent ouvrage comprend deux parties : la première est consacrée à l'étude des dérivations dans des anneaux de Krull et à l'application à la factorialité de certains anneaux tandis que la seconde concerne des dérivations de noyau k d'un corps K de caractéristique p non nulle, extension purement inséparable d'exposant 1 de k.

PARTIE I

La première partie est subdivisée en deux chapitres, suivis d'un appendice : au début du premier chapitre sont rappelés quelques résultats classiques concernant les anneaux de Krull et leurs classes de diviseurs ; soient A un anneau de Krull, A' un sous anneau de Krull de A, le groupe C(A) (respectivement C(A')) des diviseurs de A (resp. A') ; il existe alors un homomorphisme canonique $\bar{j}$ de C(A') dans C(A). Puis est énoncé un important théorème (théorème 0) relatif à la descente p-radicielle en caractéristique p non nulle affirmant l'existence d'un monomorphisme canonique $\bar{\Phi}$ de ker $\bar{j}$ dans $\mathfrak{D}/\mathfrak{D}$, ($\mathfrak{D}$ est le sous-groupe de A formé de dérivées logarithmiques d' unités de K ; $\mathfrak{D}'$ est le sous-groupe des dérivées logarithmiques d'unités). A propos de ce théorème, deux conjectures ont été faites :

(1) Soit $\mathcal{U}$ l'idéal A.DA. Toute dérivée logarithmique qui se trouve dans $\mathcal{U}$ est la dérivée logarithmique d'une unité.

(2) Un élément de $\mathcal{U}$ qui est la dérivée d'un élément de K est aussi la dérivée d'un élément de A.

Ces conjectures sont démontrées lorsque A est un anneau de séries formelles, la dérivation étant nulle sur le corps des coefficients ; lorsque A est un anneau local, son idéal maximal contenant $\mathcal{U}$ et la dérivation D^p étant proportionnelle à D ; enfin lorsque A est de valuation discrète, son idéal maximal contenant $\mathcal{U}$.

Le premier chapitre se termine par une interprétation du théorème 0 grâce aux groupes de cohomologie des groupes multiplicatifs des anneaux de nombres duaux construits à partir des corps considérés.

Le second chapitre est un exemple d'application de la théorie développée au premier chapitre : étant donnés un corps k de caractéristique 2, u une indéterminée sur k, soit l'anneau A' :

$$A' = k(u)\left[\!\left[x,y,z \right]\!\right]$$

où x, y, z sont liés par la relation $x^2 + y^i + uz^{2j} = 0$, i et j étant deux entiers impairs positifs. Pour quelles valeurs de i et j l'anneau A' est-il factoriel ? Nous verrons que la factorialité de A' est tout-à-fait exceptionnelle.

Pour résoudre ce problème, nous serons amenés à utiliser des raisonnements d'arithmétique ; en particulier apparaitra la permutation σ de $2s$ objets définie par :

$$\sigma(2\ell) = \ell$$
$$\sigma(2\ell-1) = \ell + s \qquad \ell = 1,\ldots,s$$

qui est déjà intervenue dans certaines études de descente p-radicielle [3]. Quelques propriétés de cette permutation seront dégagées dans l'appendice.

CHAPITRE I

RESULTATS RELATIFS A LA THEORIE DE LA DESCENTE P-RADICIELLE

A) Quelques rappels

Soit A un anneau intègre. La relation $(A : \mathfrak{B}) = (A : \mathfrak{B}')$ entre idéaux (entiers ou fractionnaires) $\mathfrak{B}$, $\mathfrak{B}'$ de A est une relation d'équivalence, dite "équivalence d'Artin". Les classes d'équivalence s'appellent les diviseurs de A. La multiplication des idéaux donne une multiplication des diviseurs ; muni de cette loi et de la relation correspondant à l'inclusion, l'ensemble des diviseurs de A est un monoïde ordonné, noté D (A). 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 (qui correspondent aux idéaux entiers de A) vérifient la condition minimale, l'anneau A est un anneau de Krull : par exemple, un anneau noethérien et intégralement clos est un anneau de Krull. Considérons alors un anneau A de Krull. Soit P (A) l'ensemble des idéaux premiers $\mathfrak{p}$ de hauteur 1 de A (c'est-à-dire que $\mathfrak{p} \neq (0)$ et ne contient pas d'autre idéal premier que lui-même et (0)). Nous avons alors les résultats suivants [1] :

- pour tout élément $\mathfrak{p}$ de (P (A), l'anneau de fractions $A_{\mathfrak{p}}$ est l'anneau d'une valuation discrète nommée .
- l'anneau A est l'intersection de ces $A_{\mathfrak{p}}$.
- tout diviseur δ de A s'écrit, et de façon unique, sous la forme :

$$\delta = \sum_{\mathfrak{p} \in P(A)} n(\mathfrak{p}) \cdot \mathfrak{p}$$

où les $n(\mathfrak{p})$ sont des entiers presque tous nuls.

Le diviseur correspondant à l'idéal principal Aa, que nous noterons (a) s 'écrit :

$$(a) = \sum_{\mathfrak{p} \in P(A)} v_{\mathfrak{p}}(a) \cdot \mathfrak{p}$$

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) soit nul. Soient maintenant A un anneau de Krull de caractéristique $p \neq o$, de corps des fractions K et D une dérivation de K telle que :

$$D(A) \subset A$$

Notons K' le noyau de K et A' l'anneau $K' \cap A$. Comme K^p (resp. A^p) est contenu dans K' (resp. A'), l'anneau A est entier sur A'. De plus, l'anneau A' est de Krull. Pour tout élément $\mathfrak{p}$ de P (A'), il existe un seul élément $\mathfrak{P}$ de P (A) tel que $\mathfrak{P} \cap A' = \mathfrak{p}$: c'est l'ensemble des x de A tels que x^p soit dans $\mathfrak{p}$ [2]. La

restriction de $v_{\mathfrak{P}}$ à K' est une valuation équivalente à $v_{\mathfrak{p}}$. Soit $e(\mathfrak{P},\mathfrak{p})$ l'indice de ramification correspondant au couple $(\mathfrak{P},\mathfrak{p})$. Faisons correspondre à $\mathfrak{p}$ le diviseur $j(\mathfrak{p})$:

$$j(\mathfrak{p}) = \sum_{\mathfrak{P}\cap A'=\mathfrak{p}} e(\mathfrak{P},\mathfrak{p})\,\mathfrak{P}$$

Par linéarité j s'étend en un homomorphisme de D (A') dans D (A). Comme A est entier sur A', pour tout élément $\mathfrak{P}$ de P(A), l'idéal premier $\mathfrak{P}\cap A'$ est nul ou de hauteur 1 donc l'homomorphisme j applique F(A') dans F(A) d'où un homomorphisme canonique $\bar{j}$ de C(A') dans C(A). Soit $\mathfrak{D}$ le sous groupe additif de A composé des éléments de la forme $\frac{Dt}{t}$ avec t dans K (ce sont des "dérivées logarithmiques") : il contient le sous groupe $\mathfrak{D}'$ des dérivées logarithmiques d'unités (c'est-à-dire des $\frac{Du}{u}$ où u parcourt le groupe des unités A^* de A). Nous avons le théorème suivant [3] :

Théorème 0

Il existe un monomorphisme canonique $\bar{\phi}$:

$$\bar{\phi} : \ker \bar{j} \longrightarrow \mathfrak{D}/\mathfrak{D}'$$

Si de plus le degré de K sur K' est p et si D.A n'est contenu dans aucun idéal premier de hauteur 1 de A, alors $\bar{\phi}$ est un isomorphisme.

A propos de ce théorème, deux conjectures ont été faites :

1 - Soit $\mathfrak{U}$ l'idéal A. DA. Toute dérivée logarithmique qui se trouve dans $\mathfrak{U}$ est la dérivée logarithmique d'une unité.

2 - Un élément de $\mathfrak{U}$ qui est la dérivée d'un élément de K est aussi la dérivée d'un élément de A.

Ces deux conjectures ont été démontrées dans quelques cas particuliers.

B) Etude de quelques cas particuliers

1) A est un anneau de séries formelles à une indéterminée X sur un corps L et la dérivation D est nulle sur le corps L. Soit x l'élément DX que nous supposerons dans l'idéal maximal $\mathfrak{M}$ de A : alors l'idéal $\mathfrak{U}$ est l'idéal maximal x A et est contenu dans $\mathfrak{M}$. L'ensemble des unités de A est le groupe multiplicatif A^* des séries formelles d'ordre nul.

Dans ces conditions, les conjectures 1 et 2 sont vraies, démontrons la conjecture 1 : la dérivée logarithmique $\frac{DP}{P}$ est dans $\mathfrak{U}$ donc s'écrit xQ, où Q est dans A ; la série P peut s'écrire comme le produit d'une puissance de X et d'une série R d'ordre nul

$$P = X^n R$$

$$xQ = x\left(\frac{n}{X} + \frac{R'}{R}\right)$$

Comme R appartient à A^*, l'élément $Q - \frac{R'}{R}$ appartient à A donc n est nul modulo la caractéristique p : la dérivée logarithmique $\frac{DP}{P}$ est aussi la dérivée

logarithmique de l'unité R.

La conjecture 2 se démontre d'une manière analogue.

2) L'anneau A est local, son idéal maximal $\mathfrak{M}$ contient l'idéal $\mathfrak{U}$ et la dérivation D^p est de la forme a. D où a est dans K.

Nécessairement, l'élément a est dans K' : en effet, appliquons la formule de Barsotti-Cartier [4] à un élément x de A n'appartenant pas à A' :

$$\frac{D^p x}{\overset{\cdot}{x}} = \left(\frac{Dx}{x}\right)^p \bullet D^{p-1}\left(\frac{Dx}{x}\right) = a\,\frac{Dx}{x}$$

Appliquant la dérivation D, nous obtenons :

$$Da\,\frac{Dx}{x} + aD\left(\frac{Dx}{x}\right) = aD\left(\frac{Dx}{x}\right) \Rightarrow Da = 0$$

Si l'élément a appartient à A , la conjecture 1 est vraie :

soit t un élément de $\mathfrak{U}$ qui est la dérivée logarithmique d'un élément x de K : quitte à remplacer x par un élément de $A^p x$, nous pouvons supposer que x appartient à A. Comme a appartient à A^* , l'élément $\frac{Dx}{ax}$ est dans $\mathfrak{M}$; par récurrence, nous voyons que $\frac{D^n x}{ax}$ est dans $\mathfrak{M}$ pour tout n positif : l'élément $u = -1 + \frac{D^{p-1}x}{ax}$ est alors une unité et t est la dérivée logarithmique de u^{-1}.

Supposant toujours a dans A^*, nous obtenons un résultat plus fort que la conjecture 2 : tout élément t de A qui est la dérivée d'un élément x de K est la dérivée d'un élément de A. Nous voyons en effet que t est la dérivée de l'élément $D^{p-2}(a^{-1}t)$ de A (le cas p = 2 ne fait pas exception, car D^0 est l'identité).

3) L'anneau A est de valuation discrète et son idéal maximal $\mathfrak{M}$ contient l'idéal $\mathfrak{U}$

Soit z une uniformisante de l'anneau A.

a) étude de l'idéal $\mathfrak{U}$

Comme l'anneau A est de valuation discrète, l'idéal $\mathfrak{U}$ est principal. Soit y un élément de A tel que v (Dy) soit minimal : ainsi $\mathfrak{U}$ est l'idéal engendré par Dy. Si v (Dy) est égal à v (Dz), l'idéal $\mathfrak{U}$ est engendré par Dz. Sinon montrons qu'il existe un élément u dans A^* tel que v (Du) soit égal à v (Dy) : l'élément y de A s'écrit uz^n, avec u dans A^* et n entier positif ou nul.

Si n est nul modulo p, l'égalité v (Dy) = v (Du) + n entraine que n est nul, donc y appartient à A^*. Si n n'est pas multiple de p, v (Dz) ne peut être supérieur à v (Dy) que si Du n'est pas nul :

$$v(Dy) \geq \mathrm{Inf}\left[n+v(Du), n-1+v(Dz)\right]$$

Or, les trois hypothèses n différent de 0, v (Dy) inférieur (resp. inférieur ou égal) à v (Dz) (resp. v (Du)) conduisent à une incompatibilité.

b) Etude de la validité des conjectures 1 et 2

Si l'idéal U est engendré par Dz, la conjecture 1 est vraie : supposons que l'élément t, de la forme b Dz, b appartenant à A, soit la dérivée logarithmique de x, que nous écrirons uz^r ; l'entier relatif r s'écrit hp + 1, s étant un entier non négatif, inférieur à p. La dérivée logarithmique de uz^s est t, donc nous pouvons nous limiter au cas où r est un entier non négatif, inférieur à p.

$$Dx = Du\ z^r + r\ Dz\ z^{r-1}\ u$$

$$Dx = x\ b\ Dz$$

Si r n'est pas nul, v (Dx) vaut v (Dz) + v(x) - 1, maisaussi v (Dz) + v (x) + v (b), ce qui contredit le fait que b est dans A : la dérivée logarithmique de x n'est donc dans U que si v(x) est multiple de p et nous avons alors que t est la dérivée logarithmique de l'unité u. Lorsque U est engendré par Dz, nous pouvons seulement en déduire que si un élément t de U est la dérivée d'un élément de K, il est ou bien la dérivée d'un élément de A, ou bien la dérivée d'un élément $u\ z^{hp}$ où u est un élément de A^* et h un entier relatif ; supposons en effet que l'élément t, de la forme b Dz, b appartenant à A, soit la dérivée de x, que nous écrirons uz^r ; l'entier relatif r s'écrit hp + s, s étant un entier non négatif, inférieur à p. Si s est non nul, nous avons :

$$v\ (Dx) = v\ (b) + v\ (Dz)$$

$$v\ (Dx) = v\ (Dz) + r - 1$$

Comme b est dans A, r est supérieur ou égal à 1 donc x est dans A.

Si s est nul, nous avons :

$$v(b) + v(Dz) = v(Du) + hp.$$

Nous en déduisons seulement que x est de la forme uz^{hp}.

c) Etude de l'anneau A'

Lorsque U est engendré par Dz, l'anneau A' est l'ensemble des éléments de la forme uz^{hp}, où u est un élément de A'^* et h un entier non négatif.

Il est clair que les éléments de cette forme appartiennent à . Soit x un élément de A' que nous écrirons uz^n :

$$Duz^n + n\ Dz\ z^{n-1}\ u = 0$$

Si n est nul modulo p, Du est nécessairement nul, donc u appartient à A'^*.

Si n n'est pas multiple de p, comme v (Du) est supérieur ou égal à v (Dz), l'égalité $z\ Du + n\ Dz\ u = 0$ entraine la nullité de Du, donc celle de n modulo p, d'où une contradiction.

d) Etude de dérivations D telles que D^p soit de la forme aD

Comme dans le paragraphe B) 2), nous démontrons que Da est nul.

montrons que a appartient à l'anneau A' :

- supposons que, quel que soit x dans A, $v(Dx)$ soit supérieur ou égal à $v(x)$: comme D n'est pas la dérivation nulle, il existe un x dans A tel que Dx soit différent de zéro. L'hypothèse, appliquée successivement à Dx, D^2x, ..., $D^{p-1}x$ montre que :

$$v(a) + v(Dx) = v(D^p x) \geq v(D^{p-1}x) \geq \cdots \geq v(D^2 x) \geq v(Dx)$$

Alors, $v(a)$ est positif ou nul, donc a est un élément de A'

- supposons qu'il existe un x dans A tel que $v(Dx)$ soit inférieur à $v(x)$: écrivons x sous la forme uz^n. Si n était multiple de p, $v(Dx)$ serait égal à $n+v(Du)$, donc ne pourrait être inférieur à n, puisque Du appartient à A. Sinon :

$$v(Dx) \geq \mathrm{Inf}[v(Du) + n, v(Dz) + n - 1]$$

Les deux nombres $v(Du) + n$, $v(Dz) + n - 1$ sont supérieurs ou égaux à n, d'où une contradiction. Par une démonstration analogue, nous obtenons le résultat suivant : l'élément a est dans U si et seulement si $v(Dz)$ est égal à $v(z)$ (donc vaut 1). Dans ces conditions, nous avons :

$$v(x) = v(D^n x) \quad \forall\ n \neq 0 \text{ si } v(x) \neq hp$$

C) Généralisation du théorème 0 et interprétation par les groupes de cohomologie.

1) Constructions préliminaires

Etant donné l'anneau de Krull A de caractéristique p non nulle et de corps des fractions K, considérons n dérivations $D_1, \ldots, D_n$ indépendantes de K telles que, pour tout i, nous ayons ;

$$D_i\ A \subset A$$

Désignons par K'_i le sous corps de K noyau de D_i, par A'i l'anneau $A \cap K'_i$ (qui est aussi le noyau de la restriction de D_i à A), par A'_i le groupe des unités de A'_i. Alors, si A^* désigne le groupe des unités de A, nous avons :

$$A'^*_i = A^* \cap A'_i$$

Soit ε un élément tel que ε^2 soit nul. Appelons L l'anneau de nombres duaux $K \oplus K\varepsilon$, B l'anneau $A \oplus K\varepsilon$ et M l'ensemble $A^* \oplus K\varepsilon$. Le groupe multiplicatif de L, soit L^*, est $K^* \oplus K\varepsilon$ tandis que celui de B, soit B^*, est M.

Les n applications $s_1, \ldots, s_n$ de L dans L définies par :

$$s_i(a + b) = a + (b + D_i a)\varepsilon$$

sont des automorphismes de L dans L. Leurs restrictions à B et B^* sont aussi des automorphismes de B et B^*.

Nous avons :

$$s_i s_j(a + b\varepsilon) = a + (b + (D_i + D_j)a)\varepsilon$$

Le groupe G engendré par les est isomorphe à $(Z/pZ)^n$. Comme le groupe L^*/B^*

est isomorphe à K^*/A^*, il est aussi isomorphe à F (A), groupe des diviseurs principaux de A, d'où la suite exacte :

$$1 \longrightarrow B^* \longrightarrow L^* \longrightarrow F(A) \longrightarrow 0$$

Notons $(B^*)^G$ et $(L^*)^G$ les invariants de B^* et L^* par G ; le groupe F (A) est invariant par G et nous avons la suite exacte :

$$(1) \qquad 1 \longrightarrow (B^*)^G \longrightarrow (L^*)^G \longrightarrow F(A) \longrightarrow H^1(G,B^*) \longrightarrow H^1(G,L^*) \longrightarrow H^1(G,F(A))\ldots$$

2) Etude des différents termes de la suite exacte (1)

a) Etude de $(B^*)^G$

L'élément $a+b\varepsilon$ de B^* est dans $(B^*)^G$ si et seulement si pour tout i nous avons :

$$a+b\varepsilon = s_i(a+b\varepsilon)$$
$$= a+(b+D_i a)\varepsilon$$

$$a+b\varepsilon \in (B^*)^G \iff D_i a = 0$$
$$\iff a \in A_1'^* \cap A_2'^* \cap \ldots \cap A_n'^* = A'^*$$

Les invariants par G de B^* sont donc les éléments de $A'^* \oplus K\varepsilon$

b) Etude de $(L^*)^G$

Un raisonnement analogue au précédent montre que les invariants par G de L^* sont les éléments de $K' \oplus K\varepsilon$, où K' désigne le corps $K_1' \cap K_2' \cap \ldots \cap K_n'$

c) Etude de $H^1(G, B^*)$

Un 1 - cocycle f est une application de G dans B^* telle que :

$$f(st) = s(f(t)).\ f(s) \qquad \forall s,t \in G$$

Pour déterminer f, il suffit de connaître les images $f(s_i)$ lorsque i varie de 1 à n :

$$f(s_i) = a_i + b_i\varepsilon$$

Calculons $f(s_i^p)$; d'après la définition de s_i, nous avons :

$$s_i^n(a+b) = a + (b + nD_i a)\varepsilon$$
$$s_i^p = 1 \Rightarrow f(s_i^p) = 1$$

D'autre part, calculons $f(s_i^2)$:

$$f(s_i^2) = (s_i(a_i + b_i\varepsilon)).(a_i + b_i\varepsilon)$$
$$= a_i^2 + (a_i(b_i + D_i a_i) + a_i b_i)\varepsilon$$

Par récurrence, nous obtenons :

$$f(s_i^p) = a_i^p + m_i\varepsilon$$

Comparant les deux expressions de $f(s_i^p)$, nous en déduisons que a_i^p est égal à 1. Or $a_i^p - 1 = 0$ peut encore s'écrire $(a_i - 1)^p = 0$ donc a_i est égal à 1.

$$m_i = C'_p\ b_i = p\ b_i \Rightarrow m_i = 0$$

Pour que f soit un 1-cobord, il faut et il suffit qu'il existe un élément $a + b\varepsilon$ dans B^* tel que :

$$f(s) = (s(a + b\varepsilon))\,(a + b\varepsilon)^{-1} \quad \forall s \in G$$

$$a + (b + D_i a)\varepsilon = (a + b\varepsilon)\,(1 + b_i a)$$

$$= a + (b + b_i a)\varepsilon$$

$$b_i = \frac{D_i a}{a}$$

Soit $\mathfrak{D}'$ le sous groupe additif de K^n constitué par les dérivées logarithmiques d'unités (c'est-à-dire l'ensemble des $(\frac{D_i a}{a})_{i=1,\ldots,n}$ lorsque a décrit A^*).
Nous venons de démontrer que H^1 (G, B^*) est isomorphe à $K^n/\mathfrak{D}'$.

d) Etude de H^1 (G, L^*)

Soit $\mathfrak{D}$ le sous-groupe additif de A^n constitué par les dérivées logarithmiques d'éléments de K (c'est-à-dire l'ensemble des $(\frac{D_i a}{a})_{i=1,\ldots,n}$ appartenant à A^n).

Un raisonnement analogue à celui fait au c) montre que H^1 (G,L^*) est isomorphe à $K^n/\mathfrak{D}$.

e) Etude de H^1 (G, F (A))

Comme G opère trivialement sur F (A), le groupe H^1 (G, F (A)) est constitué par les homomorphismes f de G dans F (A). Pour déterminer f, il suffit de connaître les images $f(s_i)$ lorsque i varie de 1 à n. Soit X_i un élément de K^* tel que le diviseur principal (x_i) engendré par x_i soit $f(s_i)$. Comme a_i^p est l'identité, le diviseur (x_i^p) est le diviseur unité. Cela signifie que x_i^p est une unité, c'est-à-dire que $v(x_i)$ est nulle pour toute valuation discrète v de l'anneau A : l'élément x_i appartient donc à A^* et (x_i) est le diviseur unité. L'homomorphisme envoie tout automorphisme s_i sur le diviseur unité donc le groupe H^1 (G, F(A)) se réduit à son élément neutre.
Nous obtenons finalement la suite exacte :

$$(2) \qquad 1 \longrightarrow (B^*)^G \longrightarrow (L^*)^G \longrightarrow F(A) \longrightarrow K^n/\mathfrak{D}' \longrightarrow K^n/\mathfrak{D} \longrightarrow 0$$

3) Lien avec la théorie de la descente p-radicielle

Etant donné l'anneau $A' = A'_1 \cap A'_2 \cap \ldots \cap A'_n$, nous avons la suite exacte :

$$1 \longrightarrow (B^*)^G \longrightarrow (L^*)^G \longrightarrow F(A') \longrightarrow 0$$

Compte tenu de la suite exacte (2), nous obtenons la suite exacte (3) :

$$(3) \qquad 0 \longrightarrow F(A') \longrightarrow F(A) \longrightarrow K^n/\mathfrak{D}' \longrightarrow K^n/\mathfrak{D} \longrightarrow 0$$

Comme dans la partie A), considérons l'homomorphisme canonique $\bar{j}$ de C (A') dans C (A) : son noyau est j^{-1} (F(A))/ F(A').

La suite exacte (3) permet de définir un homomorphisme de j^{-1} (F(A)) dans $\mathfrak{D}/\mathfrak{D}'$ dont le noyau est F (A') d'où un monomorphisme Φ de ker $\bar{j}$ dans $\mathfrak{D}/\mathfrak{D}'$: ceci est une généralisation du théorème 0.

Remarque : Il est à noter que cette interprétation du théorème 0 par les groupes de cohomologie renforce l'analogie entre la descente p-radicielle et la descente galoisienne (où les dérivations sont remplacées par les automorphismes) puisque cette dernière théorie avait été interprétée par la cohomologie.

CHAPITRE II

APPLICATION A L'ETUDE DE LA FACTORIALITE DE CERTAINS ANNEAUX

Soient k un corps de caractéristique 2, u une indéterminée sur k et A' l'anneau :

$$A' = k(u)\left[\left[x,y,z\right]\right] \quad \text{où} \quad x^2 + y^i + uz^{2j} = 0$$

i et j étant deux nombres entiers impairs supérieurs ou égaux à 1. Le problème consiste à étudier pour quelles valeurs de i et j l'anneau A' est factoriel.

A) LIEN AVEC LA THEORIE DE LA DESCENTE p-RADICIELLE

Soit K' le corps des fractions de A' ; nous cherchons à plonger K' dans un corps K et à construire une dérivation D de K de noyau K'.

Considérons l'anneau A :

$$A = k(t)\left[\left[Y,z\right]\right]$$

où t est une indéterminée sur k, et K son corps des fractions :

$$K = k(t)\left(\left(Y,z\right)\right)$$

Soit D la k-dérivation de A définie par :

$$Dt = Y^{i-1}$$

$$DY = z^j$$

$$Dz = 0$$

Il est clair que $k(t^2)\left[\left[Y^2,z\right]\right]$ est contenu dans le noyau de D. D'autre part, considérons l'élément x défini par :

$$x = Y^i + tz^j$$

$$Dx = 2\,Y^{i-1}z^j = 0$$

Introduisons les notations suivantes :

$$t^2 = u \qquad Y^2 = y$$

Le corps $k(u)\ ((x,y,z))$ est contenu dans le noyau de la dérivation D étendue à K, où x est défini par :

$$x = Y^i + tz^j$$

$$x^2 = y^i + uz^{2j}$$

Le corps K est de degré 2 sur $k(u)((x,y,z))$. Par construction, la dérivation D^2 est nulle : nous en déduisons que K est de degré 2 sur ker D donc:

$$\ker D = k(u)((x,y,z)) \quad \text{où} \quad x^2 = y^i + uz^{2j}$$

Etudions la surface $x^2 = y^i + uz^{2j}$. Posons $f(x,y) = x^2 - y^i - uz^{2j}$. Comme nous sommes en caractéristique 2, nous avons :

$$f'x = 0$$

$$f'y = y^{i-1}$$

$$f'z = 0$$

Le critère jacobien montre que la surface ne contient qu'une seule courbe singulière définie par :

$$\begin{cases} y = 0 \\ x^2 = uz^{2j} \end{cases}$$

Dans A', cette courbe singulière est définie par l'idéal premier A'y : il en résulte que l'anneau $A'_{A'y}$ est de valuation discrète, donc l'anneau A' est normal en codimension 1. Comme A' est un anneau de Macaulay, il est intégralement clos.

Dans ces conditions, nous avons :

$$A' = k(u)((x,y,z)) \cap A$$

L'anneau A' est le noyau de la restriction de D à A et l'homomorphisme canonique $\bar{j}$:

$$\bar{j} : C(A') \longrightarrow C(A)$$

est défini. Comme l'anneau A est factoriel, le groupe $C(A)$ est nul et le noyau de $\bar{j}$ est le groupe $C(A')$ tout entier.

Appliquons le théorème 0 rappelé au chapitre I : il existe un isomorphisme $\bar{\Phi}$ de $\ker \bar{j}$ sur Ω / Ω',

$$\ker \bar{j} = C(A') \longrightarrow \Omega / \Omega' ,$$

Pour étudier $C(A')$, il suffit donc de voir la forme de Ω / Ω' .

Etudions les éléments de Ω : si F appartient à Ω , il existe un élément G de K tel que :

$$F = \frac{DG}{G}$$

Calculons DF ; compte tenu de la nullité de D^2, nous obtenons :

$$DF = \left(\frac{DG}{G}\right)^2$$

$$DF = F^2$$

Réciproquement, si F est solution de l'équation $F^2 = DF$, l'élément F est la dérivée logarithmique de F car $F = \frac{DF}{F}$. Les éléments de Ω sont donc les solutions de l'équation (1) :

$$(1) \qquad F^2 = DF$$

qui appartiennent à l'anneau A.

B) RESOLUTION DANS L'ANNEAU A DE L'EQUATION (1)

Munissons Y du poids j et z du poids i. Soit F_n la composante isobare de F, de poids n :

$$F_n = \sum_{\ell m} a_\ell \; Y^\ell \; z^m \qquad a_\ell \in k(t)$$

où ℓ, m sont liés par la relation :

$$n = \ell j + mi$$

Etudions DF_n :

$$DF_n = \sum_{\ell,m} a'_\ell \; Y^{i-1+\ell} \; z^m + \ell . a_\ell \; Y^{\ell-1} \; z^{m+j}$$

où a'_ℓ désigne la dérivée usuelle de a_ℓ, considéré comme fraction rationnelle en t.

Ainsi DF_n est isobare, de poids $n + ij - j$. Décomposons chaque série F en somme (infinie) de composantes isobares :

$$F = F_q + F_{q+1} + \ldots$$

Nous appellerons ordre de F, et nous noterons O(F), le poids de sa plus basse composante non nulle. Nous introduirons $\mathfrak{D}_q$, le sous groupe de $\mathfrak{D}$ formé des dérivées logarithmiques d'ordre supérieur ou égal à q : ainsi $(\mathfrak{D}_q)$ est une filtration de $\mathfrak{D}$. Munissons $\mathfrak{D}'$ de la filtration induite :

$$(\mathfrak{D}'_q) = (\mathfrak{D}_q \cap \mathfrak{D}')$$

et le groupe quotient $\mathfrak{G} = \mathfrak{D}/\mathfrak{D}'$ de la filtration quotient $(\mathfrak{G}_q)$. Nous avons :

$$\mathfrak{G}_q = (\mathfrak{D}' + \mathfrak{D}_q)/\mathfrak{D}' = \mathfrak{D}_q/\mathfrak{D}'_q$$

Le groupe $\mathfrak{G}$ est isomorphe au groupe gradué $\sum_q \mathfrak{G}_q/\mathfrak{G}_{q+1}$ (car il s'agit

d'espaces vectoriels sur F_2).

Soit F une dérivée logarithmique non nulle : l'ordre de F^2 est égal à deux fois l'ordre de F ; d'autre part, l'ordre de DF est supérieur ou égal à l'ordre de F augmenté de ij - j . Comme F est solution de l'équation (1), nous en déduisons :

$$2\,O(F) \geq O(F) + ij - j$$

$$O(F) \geq ij - j$$

1) RECHERCHE DE LA COMPOSANTE ISOBARE DE F DE POIDS ij - j .

Le poids de la composante F_{ij-j} est 2(ij - j) donc Fij - j est elle-même solution de l'équation (1). Pour alléger les notations, nous poserons :

$$Fij - j = G$$

$$G = \sum_{n,m} a_n Y^r z^m$$

Les entiers n et m sont liés par la relation :

$$nj + mi = j(i - 1)$$

Soit d le pgcd de i et j : d est un entier impair :

$$j = dj' \qquad i = di'$$

$$nj' + mi' = j'(i'd - 1)$$

$$(i'd - n - 1)j' = mi'$$

D'après des propriétés de divisibilité, nous en déduisons :

$$m = \ell j' \qquad \ell = 0,\ldots,d - 1$$

$$n = i - 1 - \ell i'$$

a) les entiers i et j sont premiers entre eux : d vaut 1

Alors, G se réduit au monôme aY^{i-1}. Comme G est solution de l'équation (1), nous avons :

$$a' Y^{2i-2} = a^2 Y^{2i-2}$$

$$a' = a^2$$

Dans ces conditions, ou bien G est nul (et il est la dérivée logarithmique de l'unité 1), ou bien G est la dérivée logarithmique de l'unité a.

b) cas général : d est supérieur à 1

Comme d est impair, il est de la forme $2s + 1$, où s est un entier supérieur ou égal à 1.

$$G = \sum_{\ell=0}^{2s} a_\ell \, Y^{i-1-\ell i'} \, z^{\ell j'}$$

Mettons en évidence les exposants pairs et impairs de Y :

$$G = \sum_{\ell=0}^{s} a_{2\ell} \, Y^{i-1-2\ell i'} \, z^{2\ell j'} + \sum_{\ell=0}^{s-1} a_{2\ell+1} \, Y^{i-1-i'(2\ell+1)} \, z^{(2\ell+1)j'}$$

Calculons DG :

$$DG = \sum_{\ell=0}^{s} a'_{2\ell} Y^{2i-2-2\ell i'} z^{2\ell j'} + \sum_{\ell=0}^{s-1} \left(a'_{2\ell+1} \, Y^{i} + a_{2\ell+1} \, z^{j} \right)$$

$$Y^{i-2-i'(2\ell+1)} \, z^{(2\ell+1)j'}$$

Ecrivons que G est solution de l'équation (1) ; par identification, nous obtenons les relations suivantes :

$$(2) \quad \begin{cases} a'_{2\ell} = a_\ell^2 & \ell = 0,\ldots,s \\ a_{2\ell+1} = a_{\ell+s+1}^2 & \ell = 0,\ldots,s-1 \end{cases}$$

Nous allons montrer que les a_ℓ sont nuls pour ℓ différent de 0.

Faisons tout d'abord quelques remarques sur les valuations v de $k(t)$ triviales sur k ; elles sont de deux types :

- ou bien v est la valuation à l'infini, et alors nous avons :

$$v(f') \geq v(f) + 1 \qquad \forall f \in k(t)$$

- ou bien v n'est pas la valuation à l'infini, et alors nous avons :

$$v(f') \geq v(f) - 1 \qquad \forall f \in k(t)$$

Dans tous les cas, nous avons donc :

$$v(f') \geq v(f) - 1.$$

Soit σ la permutation de $2s$ objets définie par :

$$\begin{cases} \sigma(2\ell) = \ell \\ \\ \sigma(2\ell-1) = \ell + s \end{cases} \qquad \ell = 1,\ldots,s$$

Appelons α le nombre d'éléments du cycle engendré par j : remarquant que quel que soit j, son cycle contient au moins un nombre pair et un nombre impair, nous en déduisons que α est supérieur ou égal à 2.

Partant de a^2_j, nous aurons α égalités du type de celles écrites en (2) faisant intervenir au premier membre tantôt la dérivée d'un a_ℓ , tantôt un a_ℓ mais une fois au moins nous aurons un a_ℓ. La dernière égalité aboutira à l'élément a_j.

Soit v une valuation quelconque de $k(t)$, triviale sur k. Prenons les valuations des α égalités ainsi écrites et additionnons les membre à membre après avoir multiplié 1'avant dernière relation par 2, la précédente par $2^2,\ldots$, la première par $2^{\alpha-1}$. Compte tenu du fait que $v(f')$ est supérieur ou égal à $v(f) - 1$, nous obtenons :

$$2^{\alpha}\, v(a_j) \geq v(a_j) - (2 + 2^2 + \cdots + 2^{\alpha-1})$$

$$(2^{\alpha} - 1)\, v(a_j) \geq 2 - 2^{\alpha}$$

Comme $v(a_j)$ appartient à $\mathbb{Z}$, il est positif ou nul : ceci étant vrai pour toutes les valuations de $k(t)$, les a_j sont des polynômes en t.

Soit $d(a_\ell)$ le degré du polynôme a_ℓ. Nous avons :

$$d^\circ(a'_j) \leq d^\circ(a_j) - 1$$

Prenant le degré des polynômes intervenant dans les α relations écrites ci-dessus, nous obtenons :

$$2^{\alpha}\, d^\circ(a_j) \leq d^\circ(a_j) - 1$$

$$(2^{\alpha} - 1)\, d^\circ(a_j) \leq -1$$

Le degré d'un polynôme ne pouvant être négatif, tous les a_ℓ sont nuls.

Dans ces conditions, G se réduit à :

$$G = a\, Y^{i-1} \qquad a \in k(t)$$

Comme dans le cas a), G est ou bien nul, ou bien la dérivée logarithmique de a.

2) ETUDE DES COMPOSANTES ISOBARES DE F DE POIDS SUPERIEUR A $ij - j$.

Nous pouvons donc nous limiter à l'étude de $\mathfrak{D}_q$, $\mathfrak{D}'_q$ et $\mathfrak{I}_q$ pour q supérieur à $ij - j$. Notons P_q l'ensemble des polynômes isobares de poids q. Soit Ψ l'homomorphisme de $\mathfrak{D}_q$ dans P_q qui, à tout $F = F_q + F_{q+1} + \cdots$ appartenant à $\mathfrak{D}_q$ fait correspondre sa composante F_q de poids q. Le noyau de Ψ est $\mathfrak{D}_{q+1}$.

Soit F un élément de $\mathfrak{D}_q$: l'ordre de F^2 est supérieur ou égal à $2q$, tandis

que, si DF_q est non nul, il est d'ordre $q + ij - j$ strictement inférieur à $2q$ (puisque q est strictement supérieur à $ij - j$). Comme F est solution de l'équation (1), c'est que DF_q est nul :

$$F_q \in A' \cap P_q$$

$$\Psi(\Omega_q) \subset A' \cap P_q$$

Soit $\mathcal{H}$ l'idéal de A engendré par Y^{i-1} et z^j. Comme toute dérivée logarithmique d'unité appartient à $\mathcal{H}$, nous avons les relations :

$$\Psi(\Omega_q) \subset A' \cap P_q$$

$$\Psi(\Omega'_q) \subset \mathcal{H} \cap A' \cap P_q$$

Montrons que nous avons surjectivité, c'est-à-dire que nous avons les relations (3):

$$\Psi(\Omega_q) = A' \cap P_q$$

(3)

$$\Psi(\Omega'_q) = \mathcal{H} \cap A' \cap P_q$$

Soit donc F_q un élément de $A' \cap P_q$. Nous cherchons des polynômes isobares F_n $(n \geq q)$ tels que F défini par :

$$F = F_q + F_{q+1} + \cdots$$

soit solution de l'équation $F^2 = DF$ (1).

Comparant les composantes isobares, l'équation (1) se traduit par :

$$F_n^2 = DF_{2n-ij} + j$$

$$n > ij = j \Rightarrow 2n - ij + j > n$$

De plus, l'entier $2n - ij + j$ est pair. Chaque F_m est donc déterminé par "inté-

gration" à partir d'un F_s^2 avec s strictement inférieur à m. Remarquons que, si m est impair, la condition sur F_m s'écrit $DF_m = 0$. Il s'agit donc de 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 supérieur ou égal à q. Par additivité de la dérivation et de l'élévation au carré, nous sommes ramenés au cas d'un monôme $G = a\, Y^{\ell}\, z^n$ où a appartient à $k(t)$, les entiers m, ℓ, n vérifiant :

$$m + ij - j = 2\,(\ell j + ni)$$

Si 2ℓ est supérieur ou égal à $i - 1$, nous prendrons :

$$F_m = a^2\, \frac{t}{Y^{i-1}}\, Y^{2\ell}\, z^{2n}$$

Si $2n$ est supérieur ou égal à j, nous prendrons :

$$F_m = a^2\, Y^{2\ell+1}\, z^{2n-j}$$

Nous sommes toujours dans l'un de ces deux cas, car, si 2ℓ est inférieur à $i - 1$, et si $2n$ est inférieur à j, par des considérations de parité, nous obtenons :

$$2\ell \leqq i - 3 \qquad\qquad 2n \leqq j - 1$$

$$m + ij - j \leqq (i - 3)j + i(j - 1)$$

$$m \leqq ij - 2j - i$$

Or m est supérieur à $ij - j$.

De plus, si nous supposons par récurrence que nous avons G dans $\mathcal{U}$, nous aurons ou bien ℓ supérieur ou égal à $i - 1$ et $2\ell - i + 1$ sera encore supérieur à $i - 1$, ou bien n supérieur ou égal à j et $2n - j$ sera encore supérieur à j, de sorte que F_m peut être pris dans $\mathcal{U}$.

Les relations (3) se trouvent ainsi démontrées : elles montrent qu'il existe un isomorphisme canonique de $\mathcal{G}_q/\mathcal{G}_{q+1}$ sur $(A' \cap P_q)/(\mathcal{U} \cap A' \cap P_q)$. Donc

$\mathcal{G}_q/\mathcal{G}_{q+1}$ a une structure de $k(t^2)$ espace vectoriel de dimension finie $n(q)$.

C) CONCLUSION

Le groupe $C(A')$ est donc un $k(u)$-espace vectoriel de dimension finie

$$N(i,j) = \sum_{q>ij-j} n(q)$$

Etudions cet entier $N(i,j)$: dans l'anneau A, l'idéal $\mathcal{H} = (Y^{i-1}, z^j)$ admet un supplémentaire engendré par les monômes $Y^\ell z^n$ tels que $\ell < i-1$ et $n < j$. Comme $Y^{i-1} + tz^j$ appartient à $\mathcal{H}$, un supplémentaire de $\mathcal{H} \cap A'$ dans A' est engendré par les monômes $Y^{2\ell}z^n$ tels que $2\ell < i-1$ et $n < j$. L'entier $N(i,j)$ est égal au nombre de ces monômes qui sont de poids strictement supérieur à $ij - j$: $N(i,j)$ est le nombre des couples (ℓ,n) tels que :

$$\begin{cases} 2\ell < i-1 \\ n < j \\ 2\ell j + ni > ij - j \end{cases}$$

THEOREME 1 - Soient k un corps de caractéristique 2, u une indéterminée sur k et A' l'anneau $k(u)[[x,y,z]]$ où $x^2 + y^i + uz^{2j} = 0$, i et j étant deux nombres entiers impairs supérieurs ou égaux à 1. Alors le groupe $C(A')$ des classes de diviseurs de A' est un $k(u)$-espace vectoriel de dimension $N(i,j)$ égale au nombre de couples (ℓ,n) tels que :

$$0 \leq 2\ell < i-1, \quad 0 \leq n < j \quad \text{et} \quad 2\ell j + ni > ij - j$$

Pour que l'entier $N(i,j)$ soit nul, il faut que l'inégalité :

$$(i-3)j + (j-1)i \leq ij - j$$

soit satisfaite ;

$$ij - 2j - i \leq 0$$

Si i vaut 1 ; cette condition est vérifiée quel que soit j ; de même si j vaut 1, cette condition est vérifiée quel que soit i. A part ces deux cas là, N(i,j) ne peut être nul que si i et j valent tous les deux 3.

COROLLAIRE - Les seuls anneaux factoriels de la famille $k(u)\left[\left[x,y,z\right]\right]$ avec $x^2 + y^i + uz^{2j} = 0$ sont :

$$k(u)\left[\left[x,y,z\right]\right] \text{ avec } x^2 + y + uz^{2j} = 0 \qquad \forall_j \text{ impair} \geq 1$$

$$k(u)\left[\left[x,y,z\right]\right] \text{ avec } x^2 + y^i + uz^2 = 0 \qquad \forall_i \text{ impair} \geq 1$$

$$k(u)\left[\left[x,y,z\right]\right] \text{ avec } x^2 + y^3 + uz^6 = 0$$

CAS PARTICULIER : lorsque les entiers i et j sont égaux, il est facile de calculer N(i,j) :

$$\begin{cases} 2\ell < i - 1 \\ n < i \\ 2\ell + n \geq i \end{cases}$$

Posons $i = 2s + 1$.

$$\begin{cases} 2\ell < 2s \qquad \ell < s \\ n < 2s + 1 \\ 2\ell + n \geq 2s + 1 \end{cases}$$

Le nombre n peut prendre $2s + 1$ valeurs. Si n est pair, il lui correspond $\frac{n}{2} - 1$ valeurs de ℓ donc $(\frac{n}{2} - 1)$ couples (ℓ,n) ; Si n est impair, il lui correspond $\frac{n-1}{2}$ valeurs de ℓ donc $(\frac{n-1}{2})$ couples (ℓ,n). D'où :

$$N(i,i) = 2\ 1 + 2 + \cdots + (s - 1)$$

$$N(i,i) = s(s - 1)$$

Nous retrouvons bien que l'anneau $k(u)\left[\left[x,y,z\right]\right]$ avec $x^2 + y^i + uz^{2i} = 0$ n'est factoriel que si i vaut 1 ou 3.

REMARQUE

Dans un récent article [10], Salmon a étudié l'anneau $A' = k(u)\left[\left[x,y,z\right]\right]$ où $x^2 + y^3 + uz^6 = 0$; cherchant à donner une réponse à la question suivante posée par P. Samuel dans [8] : si B est un anneau local, factoriel et complet, l'anneau des séries formelles $B\left[\left[T\right]\right]$ est-il factoriel ? Salmon a démontré que l'anneau $A = k(u)\left[\left[x,y,z\right]\right]$ où $x^2 + y^3 + uz^6 = 0$ était factoriel, alors que l'anneau $A'\left[\left[T\right]\right]$ ne l'était pas. Il est à noter que si cet exemple répond par la négative à la question posée, c'est le seul anneau de la famille qui pouvait convenir.

Etudions la factorialité de l'anneau $A'\left[\left[T\right]\right]$. Pour cela, rappelons un lemme explicité dans [8] : soit B un anneau intègre, noéthérien ; supposons qu'il existe trois éléments U, V, W dans B et trois entiers non nuls n, m, ℓ tels que :

- U est premier
- V n'appartient pas à UB
- W^{n-1} n'appartient pas à $UB + VB$ mais W^n appartient à $U^{\ell}B + V^{m}B$
- $\ell mn - \ell m - mn - n\ell \geq 0$

Alors l'anneau $B\left[\left[T\right]\right]$ n'est pas factoriel. Pour utiliser ce lemme, nous poserons

$U = y \qquad V = z \qquad W = x$

$n = 2 \qquad \ell = i \qquad m = 2j$

- Si i et j sont tous les deux supérieurs ou égaux à 3, l'inégalité $4ij - 2ij - 2i - 4j \geq 0$ est vérifiée donc $A'\left[\left[T\right]\right]$ n'est pas factoriel.

- Si i vaut 1, l'anneau $A'\left[\left[T\right]\right]$ n'est autre que $k(u)\left[\left[x,z,T\right]\right]$ donc il est factoriel.

APPLICATION

L'étude précédente nous permet de déterminer dans quel cas l'anneau $A_1 = k(u)\left[x,y,z\right]$ avec $x^2 + y^i + uz^{2j} = 0$ est factoriel, k étant toujours un corps de caractéristique 2, u une indéterminée sur k, i et j deux entiers impairs supérieurs ou égaux à 1. En effet, le groupe $C(A_1)$ est encore isomorphe à $\mathfrak{D}_1/\mathfrak{D}'_1$ où $\mathfrak{D}_1$ désigne le sous groupe de A_1 formé de dérivées logarithmiques de K_1 et $\mathfrak{D}'_1$ le sous groupe formé de dérivées logarithmiques d'unités. Un élément F de A_1 est dans $\mathfrak{D}_1$ si et seulement si il est solution de l'équation :

$$F^2 = DF$$

Décomposons encore F en somme de composantes isobares :

$$F = F_q + \ldots + F_r$$

avec $F_q \neq 0$, $r \geq q$

Le poids des composantes isobares de DF varie entre $q + ij - j$ et $r + ij - j$. Nous avons donc nécessairement :

$$2q \geq q + ij - j$$

$$2r \leq r + ij - j$$

Il en résulte que :

$$r = q = ij - j$$

Alors F se réduit à F_{ij-j} : d'après l'étude faite au paragraphe B) 1), F est la dérivée logarithmique d'une unité donc $\mathfrak{D}_1/\mathfrak{D}'_1$ se réduit à 0.

THEOREME 2 - Soient k un corps de caractéristique 2, u une indéterminée sur k et A_1 l'anneau $k(u)[x,yz]$ où $x^2 + y^i + uz^{2j} = 0$, i et j étant deux entiers impairs supérieurs ou égaux à 1. Alors, l'anneau A_1 est factoriel.

APPENDICE

ETUDE DE LA PERMUTATION σ DEFINIE PAR :

$$\sigma(2\ell) = \ell \qquad \ell = 1,\ldots,s$$

$$\sigma(2\ell-1) = \ell + s$$

1. La permutation σ peut s'interpréter comme une homothétie de $Z_{/(2s+1)}$

Considérons l'application τ de Z dans Z définie par :

$$\tau(i) = i(s + 1)$$

Si i et j sont égaux modulo $2s + 1$, il en est de même de $\tau(i)$ et $\tau(j)$ donc l'application τ induit sur $Z_{/(2s+1)}$ une application $\bar{\tau}$.

$$\tau(2i) = 2i(s + 1)$$

$$= i \quad \text{modulo} \quad 2s + 1$$

$$\tau(2i - 1) = (2i - 1)(s + 1)$$

$$= i + s \quad \text{modulo} \quad 2s + 1$$

L'application induite $\bar{\tau}$ coïncide sur $Z_{/(2s+1)} - \{0\}$ avec σ .

2. Etude des orbites de longueur maximum

Soit i un élément de $\{1,\ldots,2s\}$. Etudions la longueur ℓ de l'orbite de i :

$$\tau(i) = i(s + 1)$$

$$\tau^n(i) = i(s + 1)^n$$

$$\tau^n(i) - i = i \left[(s + 1)^n - 1\right]$$

La longueur de l'orbite de i est le plus petit entier ℓ tel que $i\left[(s+1)^r - 1\right]$ soit nul modulo $2s+1$; soit L la longueur de l'orbite de **1**; nous avons alors :

$$(s+1)^L - 1 = 0 \qquad (2s+1)$$

Quel que soit i, la longueur de son orbite ℓ est un diviseur de L. D'autre part, si i et $2s+1$ sont premiers, la longueur de l'orbite de i est L donc il y a au moins $\phi(2s+1)$ éléments appartenant à des orbites de longueur maximum L ($\phi(2s+1)$ est la fonction d'Euler et désigne le nombre d'entiers positifs inférieurs ou égaux à $2s+1$ et premiers à $2s+1$).

Comme 2^L et $2s+1$ sont premiers, nous avons :

$$2(s+1)^L - 2^L = 0 \qquad (2s+1)$$

$$2^L - 1 = 0 \qquad (2s+1)$$

Le plus petit entier L vérifiant $2^L - 1 = 0\ (2s+1)$ est appelé l'ordre du nombre 2 modulo $(2s+1)$. D'après un théorème dû à Euler, l'entier L est un diviseur de $\phi(2s+1)$ [11]

Propriété 1 : Il existe au moins $\phi(2s+1)$ éléments appartenant à des orbites de longueur maximale L, où L est l'ordre du nombre 2 modulo $(2s+1)$ donc diviseur de $\phi(2s+1)$

2) la longueur de l'orbite d'un élément quelconque est un diviseur de L.

3. Conditions pour que toutes les orbites aient la même longueur

Etudions tout d'abord dans quel cas il n'y aura qu'une seule orbite : il faut que L soit égal au nombre d'objets $2s$. Or L est un diviseur de $\phi(2s+1)$ et :

$$\phi(2s+1) \leq 2s$$

$$\phi(2s+1) = 2 \Longleftrightarrow 2s+1 \text{ est premier}$$

Si $2s + 1$ est premier et si 2 est d'ordre $2s$ modulo $2s + 1$, le nombre 2 est appelé racine primitive de $2s + 1$.

PROPRIETE 2 : pour qu'il n'y ait qu'une seule orbite, il faut et il suffit que $2s + 1$ soit premier et que 2 soit racine primitive de $2s + 1$.

Etudions ce qui se passe lorsque $2s + 1$ est premier : la condition $i(2^{\ell} - 1) = 0$ (modulo $2s + 1$) entraine $2^{\ell} - 1 = 0$ (modulo $2s + 1$) donc tous les cycles ont la même longueur L.

D'autre part, la longueur de toute orbite est un diviseur de L donc si L est premier, toutes les orbites ont la même longueur L.

PROPRIETE 3 : les orbites ont toutes la même longueur dans les cas suivants :

1) $2s + 1$ est premier

2) l'ordre de 2 modulo $2s + 1$ est un nombre premier. Si N est le nombre d'orbites distinctes, nous avons :

$$NL = 2s$$

Ce ne sont pas là les seuls cas où toutes les orbites ont la même longueur ; considérons le nombre $2s + 1$:

$$2s + 1 = \frac{2^{25} - 1}{2^5 - 1}$$

$$= 2^{20} + 2^{15} + 2^{10} + 2^5 + 1$$

Le nombre $2s + 1$ n'est pas premier car il est égal au produit des deux nombres premiers 601 et 1801 :

$$2s + 1 = 601 \times 1801$$

L'ordre de 2 modulo 601 est 25 ; de même l'ordre de 2 modulo 1801 est 25 donc l'ordre de 2 modulo $2s + 1$ est un multiple de 25. D'autre part, nous avons :

$$2^{25} - 1 = (2^5 - 1)(2s + 1)$$

donc 25 est un multiple de l'ordre de 2 modulo $2s + 1$: finalement l'ordre de 2 modulo $2s + 1$ est 25. Les seules longueurs d'orbites possibles sont 5 et 25 : soit i un élément de $\{1,\ldots,2s\}$ dont l'orbite est de longueur 5 :

$$i = 601\ t + r \qquad 0 \leq r < 601$$

$$i(2^5 - 1) = 0 \qquad \text{(modulo } 2s + 1)$$

$$r(2^5 - 1) = 0 \qquad \text{(modulo } 601)$$

Ceci est impossible donc r est nul : i est multiple de 601 ; faisant le même raisonnement avec 1801, nous voyons que i est à la fois multiple de 601 et de 1801, ce qui est impossible donc la permutation définie par :

$$2s + 1 = 2^{20} + 2^{15} + 2^{10} + 2^5 + 1$$

nombre non premier, a toutes ses orbites de longueur 25, bien que l'ordre de 2 modulo $2s + 1$ ne soit pas premier.

Etudions le cas où $2s + 1$ est premier : pour qu'il n'y ait qu'une orbite, il faut et il suffit que 2 soit racine primitive de $2s + 1$. Soit L l'ordre de 2 modulo $2s + 1$: alors L divise 2s.

Rappelons un théorème [12] : soit $2s + 1$ premier ; alors :

$$(2s + 1) \mid 2^s - 1 \iff 2s + 1 = 8i \pm 1$$

$$(2s + 1) \mid 2^s + 1 \iff 2s + 1 = 8i \pm 3$$

Si $2s + 1$ est de la forme $8i \pm 3$, alors $2s + 1$ divise $2^s + 1$; si L divisait s, $2^s - 1$ serait nul modulo $2s + 1$, ce qui est impossible. Comme L divise 2s, L est de la forme 2a, où a est un diviseur de s.

Si $2s + 1$ est de la forme $8i \pm 1$, alors L est inférieur ou égal à s donc il y a plus d'un cycle : pour rechercher des s ne donnant qu'une seule orbite, nous

pouvons nous limiter à étudier les nombres premiers $2s + 1$ de la forme $8i \pm 3$. Mais tous les nombres de cette forme ne conviennent pas : par exemple, pour $43 = 8.5 + 3$, il y a trois orbites de longueur 14. Le nombre $\upsilon(N)$ d'entiers q premiers inférieurs ou égaux à N tels que 2 soit racine primitive de q a été étudié par Artin ; celui-ci a fait la conjecture suivante [13] : si $\Pi(N)$ désigne le nombre de nombres premiers inférieurs à N, on a :

$$\upsilon(N) \sim \Pi(N).A$$

où A désigne le produit infini pris sur tous les nombres premiers :

$$A = \prod_p (1 - \frac{1}{p(p-1)})$$

Ici, nous avons retrouvé le premier facteur de ce produit, à savoir $(1 - \frac{1}{2})$.

4. Etude de la décomposition en facteurs premiers de $2s + 1$

Soient $2s'+ 1$ un diviseur de $2s + 1$:

$$2s + 1 = \lambda(2s' + 1)$$

et ℓ' la longueur d'une orbite de la permutation définie à partir de $2s' + 1$: il existe un entier i appartenant à $\{1,...,2s'\}$ tel que ℓ' soit le plus petit nombre annulant $i(2^{\ell'} - 1)$ modulo $2s' + 1$; le nombre λi appartient à $\{1,...,2s\}$ et ℓ' est le plus petit entier tel que $\lambda i(2^{\ell'} - 1)$ soit nul modulo $2s + 1$ donc la longueur de l'orbite de λi relativement à la permutation définie par $2s + 1$ est ℓ' : dans les longueurs d'orbites relatives à la permutation définie par $2s + 1$ figurent déjà toutes les longueurs d'orbites relatives aux permutations définies par des diviseurs de $2s + 1$.

Supposons que pour la permutation définie par $2s + 1 = q$ premier, nous ayons α orbites de longueur $L = \frac{q-1}{\alpha}$. Peut-on en déduire des renseignements sur les longueurs des orbites pour la permutation σ_n définie par $q^n = 2S + 1$, où n est un entier positif ?

Soit L_n la longueur de l'orbite de 1 pour la permutation σ_n :

$$2^{L_n} - 1 = 0 \quad (q^n)$$

$$2^{L_n} - 1 = 0 \quad (q) \quad > L \mid L_n$$

$$L_n = \lambda L$$

D'autre part, la relation $2^L - 1 = 0$ (modulo q) entraine :

$$2^{Lq^{n-1}} - 1 = 0 \quad (\text{modulo } q^n)$$

$$\Rightarrow L_n \mid Lq^{n-1}$$

Nous en déduisons que λ est un diviseur de q^{n-1}.

Etudions le cas où n vaut 2 : alors L_2 vaut ou bien L, ou bien Lq ; si L_2 vaut L, nous avons :

$$2^{\frac{q-1}{\alpha}} - 1 = 0 \quad (\text{modulo } q^2)$$

Donc q^2 divise $2^{q-1} - 1$: ceci n'arrive que si q^2 est un nombre de Wieferich, cas tout à fait exceptionnel; écartons donc provisoirement ce cas : alors L_2 vaut L_q.

Montrons que si $2^{Lq^{i-2}} - 1$ n'est pas divisible par q^i, $2^{Lq^{i-1}} - 1$ n'est pas divisible par q^{i+1} :

$$2^{Lq^{i-2}} = 1 + hq^{i-1}$$

où h n'est pas divisible par q ; élevons à la puissance q ; comme q est premier, tous les coefficients binomiaux $\binom{q}{j}$ sont divisibles par q :

$$2^{Lq^{i-1}} = 1 + hq^i + h^2 q^{2i-1} \times \mu$$

où μ est entier ; comme i est supérieur ou égal à 2 , i + 1 est inférieur ou

égal à $2i - 1$; $2^{Lq^{i-1}} - 1$ ne peut pas être divisible par q^{i+1}. Par récurrence, nous obtenons que $2^{Lq^{n-2}} - 1$ ne soit pas divisible par q^n donc L_n est égal à Lq^{n-1}.

Il y a au moins $q^n - q^{n-1}$ nombres appartenant à des orbites de longueur L_n.

Soit λq l'un des $q^{n-1} - q^{n-2}$ nombres divisibles par q et non divisibles par q^2 : q est dans une orbite de longueur L_{n-1}.

Nous avons au moins $q^n - q^{n-1}$ éléments dans des orbites de longueur L_n, au moins $q^{n-1} - q^{n-2}$ dans des orbites de longueur L_{n-1}, et ainsi de suite. Or, il n'y a que $q^n - 1$ éléments donc il y a exactement α orbites de longueur Lq^{n-1}, α orbites de longueur Lq^{n-2}, ..., orbites de longueur L.

PROPRIETE 4 : soit q un nombre premier (> 2) tel que q^2 ne soit pas un nombre de Wieferich ; supposons que la permutation définie à partir de q ait α orbites de longueur $L = \frac{q-1}{\quad}$. Alors la permutation définie à partir de q^n a $n\alpha$ orbites : α de longueur Lq^{n-1}, α de longueur Lq^{n-2}, ..., α de longueur L.

Etudions maintenant le cas où q^2 est un nombre de Wieferich : L_2 vaut L ; toutes les orbites sont de longueur L et elles sont en nombre $\frac{q^2-1}{L} = \alpha(q + 1)$. La généralisation se fait d'une manière analogue : la permutation définie à partir de q^n a αq orbites de longueur Lq^{n-2}, αq de longueur Lq^{n-3}, ..., αq de longueur Lq, $\alpha(q+1)$ de longueur L. Remarquons que ce cas est tout à fait exceptionnel puisqu'il n'existe que deux nombres q inférieurs à 10^6 tels que q^2 soit un nombre de Wieferich ; ce sont :

$q = 1093$ $q = 3511$

PARTIE II

La seconde partie est subdivisée en quatre chapitres et est consacrée à l'étude de dérivations d'un corps K extension purement inséparable d'exposant 1 d'un corps k de caractéristique p non nulle.

Dans le premier chapitre, des rappels concernant la notion de p-base de telles extensions sont d'abord faits : l'existence et les propriétés des p-bases constituent des résultats analogues à ceux relatifs aux bases des espaces vectoriels. Puis sont énoncés deux lemmes : le premier permet de prolonger une dérivation d'un corps L, de noyau k à un corps M de degré p sur L, le degré restant k, le second concerne le noyau d'une dérivation, combinaison linéaire à coefficients dans k des puissances d'une dérivation de noyau k.

Dans le second chapitre, nous définirons une famille de dérivations particulières appelées "bonnes dérivations" lorsque K est de degré au plus dénombrable sur k. Après avoir donné quelques propriétés de ces bonnes dérivations, nous montrerons qu'il en existe toujours et qu'il est possible de faire se correspondre les p-bases et les bonnes dérivations de K sur k. Enfin, nous examinerons quelques problèmes d'extension de bonnes dérivations.

Dans le troisième chapitre sont étudiées de façon systématique les bonnes dérivations lorsque K admet sur k une p-base dénombrable ; lorsque le cardinal de cette p-base est fini et égal à n, le théorème 4 affirme que, D désignant une bonne dérivation, les D^{p^j} ($j = 0, 1, \ldots, n-1$) constituent une base de l'espace vectoriel $\mathcal{Y}$ engendré sur K par les D^{p^j} ($j \geq 0$) et même que $\mathcal{Y}$ est l'algèbre de Lie de toutes les dérivations de K. La connaissance d'une bonne dérivation entraine donc la connaissance de toutes les k-dérivations du corps.

Dans le cas où la p-base de K est infinie dénombrable, le théorème 5 donne des résultats qui étendent ceux du théorème 4 : l'espace vectoriel envisagé est maintenant l'ensemble des séries formelles $\sum_{i=0}^{\infty} a_i D^{p^i}$, $a_i \in K$, qui est aussi l'algèbre de Lie de toutes les k-dérivations de K ; sur $\mathcal{Y}$, les topologies de Krull et des séries formelles sont identiques et tout élément de $\mathcal{Y}$ peut être considéré comme limite d'éléments du plus petit sous espace $\mathcal{Y}_D$ de $\mathcal{Y}$ contenant

D et stable par élévation à la puissance p.

Dans le quatrième chapitre sont étudiées toutes les dérivations de K de noyau k lorsque le degré $[K : k]$ est fini et égal à n : il s'agit bien d'une étude plus générale que celle du chapitre 3 car dans celui-ci, seules les bonnes dérivations, c'est-à-dire telles que D^{p^r} soit nul, intervenaient.

Après avoir donné quelques lemmes généraux sur les dérivations et les liens entre les dérivations et la p-indépendance d'éléments de K, le théorème 6 énoncera une condition nécessaire et suffisante pour qu'une dérivation de K dans K ait exactement k pour noyau : la forme de cette condition montrera en particulier que l'ensemble des dérivations de K dont le noyau est k définit un k-ouvert de Zariski dans l'ensemble des dérivations de K nulles sur k.

Enfin, après avoir généralisé la formule de Barsotti-Cartier, nous reviendrons à l'étude des dérivées logarithmiques : le théorème 7 permettra de caractériser les éléments p de K qui sont dérivées logarithmiques relativement à une dérivation de noyau k : la condition est une équation différentielle du $(p^n - 1)^{ième}$ ordre.

CHAPITRE I

PRELIMINAIRES

A) RAPPELS CONCERNANT LA NOTION DE p-BASE

Soit K un corps de caractéristique p différente de 0, contenant un sous corps k. Supposons que K soit une extension algébrique de k telle que le polynôme minimal de tout élément x de K soit de la forme $X^p - a = 0$, où a est un élément de k : un tel corps K est appelé extension purement inséparable d'exposant 1 de k.

Etant donnée une famille $(\rho_i)_{i \in I}$ d'éléments de K, nous noterons $k(\rho_i)_{i \in I}$ le corps obtenu à partir de k par adjonction des $(\rho_i)_{i \in I}$. Une famille $(\rho_i)_{i \in I}$ d'éléments de K est une p-base de K sur k si elle est p-indépendante sur k (c'est-à-dire si pour toute partie J de I, distincte de I, les corps $k(\rho_i)_{i \in I}$ et $k(\rho_i)_{i \in J}$ sont distincts) et si K est obtenu à partir de k par adjonction des $(\rho_i)_{i \in I}$

PROPRIETE : Toute extension K purement inséparable d'exposant 1 de k admet une p-base $(\rho_i)_{i \in I}$ sur k.

Ceci constitue une propriété classique [5].

Soit $\mathcal{F}$ l'ensemble des familles d'éléments de K p-indépendantes sur k : cet ensemble n'est pas vide car la famille réduite au seul élément ρ de $K - k$ est indépendante sur k, et il est ordonné par inclusion. Nous allons montrer que $\mathcal{F}$ est un ensemble inductif : pour cela, considérons une partie totalement ordonnée de $\mathcal{F}$, soit $(F_\lambda)_{\lambda \in \Lambda}$:

Etudions la famille F définie par :

$$F = \bigcup_{\lambda \in \Lambda} F_\lambda$$

Soit G une partie de F distincte de F : il existe un élément ρ dans $F - G$ donc un indice λ_o dans Λ tel que ρ soit dans F_{λ_o} ; ρ appartient au corps $k(F)$. Notons $G_\lambda = F_\lambda \cap G$; comme l'ensemble des F_λ est totalement ordonné, il en est de même des G_λ et nous avons :

$$k(G) = \bigcup_{\lambda \in \Lambda} k(G_\lambda)$$

Supposons que ρ soit dans $k(G)$: alors il existe un μ dans Λ tel que ρ soit dans $k(G_\mu)$. Comme la famille des F_λ est totalement ordonnée, deux cas sont possibles :

- ou F_{λ_o} est contenu dans F_μ : alors G_μ et $G_\mu \cup \{\rho\}$ sont deux parties distinctes de F_μ qui est p-indépendante donc les corps $k(G_\mu)$ et $k(G_\mu \cup \{\rho\})$ sont distincts ce qui contredit le fait que ρ appartient à $k(G_\mu)$.

- ou F_μ est contenu dans F_{λ_o} : alors G_μ et $G_\mu \cup \{\rho\}$ sont deux parties distinctes de F_{λ_o} et nous aboutissons à la même contradiction. Finalement, l'élément ρ appartient à $k(F) - k(G)$ et la famille F est p-indépendante.

D'après le théorème de Zorn, l'ensemble ordonné inductif $\mathcal{F}$ possède un élément maximal, soit F. Montrons que F constitue une p-base de K, c'est-à-dire que K est égal à $k(F)$: supposons en effet, qu'il existe un élément ρ dans $K - k(F)$. Soit F' la famille $F \cup \{\rho\}$. Pour toute partie G' de F, distincte de F', ou bien G' est contenue dans F et $k(G')$ est contenu dans $k(F)$ donc distinct de $k(F')$, ou bien G' contient ρ donc $G' - \{\rho\}$ est unepartie de F distincte de F : les corps $k(G' - \{\rho\})$ et $k(F)$ sont alors distincts ; comme les degrés de $k(F')$ sur $k(F)$ et de $k(G')$ sur $k(G' - \{\rho\})$ sont égaux et valent p, les corps $k(F')$ et $k(G')$ sont aussi distincts. La famille F' est p-indépendante, ce qui contredit le caractère maximal de F : la famille F constitue donc une p-base de K sur k que nous noterons $(\rho_i)_{i \in I}$.

Montrons que les $\rho_{i_1}^{v_1} \cdots \rho_{i_n}^{v_n}$, où les v_i sont des entiers strictement inférieurs à p, sont linéairement indépendants sur k :

soit $\sum_i \lambda_i \rho_{i_1}^{v_1} \cdots \rho_{i_n}^{v_n} = 0$ une relation de dépendance linéaire ; considérons J :

$$J = \{i_j \mid i_j \in I \; ; \; \lambda_i \neq 0\}$$

C'est une partie finie de I ; fixons N dans J : ρ_N vérifie une équation polynômiale de degré inférieur à p, à coefficients dans $k(\rho_i)_{i \in J - \{N\}}$; or, son polynôme minimal sur k est de degré p donc ρ_N appartient à $k(\rho_i)_{i \in J - \{N\}}$, ce qui contredit la p-indépendance des ρ_i : l'ensemble J est donc vide.

COROLLAIRE :

Pour que I soit fini et égal à $\{1,\ldots,n\}$, il faut et il suffit que le degré de K sur k soit p^n. Les $\rho_1^{v_1} \ldots \rho_n^{v_n}$ $(0 \leq v_i < p)$ constituent alors une base de K sur k.

Comme les $i_1^{v_1} \ldots i_n^{v_n}$, où les v_i sont des entiers strictement inférieurs à p sont linéairement indépendants sur k, deux p-bases différentes ont le même cardinal, ceci en utilisant une propriété analogue des bases des espaces vectoriels.

Remarquons qu'une dérivation D de K dans K, nulle sur k. est entièrement déterminée par la donnée des images par D des éléments d'une p-base de K sur k. De plus, le choix de ces images est entièrement arbitraire.

B) QUELQUES LEMMES CONCERNANT LES DERIVATIONS

Soient K une extension purement inséparable d'exposant 1 de k et $(\rho_i)_{i \in I}$ une p-base de K sur k.

LEMME 1 :

Soient J une partie de I distincte de I et i un élément de $I - J$. Considérons le corps L (resp. M) admettant $(\rho_j)_{j \in J}$ (respectivement $(\rho_j)_{j \in J \cup \{i\}}$) comme p-base sur k. Soient Δ une dérivation de L dans M de noyau k et β un élément de $K - \mathrm{Im}\,\Delta$ tel que :

(1) si $\mathrm{Im}\,\Delta$ est une partie de L, distincte de L, β appartient à L

(2) sinon, β appartient à $K - M$.

Alors Δ peut se prolonger en une dérivation $\bar{\Delta}$ de M dans K de noyau k en posant $\bar{\Delta}(\rho_i) = \beta$.

Considérons la dérivation $\bar{\Delta}$ de M dans K définie par :

$$\bar{\Delta}x = \Delta x \qquad \forall x \in L$$
$$\bar{\Delta}\rho_i = \beta$$

Montrons que le noyau de $\bar{\Delta}$ est k : soit x un élément du noyau de $\bar{\Delta}$; comme M^p est contenu dans le noyau de Δ, nous pouvons supposer que x est un polynôme en ρ_i à coefficients dans L, de degré inférieur à p :

$$x = a_1\rho_i^{p-1} + a_2\rho_i^{p-2} + \ldots + a_{p-1}\rho_i + a_p \qquad a_i \in L$$

$$\bar{\Delta}x = (\Delta a_1)\,\rho_i^{p-1} + \ldots + (a_{p-1})\rho_i + \Delta a_p + \beta\, a_1(p-1)\rho_i^{p-2} + \ldots + a_{p-1}$$

Deux cas sont à distinguer :

(1) On a $\mathrm{Im}(\Delta)$ contenu dans L et l'élément β est dans $L - \mathrm{Im}\Delta$: les ρ_i^j ($j = o, \ldots, p-1$) constituent une base de M sur L ; la nullité de $\bar{\Delta}x$ entraîne:

$$\Delta a_1 = 0$$
$$a_j\beta(p-j) + \Delta a_{j+1} = 0 \qquad j = 1, \ldots, p-1$$

Comme le noyau de Δ est k, l'élément a_1 est dans k.

$$\Delta a_2 = - a_1 (p-1)\,\beta$$

Comme β a été choisi dans $L - \mathrm{Im}\Delta$, il ne peut être l'image par Δ de $-\dfrac{a_2}{a_1(p-1)}$

donc a_1 est nul : l'élément a_2 est alors dans k. De proche en proche, nous démontrons ainsi que :

$$a_1 = a_2 = \ldots = a_{p-1} = \Delta a_p = 0$$

$$\Delta a_p = 0 \Longrightarrow a_p \in k$$

L'élément x est égal à a_p donc appartient à k : le noyau de $\bar{\Delta}$ est bien k.

(2) L'élément β est dans $K - M$

Comme $(\Delta a_1)\rho_i^{p-1} + \ldots + (a_{p-1})_i + a_p$ appartient à M et que β est dans $K - M$, la nullité de $\bar{\Delta}x$ entraîne celle de $a_1 (p-1)\rho_i^{p-2} + \ldots + a_{p-1}$ et l'indépendance des ρ_i^j $(j = 0, \ldots, p-2)$ sur L montre que :

$$a_1 = a_2 = \ldots = a_{p-1} = 0$$

L'élément x est donc égal à a_p : il appartient au noyau de Δ qui est k.

LEMME 2

Soient Δ une dérivation de K de noyau k et Γ une combinaison linéaire à coefficients dans K de $1, \Delta, \ldots, \Delta^m$:

$$\Gamma = a_m\Delta^m + a_{m-1}\Delta^{m-1} + \ldots + a_1\Delta + a_o 1 \qquad a_i \in K$$

Supposons a_m différent de 0. Alors, la dimension sur k du noyau de Γ est au plus égale à m.

Si ker Γ est réduit à 0, le résultat est établi. Sinon, soit α_o un élément non nul de ker Γ. Considérons l'élément x_1 de K défini par :

$$x = \alpha_o x_1$$

où x désigne un élément quelconque de ker Γ. Comme $\Gamma(\alpha_o x_1)$ est nul, nous avons :

$$a_m\Delta^m(\alpha_o x_1) + \ldots + a_o\,\alpha_o x_1 = 0$$

Comme Δ est une dérivation, chacune des quantités $\Delta^i(\alpha_o x_1)$ peut être calculé grâce à la formule de Leibnitz :

$$\Delta^i (\alpha_o x_1) = \sum_{l=o}^{i} \binom{i}{l} \Delta^l (\alpha_o)\Delta^{i-l} (x_1)$$

La relation $\Gamma(\alpha_o x_1) = 0$ peut donc s'écrire sous la forme :

$$b_m\Delta^m (x_1) + b_{m-1}\Delta^{m-1} (x_1) +\ldots+ b_1\Delta(x_1) + b_o x_1 = 0$$

où les b_i sont des éléments de K. Calculons b_m :

$$b_m = \alpha_o a_m$$

Il est toujours non nul. Calculons b_o :

$$\begin{aligned} b_o &= a_m\Delta^m (\alpha_o) + a_{m-1}\Delta^{m-1} (\alpha_o) +\ldots+ a_1\Delta(\alpha_o) + a_o\alpha_o \\ &= \Gamma(\alpha_o) \end{aligned}$$

Comme l'élément α_o a été choisi dans le noyau de Γ , le coefficient b_o est nul.

Considérons alors l'application Γ_{m-1} de K dans K définie par :

$$\Gamma_{m-1} = b_m\Delta^{m-1} + b_{m-1}\Delta^{m-2} +\ldots+ b_2\Delta + b_1$$

Cette application est du même type que l'application Γ mais elle est de degré m-1 par rapport à Δ. L'élément Δx_1 appartient au noyau de l'application Γ_{m-1}, autrement dit x_1 s'obtient à partir d'un élément du noyau de Γ_{m-1} par "intégration". Il en résulte que :

$$\dim \ker \Gamma \leq 1 + \dim \ker \Gamma_{m-1}$$

Le raisonnement se poursuit de proche en proche : ou bien nous arrivons à une application Γ_1 (avec 1 positif) dont le noyau est réduit à 0 et nous obtenons :

$$\dim \ker \Gamma \leq m - 1 + \dim \ker \Gamma_1$$

$$\dim \ker \Gamma \leq m - 1$$

ou bien aucune des applications Γ_1 (avec 1 positif) n'a son noyau réduit à 0 et

et nous obtenons :

$$\dim \ker \Gamma \leq m + \dim \ker \Gamma_o$$

L'application Γ_o est une homothétie de rapport non nul donc son noyau est réduit à 0. Dans tous les cas, nous obtenons bien :

$$\dim \ker \Gamma \leq m.$$

CHAPITRE II

NOTION DE BONNES DERIVATIONS

Dans tout ce chapitre, nous considèrerons un corps K de caractéristique p différente de 0, extension purement inséparable d'exposant 1 de k, le degré de K sur k étant au plus dénombrable.

A - DEFINITION DES BONNES DERIVATIONS

Une dérivation D de K est appelée bonne dérivation de K sur k si et seulement si :

$$\left[\ker D^{p^i} : k\right] = \inf\left(p^i, \left[K : k\right]\right)$$

pour $i = 0, 1, \ldots$ et si $K = \bigcup_{i=o}^{\infty} \ker D^{p^i}$

Faisant $i = 0$, il en résulte immédiatement que le noyau de D est le corps k.

Nous noterons K_i le corps $\ker D^{p^i}$.

CONSEQUENCES DE LA DEFINITION

(1) Soit D une dérivation de K. Pour que D soit une bonne dérivation de K sur k, il suffit que les deux conditions suivantes soient réalisées :

a) $\ker D = k$

b) $\left[K_i : k\right] \geq \inf\left(p^i, \left[K : k\right]\right)$ et $K = \bigcup_{i=o}^{\infty} K_i$

En effet, d'après le lemme 2, le degré de K_i sur k est inférieur ou égal à p^i d'où le résultat.

(2) Si D est une bonne dérivation de K sur k et si $i \leq j$, D^{p^i} est une bonne dérivation de K_j sur K_i.

Si p^i est supérieur ou égal à $\left[K : k\right]$, les corps K_i et K_j sont égaux à K ; D^{p^i} est la dérivation nulle et le résultat est trivial.

Supposons p^i strictement inférieur à $\left[K : k\right]$; alors, le noyau de D^{p^i} est bien K_i.

$$\left[\ker (D^{p^{i+1}}) : k\right] = \inf\left(p^{i+1}, \left[K : k\right]\right)$$

$$\left[\ker (D^{p^{i+1}}) : K_i\right] = \inf\left(\frac{p^{i+1}}{\left[K_i : k\right]}, \left[K : K_i\right]\right)$$

$$\geq \inf\left(p^1, \left[K_j : K_i\right]\right)$$

La conséquence (1) entraîne alors le résultat.

(3) Si D est une bonne dérivation de K sur k, nous avons :

$$\left[\ker D^i : k\right] = \inf\left(i, \left[K : k\right]\right)$$

Il existe un entier ℓ tel que :

$$p^\ell \leq i < p^{\ell+1}$$

Si nous avions $\ker D^i = \ker D^{i+1}$, nous aurions :

$$\ker D^i = \ker D^{i+1} = \ldots = \ker D^{p^{\ell+1}}$$

Or le degré de $\ker D^{p^{\ell+1}}$ sur k est $p^{\ell+1}$ tandis que celui de $\ker D^i$ est inférieur ou égal à i (d'après le lemme 2) donc les $\ker D^i$ (i = 1,...) constituent une suite d'espaces vectoriels sur k emboités, tous distincts. Les trois relations:

$$\left[\ker D^{p^\ell} : k\right] = p^\ell$$

$$\left[\ker D^{p^{\ell+1}} : k\right] = p^{\ell+1}$$

$$\left[\ker D^{p^i} : k\right] \leq i$$

entraînent alors l'égalité : $\left[\ker D^{p^i} : k\right] = i$.

(4) Si $\left[K : k\right] = p^n$, une dérivation D de K est bonne si et seulement si $\ker D \supset k$ et D^{p^n} est la dérivation nulle.

- Si D est une bonne dérivation, nous avons :

$$\{K_i : k\} = \inf (p^i, p^n)$$

Pour tout i supérieur ou égal à n, K_i est égal à K donc D^{p^i} est la dérivation nulle.

- Si D est une dérivation de noyau k telle que D^{p^n} soit la dérivation nulle, nous avons déjà $\{K_i : k\} = \inf (p^i, p^n)$ pour tout i supérieur ou égal à n. D'autre part, $\left[K_{i+1} : K_i\right]$ est inférieur ou égal à p (d'après le lemme 2). Comme $\left[K_n : k\right]$ est égal à p^n, $\left[K_{i+1} : K_i\right]$ est égal à p donc $\left[K_i : k\right] = p^i$ pour tout i inférieur ou égal à n.

(5) Si K est de degré infini dénombrable sur k, D est une bonne dérivation si et seulement si :

a) $\left[K_i : k\right] = p^i \qquad i = 0, 1, \ldots$

b) pour tout x dans K, il existe n tel que $D^{p^n} x = 0$.

(6) Pour tout i supérieur ou égal à 1, $D(\ker D^{i+1}) = \ker D^i$

- Si x appartient à $\ker D^{i+1}$, nous avons :

$$D^i (Dx) = D^{i+1} x = 0$$

Nous avons donc :

$$D(\ker D^{i+1}) \subset \ker D^i \subset \ker D^{i+1}$$

- Comme le noyau de D est k, $D(\ker D^{i+1})$ est un k-espace vectoriel de dimension i ; de même, $\ker D^i$ est de dimension i : il en résulte que ces deux espaces vectoriels sont égaux. Si K est de degré infini dénombrable sur k, toute bonne dérivation D est surjective : en effet pour tout x dans K, il existe n tel que x appartienne à K_n.

$$K_n = D(\ker D^{p^n + 1})$$

Il en résulte que x est l'image d'un élément de $\ker D^{p^n + 1}$

(7) Si D est une bonne dérivation de K sur k, il existe une base $(e_i)_{i \in I}$ de K considéré comme espace vectoriel sur k telle que :

$$De_1 = e_o = 1 \quad \text{et} \quad De_i = e_{i-1} \quad \text{pour } i \geq 2 \quad (\text{d'où } D^i e_i = 1,\ i \geq 1)$$

et si $y_i = e_{p^i}$ $(i \geq o)$, les y_i constituent une p-base de K sur k.

- D'après la conséquence (6), k est égal à D (ker D^2) donc il existe un élément e_1 dans ker D^2 tel que $De_1 = 1$. Comme e_1 n'est pas dans k, les éléments $(1, e_1)$ constituent une k-base de ker D^2.

- Soit $(e_o = 1, e_1, \ldots, e_n)$ une k-base de ker D^{n+1} telle que :

$$De_i = e_{i-1} \qquad i \geq 1$$

Comme ker D^{n+1} = D (ker D^{n+2}), il existe un élément e_{n+1} dans ker (D^{n+2}) tel que $De_{n+1} = e_n$. Il est clair que $(e_o = 1, e_1, \ldots, e_{n+1})$ constituent une base de ker D^{n+2}. Le résultat est ainsi établi par récurrence.

- Comme $D^{p^i}(y_i) = 1$, tout y_i appartient à $K_{i+1} - K_i$ donc y_i est une p-base de K_{i+1} sur K_i ; l'ensemble des y_i constitue donc une p-base de K sur k.

B - EXISTENCE DE BONNES DERIVATIONS

THEOREME 1. : Soit K_i $(i = 0, 1, \ldots)$ une suite de sous corps de K de degré inf inf $(p^i, [K : k])$ sur k telle que $K = \bigcup_{i=0}^{\infty} K_i$. Alors, il existe une dérivation D de K telle que $\ker D^{p^i} = K_i$.

Pour $i \geq 1$, choisissons une p-base ρ_i de K_i sur K_{i-1} chaque fois que K_{i-1} est différent de K_i : alors, les $(\rho_i)_{i \in I}$ ainsi obtenus constituent une p-base de K sur k (I est fini si $[K : k]$ l'est).

- Le lemme 1 permet d'affirmer l'existence d'une dérivation D_1 de K_1 dans K_1 prolongeant la dérivation nulle de k dans k, le noyau de D_1 étant k, en choisissant $D_1\rho_1 = \beta_1$ dans $k - \{0\}$. Comme l'application D_1^2 est nulle sur ρ_1 et que tout élément de K_1 peut s'écrire sous la forme d'un polynôme en ρ_1 à coefficients dans k, de degré inférieur ou égal à $p-1$, la dérivation D_1^p est nulle sur K_1.

Calculons $D_1^{p-1}(\rho_1^{p-1})$; la formule de Leibniz donne :

$$D_1^{p-1}(\rho_1^{p-1}) = (p-1)\,!\,(D_1\rho_1)^{p-1}$$
$$= (p-1)\,!\,(\beta_1)^{p-1}$$

- Supposons construite une dérivation D_n de K_n dans K_n telle que $\ker D_n^{p^i} = K_i$ pour i inférieur ou égal à n, et que $D_n^{p^i-1}(\rho_1^{p-1} \ldots \rho_n^{p-1}) = \gamma_n$ soit dans $k - \{0\}$. Si K_n est égal à K, nous pouvons prendre $D_n = D$ et le problème est résolu. Sinon, le lemme 1 montre que la dérivation D_n peut se prolonger en une dérivation D_{n+1} de K_{n+1} dans K_{n+1} en choisissant $D_{n+1}\rho_{n+1} = \beta_{n+1}$ dans $K_n - \operatorname{Im} D_n$. Montrons que nous pouvons prendre $\beta_{n+1} = \rho_1^{p-1} \ldots \rho_n^{p-1}$: c'est bien un élément de K_n ; supposons qu'il existe un élément y dans K_n tel que :

$$\rho_1^{p-1} \ldots \rho_n^{p-1} = D_n y$$

Appliquant $D_n^{p^n-1}$, nous obtenons :

$$\gamma_n = D_n^{p^n} y.$$

Comme la dérivation $D_n^{p^n}$ est nulle sur K_n et que γ_n est différent de 0, nous aboutissons à une contradiction.

Choisissons donc $\beta_{n+1} = \rho_1^{p-1} \dots \rho_n^{p-1}$. La dérivation D_{n+1} ainsi obtenue a pour noyau k. Comme $1, \rho_{n+1}, \dots, \rho_{n+1}^{p-1}$ constituent une base de K_{n+1} sur K_n, pour prouver que la dérivation $D_{n+1}^{p^{n+1}}$ est nulle sur K_{n+1}, il suffit de voir que $D_{n+1}^{p^{n+1}}(\rho_{n+1})$ est nul :

$$\begin{aligned} D_{n+1}^{p^{n+1}}(\rho_{n+1}) &= D_{n+1}^{p^{n+1}-1}(\beta_n) \\ &= D_{n+1}^{p^{n+1}-p^n}(\gamma_n) \\ &= 0 \end{aligned}$$

D'après la conséquence (4), D_{n+1} est une bonne dérivation de K_{n+1} donc :

$$\ker D_{n+1}^{p^i} = K_i$$

pour i inférieur ou égal à n+1.

Calculons maintenant $D_{n+1}^{p^{n+1}-1}(\rho_1^{p-1} \dots \rho_n^{p-1} \rho_{n+1}^{p-1})$; comme la dérivation $D_n^{p^n}$ est nulle sur K_n, nous avons :

$$\begin{aligned} D_{n+1}^{p^n}(\rho_1^{p-1} \dots \rho_{n+1}^{p-1}) &= \rho_1^{p-1} \dots \rho_n^{p-1} D_{n+1}^{p^n}(\rho_{n+1}^{p-1}) \\ &= (p-1)\gamma_n \rho_1^{p-1} \dots \rho_n^{p-1} \rho_{n+1}^{p-2} \end{aligned}$$

Appliquons $p-1$ fois la dérivation $D_{n+1}^{p^n}$ à l'élément $\rho_1^{p-1} \dots \rho_n^{p-1} \rho_{n+1}^{p-1}$:

$$D^{p^{n+1}-p^n}_{n+1}\,(\rho_1^{p-1}\ldots\rho_{n+1}^{p-1}) = (p-1)\,!\,\partial`^{p-1}_n\ \rho_1^{p-1}\ldots\rho_n^{p-1}$$

Faisons agir maintenant l'application $D^{p^n-1}_{n+1}$:

$$D^{p^{n+1}-1}_{n+1}\,(\rho_1^{p-1}\ldots\rho_{n+1}^{p-1}) = (p-1)\,!\,\partial`^{p-1}_n\ D^{p^n-1}_{n+1}\,(\rho_1^{p-1}\ldots\rho_n^{p-1})$$

$$= (p-1)\,!\,\partial`^{p}_n$$

L'élément $\partial`_{n+1} = (p-1)\,!\,\partial`^{p}_n$ est bien dans $k - \{0\}$: les hypothèses de récurrence sont bien reconduites et nous obtenons finalement une dérivation D de K ayant les propriétés requises et telle que :

$$D^{p^n-1}\,(\rho_1^{p-1}\ldots\rho_n^{p-1}) = \beta_1^{p^n-1}\,\left[(p-1)\,!\right]^{1+p+\ldots+p^{n-1}}$$

Il est clair que la dérivation ainsi construite est une bonne dérivation de K sur k.

COROLLAIRE 1 :

Il existe des bonnes dérivations de K sur k.

En effet, soit $(\rho_i)_{i\in I}$ une p-base de K sur k où I désigne une partie de N. Considérons la suite de son corps K_i :

$$K_i = k\,(\rho_1, \ldots, \rho_i)$$

Ces sous corps K_i vérifient les hypothèses du théorème 1 donc il existe une bonne dérivation D de K telle que $\ker D^{p^i} = K_i$.

COROLLAIRE 2 :

Pour toute extension E de k de hauteur 1, il existe une dérivation de noyau k.

Par suite du corollaire 1, seul le cas de degré infini non dénombrable demande une démonstration.

Soit $(\rho_i)_{i \in I}$ une p-base de E sur k : comme toutes les p-bases ont le même cardinal, l'ensemble I est infini non dénombrable. D'après le théorème de Zermelo, l'ensemble I peut être muni d'une relation de bon ordre sans plus grand élément :

$$\rho_1, \cdots, \rho_n, \cdots, \rho_w, \rho_{w+1}, \cdots, \rho_{w+n}, \cdots, \rho_{w'}, \cdots$$

Appliquons le lemme 1 en prenant pour J l'ensemble vide et pour ρ_i l'élément ρ_1 : il existe une dérivation D :

$$D : k(\rho_1) \longrightarrow k(\rho_1, \rho_2)$$

de noyau k, définie en choisissant :

$$D\rho_1 = \rho_2^{p-1}$$

Soit maintenant J l'ensemble des éléments de I strictement inférieurs à i. Les notations étant celles du lemme 1, toute dérivation de L dans M de noyau k peut se prolonger en une dérivation D de M dans K en choisissant par exemple $D\rho_i = \rho_{i+1}^{p-1}$. Le principe de récurrence transfinie nous permet alors d'affirmer l'existence d'une dérivation D de K dans K de noyau k.

Remarque : La dérivation D ainsi construite n'est pas surjective. Nous allons montrer que ρ_1^{p-1} n'est la dérivée d'aucun élément de K. Supposons en effet qu'il existe un élément x dans K tel que :

$$Dx = \rho_1^{p-1}$$

Il existe une partie finie J de I, contenant n éléments, telle que x appartienne au corps A_n admettant $(\rho_i)_{i \in J}$ comme p-base sur k. Ordonnons J grâce à la relation de bon ordre :

$$J = \{i_1, i_2, \cdots, i_n\}$$

Comme $D\rho_j$ est différent de ρ_1^{p-1} pour tout j, l'indice 1 figure dans J et nous avons $i_1 = 1$. Soit A'_n le corps admettant $(\rho_i)_{i \in J-\{1\}}$ comme p-base sur k : alors, A_n est un espace vectoriel sur A'_n admet tant pour base ρ_1^j $(j=0,1,..,p-1)$ donc x peut s'écrire :

$$x = a_1 \rho_1^{p-1} + \ldots + a_{p-1} \rho_1 + a_p \qquad a_i \in A'_n$$

Etudions Dx : d'une part, c'est ρ_1^{p-1} ; d'autre part, nous avons :

$$Dx = \rho_2^{p-1} \quad (p-1)\, a_1 \rho_1^{p-2} + \ldots + a_{p-1} \quad + (Da_1)\, \rho_1^{p-1} + \ldots + Da_p$$

En identifiant les coefficients de ρ_1^{p-1}, nous obtenons :

$$Da_1 = 1$$

Soit A'_j le corps admettant $\rho_{i_2}, \ldots, \rho_{ij}$ comme p-base sur k ; l'élément a_1 peut s'écrire :

$$a_1 = \alpha_1^1 \rho_{i_n}^{p-1} + \alpha_2^1 \rho_{i_n}^{p-2} + \ldots + \alpha_p^1$$

où les α_i^1 appartiennent à A'_{n-1}.

La condition $Da_1 = 1$ donne :

$$D\alpha_p^1 = 1$$

$$(p-1)\, \alpha_1^1 \rho_{i_n}^{p-2} + \ldots + \alpha_{p-1}^1 = 0$$

L'indépendance des $\rho_{i_n}^j$ $(j = 0, \ldots, p-1)$ sur A'_{n-1} montre que α_i^1 est nul pour $i = 1, \ldots, p-1$ et a_1 appartient à A'_{n-1}. De proche en proche, nous démontrons ainsi que a_1 est dans $A'_{n-2}, \ldots, A'_2$ et finalement dans k, ce qui est impossible, car Da_1 n'est pas nul.

C - PROBLEME RECIPROQUE

Revenons au cas où le degré de K sur k est au plus dénombrable. Etant donnée une p-base $(\rho_i)_{i \in I}$ de K sur k, nous savons lui associer une bonne dérivation D telle que :

$$(I) \begin{cases} \ker D^{p^i} = k(\rho_1, \ldots, \rho_i) \\ D\rho_i = \rho_1^{p-1} \ldots \rho_{i-1}^{p-1} \qquad i > 1 \; ; \; D\rho_1 \in k - \{0\} \end{cases}$$

Réciproquement, étant donnée une bonne dérivation D de K sur k, peut-on lui associer une p-base telle que les relations (I) soient satisfaites ?

THEOREME 2

Soient D une bonne dérivation de K sur k, K_i les corps $\ker D^{p^i}$. Alors, il existe une p-base $(\rho_i)_{i \in I}$ de K sur k telle que les relations (I) soient satisfaites.

- D'après la conséquence (6) de la définition des bonnes dérivations, k est contenu dans $D(K_1)$ donc il existe un élément ρ_1 dans K_1 tel que $D\rho_1$ soit un élément non nul de k.

- La démonstration se poursuit par récurrence : supposons construite une p-base $\rho_1, \ldots, \rho_n$ de K_n sur k telle que :

$$K_i = k(\rho_1, \ldots, \rho_i)$$
$$D\rho_i = \rho_1^{p-1} \ldots \rho_{i-1}^{p-1} \qquad n \geq i > 1$$

D'après la conséquence (6), le corps K_n est contenu dans $D(K_{n+1})$ donc il existe un élément ρ_{n+1} dans K_{n+1} tel que :

$$D\rho_{n+1} = \rho_1^{p-1} \ldots \rho_n^{p-1}$$

D'après un calcul fait lors de la démonstration du théorème 1, $D^{p^n}(\rho_1^{p-1} \ldots \rho_n^{p-1})$ est différent de 0 donc ρ_{n+1} n'appartient pas à K_n. Il en résulte que ρ_{n+1}

est une p-base de K_{n+1} sur K_n donc les hypothèses de récurrence sont reconduites. Une fois ρ_1 choisi, les autres ρ_i sont déterminés modulo un élément de k. Quant à ρ_1, il y a Card $(k - \{0\})$ possibilités.

D - PROBLEMES D'EXTENSION DE BONNES DERIVATIONS

PROPRIETE 1

Soit L une sous extension de K de degré fini p^n sur k. Toute bonne dérivation D de L sur k se prolonge en une bonne dérivation de K sur k.

Soit $\rho_1, \ldots, \rho_n$ une p-base de L sur k associée à la bonne dérivation D comme il a été fait dans le théorème 2 ; la p-base $\rho_1, \ldots, \rho_n$ peut se compléter en une p-base $(\rho_i)_{i \in I}$ de K sur k. Prolongeons la dérivation D à k en posant :

$$D\rho_i = \rho_1^{p-1} \ldots \rho_{i-1}^{p-1}$$

Nous savons (corollaire 1 du théorème 1) que la dérivation ainsi abtenue est une bonne dérivation.

PROPRIETE 2

Soit L une sous extension de K de degré infini sur k avec L distinct de K. Il n'existe pas de prolongement d'une bonne dérivation D de L sur k en une bonne dérivation de K sur k.

Supposons qu'il existe un tel prolongement $\bar{D}$ de D. Soit ρ un élément de K - L : alors, il existe un entier n tel que $\bar{D}^{p^n} \rho$ soit nul.

$$\ker D^{p^n} \subset \ker \bar{D}^{p^n}$$

$$\left[\ker D^{p^n} : k\right] = p^n$$

Il en résulte que $\left[\ker \bar{D}^{p^n} : k\right]$ est supérieur à p^n, ce qui contredit la définition

d'une bonne dérivation.

PROPRIETE 3

Soit L une sous extension de K de degré fini p^n sur k. Pour toute bonne dérivation Δ de K sur L et toute bonne dérivation D de L sur k, il existe une bonne dérivation $\bar{D}$ de K sur k telle que $\Delta = \bar{D}^{p^n}$ qui prolonge D.

D'après la remarque (7) qui suit la définition d'une bonne dérivation, il existe une base (e_i) de K considéré comme espace vectoriel sur L telle que :

$$e_o = 1 \qquad \Delta e_i = e_{i-1} \qquad i \geq 1$$

et si $y_i = e_{p^i}$ $(i \geq 1)$, les (y_i) constituent une p-base de K sur L.

- Soit D une bonne dérivation quelconque de L sur k. Utilisant à nouveau la remarque (7), nous savons qu'il existe un élément a_o dans L tel que :

$$D^{p^n-1}(a_o) = 1$$

Posons alors $\bar{D}(y_o) = a_o$. La dérivation D se trouve ainsi prolongée en une dérivation du corps $L(y_o)$ admettant y_o comme p-base sur L.

La dérivation D^{p^n} est nulle sur L ;

$$D^{p^n}(y_o) = 1 = \Delta e_1 = \Delta y_o$$

Comme le noyau de $\bar{D}^{p^n}$ n'est pas $L(y_o)$, nous avons :

$$\ker \bar{D}^{p^n} = L$$

$$\ker \bar{D}^{p^{n+1}} = L(y_o)$$

Il en résulte que $\bar{D}$ est une bonne dérivation de $L(y_o)$ sur k telle que $\bar{D}^{p^n}$ coïncide avec Δ.

- Supposons que nous ayons pu prolonger D en une bonne dérivation $\bar{D}$ de $L(y_o, \ldots, y_i)$ sur k telle que $\bar{D}^{p^n}$ coïncide avec Δ et que $L(y_o,\ldots,y_{i-1})$ soit

le noyau de $\bar{D}^{p^{n+i-1}}$. Considérons l'élément $e = e_{p^{i+1}-1}$ de $L(y_o,\ldots,y_i)$. Par définition, nous avons :

$$\Delta^{p^{i+1}-1}(e) = 1$$

Donc x appartient à $\ker \bar{D}^{p^{n+i+1}-p^n+1}$. Par application de la remarque (6), nous en déduisons l'existence d'un élément a_{i+1} dans $L(y_o,\ldots,y_i)$ tel que :

$$\bar{D}^{p^n-1}(a_{i+1}) = e$$

Prolongeons $\bar{D}$ en une dérivation de $L(y_o,y_1,\ldots,y_{i+1})$ en posant :

$$\bar{D}y_{i+1} = a_{i+1}$$

Alors, le noyau de $\bar{D}$ reste k et $\bar{D}^{p^{n+i+2}}$ est la dérivation nulle, donc $\bar{D}$ est une bonne dérivation de $L(y_o,y_1,\ldots,y_{i+1})$ sur k. Calculons $\bar{D}^{p^n}(y_{i+1})$:

$$\bar{D}^{p^n}(y_{i+1}) = e$$

Or par définition de la base (e_i), nous avons :

$$\Delta(y_{i+1}) = e$$

Les dérivations Δ et $\bar{D}^{p^n}$ coïncident sur $L(y_o, y_1,\ldots,y_{i+1})$ et le résultat annoncé est démontré par récurrence.

CHAPITRE III

ETUDE DETAILLEE D'UNE "BONNE DERIVATION"

Dans ce paragraphe, nous allons étudier l'espace vectoriel $\mathcal{J}$ engendré par $D, D^p, \ldots, D^{p^n}, \ldots$ sur K, lorsque D est une "bonne dérivation".

RAPPEL

Soit E un corps de caractéristique p non nulle. Considérons un ensemble $\mathfrak{D}$ de dérivations de E vérifiant les propriétés suivantes :

(i) $D_1 \in \mathfrak{D}$, $D_2 \in \mathfrak{D} \Longrightarrow D_1 + D_2 \in \mathfrak{D}$

(ii) $D_1 \in \mathfrak{D}$, $D_2 \in \mathfrak{D} \Longrightarrow [D_1, D_2] = D_1D_2 - D_2D_1 \in \mathfrak{D}$

(iii) $D \in \mathfrak{D} \Longrightarrow D^p \in \mathfrak{D}$

(iv) $D \in \mathfrak{D}$, $a \in E \Longrightarrow aD \in \mathfrak{D}$

Un tel ensemble $\mathfrak{D}$ est une p-algèbre de Lie de dérivations de E.

Enonçons le théorème de Jacobson [6] : soit E un corps de caractéristique p non nulle. Considérons une p-algèbre de Lie $\mathfrak{D}$ de dérivations de E, de degré fini ℓ sur E. Soit F le sous corps des $\mathfrak{D}$ -constantes de E (c'est-à-dire l'ensemble des éléments x de E tels que, pour toute dérivation D de $\mathfrak{D}$, l'élément Dx est nul). Alors :

(1) Le corps E est une extension purement inséparable d'exposant 1 de F et le degré de E sur F est p^{ℓ}.

(2) Toute F-dérivation de E appartient à $\mathfrak{D}$

(3) Si $D_1, D_2, \ldots, D_\ell$ constituent une base de $\mathfrak{D}$ sur E, les $D_1^{\nu_1} D_2^{\nu_2} \ldots D_\ell^{\nu_\ell}$ $(0 \leq \nu_i < p \; ; \; D_i^0 = 1)$ constituent une base de l'anneau des transformations F-linéaires de E, considéré comme espace vectoriel sur E.

A - LE CORPS K EST DE DEGRE FINI SUR k

Soit p^n le degré de K sur k. Soit D une bonne dérivation de K sur k et $(\rho_1,\ldots,\rho_n)$ une p-base de K sur k associée à D comme il a été dit au chapitre II - C.

Soit $\mathcal{Y}$ l'espace vectoriel engendré par $D, D^p, \ldots, D^{p^n}, \ldots$ sur K.

THEOREME 3 :

Si K est de degré p^n sur k, alors :

(1) $\mathcal{Y}$ est un K-espace vectoriel de dimension n et les dérivations $D, D^p, \ldots, D^{p^{n-1}}$ constituent une base de $\mathcal{Y}$

(2) $\mathcal{Y}$ est une p-algèbre de Lie contenant toutes les k-dérivations de K.

D'après la construction de D, la dérivation D^{p^n} est nulle donc il en est de même pour toutes les dérivations D^{p^j} avec j supérieur à n. Soit m le plus petit entier tel que $D, D^p, \ldots, D^{p^m}$ soient linéairement dépendantes sur K. Nous pouvons alors écrire :

$$D^{p^m} = \alpha_1 D^{p^{m-1}} + \alpha_2 D^{p^{m-2}} + \ldots + \alpha_m D$$

où les α_i sont des éléments de K. Comme D^{p^n} est nul et que D ne l'est pas, l'entier m vérifie :

$$n \geq m$$

Appliquons la dérivation D^{p^m} à ρ_1^{p-1} :

$$D^{p^j}(\rho_1^{p-1}) = 0 \quad \text{si } j \geq 1$$

$$D(\rho_1^{p-1}) = (p-1)\,\rho_1^{p-2}\,(D\rho_1)$$

Nous en déduisons la nullité de α_m. Etudiant successivement les images par D^{p^m} de ρ_1^{p-1} ρ_2^{p-1}, ..., $(\rho_1^{p-1}\rho_2^{p-1}\ldots\rho_i^{p-1})$, nous démontrons que tous les α_i sont nuls en utilisant le fait que D^{p^j} $(\rho_1^{p-1}\ldots\rho_i^{p-1})$ est nul si j est supérieur ou égal à i, mais est différent de zéro si j vaut $i-1$. La dérivation D^{p^m} est nulle. Or si m était inférieur à n, nous aurions :

$$D^{p^m}(\rho_1^{p-1}\ldots\rho_{m+1}^{p-1}) \neq 0$$

Nécessairement, les entiers m et n sont égaux et les n générateurs D, D^p,... D, D^p, ..., $D^{p^{n-1}}$ de $\mathcal{G}$ sont linéairement indépendants sur K : ils constituent donc une base de $\mathcal{G}$ qui est bien un K-espace vectoriel de dimension n.

Soient Δ et Δ' deux éléments de $\mathcal{G}$; calculons $[\Delta,\Delta']$ en utilisant la formule de Leibnitz :

$$\Delta = \sum_{i=o}^{n-1} a_i D^{p^i} \qquad a_i \in K$$

$$\Delta' = \sum_{j=o}^{n-1} b_j D^{p^j} \qquad b_j \in K$$

$$[\Delta,\Delta'] = \sum_{i=o}^{n-1}\sum_{j=o}^{n-1} (a_i D^{p^i}(b_j).D^{p^j} - b_j D^{p^j}(a_i).D^{p^i})$$

La dérivation $[\Delta,\Delta']$ est encore dans $\mathcal{G}$ donc $\mathcal{G}$ est une algèbre de Lie.

Soit $\mathcal{G}'$ la p-algèbre de Lie engendrée par $\mathcal{G}$: c'est un K-espace vectoriel de dimension N. Considérons le sous corps k' des $\mathcal{G}'$-constantes de K : comme k est le sous corps de $\mathcal{G}$-constantes de K, le corps k' est contenu dans k. D'autre part, comme $\mathcal{G}'$ est la p-algèbre de Lie engendrée par $\mathcal{G}$, toute dérivation de $\mathcal{G}'$ est nulle sur k donc les corps k et k' coïncident. Appliquons alors le théorème de Jacobson : le corps K est de degré p^N sur $k = k'$ donc N est égal à n et $\mathcal{G}$ et $\mathcal{G}'$ coïncident : $\mathcal{G}$ est alors une p-algèbre de Lie. Appliquant à nouveau le théorème de Jacobson, nous voyons que toute k-dérivation de K appartient à $\mathcal{G}$ et que les D^j $(0 \leq j < p^m$; $D^\circ = 1)$ constituent une base de l'anneau des transformations k-linéaires de K, considéré comme espace vectoriel sur K.

B - LE CORPS K EST DE DEGRE INFINI DENOMBRABLE SUR k

Soit D une bonne dérivation de K sur k et $(\rho_i)_{i \in N}$ une p-base de K sur k associée à la bonne dérivation D comme il a été expliqué au chapitre II - C.

PROPRIETE

Les dérivations D, D^p, ..., D^{p^m},... sont linéairement indépendantes sur K.

Soit m le plus petit entier tel qu'il existe une relation de la forme :

$$D^{p^m} = \alpha_1 D^{p^{m-1}} + \ldots + \alpha_{m-1} D^p + \alpha_m D$$

où les α_i sont des éléments de K. Comme dans la démonstration de la première partie du théorème 4, appliquons successivement D^{p^m} à ρ_1^{p-1}, $(\rho_1\rho_2)^{p-1}$,...,$(\rho_1\rho_2\ldots\rho_i)^{p-1}$ Utilisant le fait que $D^{p^j}(\rho_1^{p-1}\ldots\rho_i^{p-1})$ est nul si j est supérieur ou égal à i mais est différent de 0 si j est égal à i-1, nous montrons que tous les α_i sont nuls, donc que la dérivation D^{p^m} est nulle. Or, par la construction même de D, nous avons :

$$D^{p^m}(\rho_1^{p-1} \ldots \rho_{m+1}^{p-1}) \neq 0$$

Nous aboutissons à une contradiction donc les dérivations D, D^p, D^{p^2},..., D^{p^m},... sont linéairement indépendantes sur K.

Soit $\mathcal{U}$ l'ensemble des séries formelles $\sum_{i=o}^{\infty} a_i D^{p^i}$, où les a_i sont des éléments de K. Considérons un élément Δ de $\mathcal{U}$: pour tout x dans K, il existe un entier n tel que x appartienne à $k(\rho_1, \ldots, \rho_n)$; par la construction même de D, nous avons :

$$\forall j \geq n \qquad D^{p^j}(x) = 0$$

Ceci nous permet de définir $\Delta(x)$:

$$\Delta(x) = \sum_{i=o}^{n-1} a_i D^{p^i}(x)$$

THEOREME 4

Si $\mathcal{U}$ est l'ensemble des séries formelles $\sum_{i=o}^{\infty} a_i D^{p^i}$ ($a_i \in K$), alors nous avons :

(1) $\mathcal{U}$ est l'ensemble de toutes les k-dérivations de K

(2) Sur $\mathcal{U}$, la topologie de Krull coïncide avec la topologie des séries formelles.

(3) Soit $\mathcal{U}_D$ le plus petit sous espace de $\mathcal{U}$ contenant D et stable par élévation à la puissance p. Alors $\mathcal{U}_D$ est partout dense dans $\mathcal{U}$.

(1) Montrons tout d'abord que tout élément Δ de $\mathcal{U}$ est une dérivation : quels que soient x et y dans K, il existe n tel que x et y appartiennent à $k(\rho_1, \ldots, \rho_n)$. Alors nous avons :

$$\Delta(x + y) = \sum_{i=o}^{n-1} a_i D^{p^i} (x + y) \qquad a_i \in K$$

$$\Delta(xy) = \sum_{i=o}^{n-1} a_i D^{p^i} (xy)$$

Une combinaison linéaire à coefficients dans K des dérivations $D, D^p, \ldots, D^{p^{n-1}}$ est encore une dérivation, d'où les relations :

$$\Delta(x + y) = \Delta x + \Delta y$$

$$\Delta(xy) = x\,\Delta y + y\,\Delta x$$

Soit x un élément de k : pour tout j, $D^{p^j}(x)$ est nul, donc Δx est nul : tout élément de $\mathcal{U}$ est bien une k-dérivation de K.

Réciproquement, soit Δ une dérivation de K dans K nulle sur k. Posons $\Delta\rho_i = \alpha_i$, où les α_i appartiennent à K. D'après la définition de D, l'élément $D\rho_1 = \beta_1$ est non nul.

$$\dot{a}_o = \frac{\alpha_1}{\beta_1}$$

Alors, les dérivations Δ et $a_o D$ coïncident sur $k(\rho_1)$ et $a_o D$ appartient à $\mathcal{U}$.

Supposons déterminés des éléments $a_o, a_1, \ldots, a_n$ de K tels que les dérivations Δ et $\sum_{i=o}^{n} a_i D^{p^i}$ coïncident sur $k(\rho_1, \ldots, \rho_{n+1})$. Posons $\sum_{i=o}^{n} a_i D^{p^i} (\rho_{n+2}) = \mu_{n+2}$.

D'après la définition de D, $D^{p^{n+1}} (\rho_{n+2}) = \gamma_{n+1}$ appartient à $k - \{0\}$. Considérons a_{n+1} défini par :

$$a_{n+1} = \frac{\alpha_{n+2} - \mu_{n+2}}{\gamma_{n+1}}$$

Comme $D^{p^{n+1}}$ est nulle sur $k(\rho_1, \ldots, \rho_{n+1})$, les dérivations Δ et $\sum_{i=o}^{n+1} a_i D^{p^i}$ coïncident sur $k(\rho_1, \ldots, \rho_{n+1})$.

D'autre part, calculons $\sum_{i=o}^{n+1} a_i D^{p^i} (\rho_{n+2})$:

$$\begin{aligned} \sum_{i=o}^{n+1} a_i D^{p^i} (\rho_{n+2}) &= \mu_{n+2} + a_{n+1} \gamma_{n+1} \\ &= \alpha_{n+2} \\ &= \Delta\rho_{n+2} \end{aligned}$$

Les dérivations Δ et $\sum_{i=o}^{n+1} a_i D^{p^i}$ coïncident donc sur $k(\rho_1, \ldots, \rho_{n+2})$. De proche en proche, nous déterminons tous les coefficients a_n donc Δ peut se mettre sous la forme $\sum_{}^{\infty} a_i D^{p^i}$: c'est un élément de $\mathcal{J}$.

(2) Soit Δ un élément de $\mathcal{J}$: la dérivation Δ^p est encore une k-dérivation de K donc appartient à $\mathcal{J}$. C'est dire que $\mathcal{J}$ est une p-algèbre de Lie.

Soit $\mathcal{U}_n$ l'ensemble des éléments de $\mathcal{J}$ d'ordre supérieur ou égal à p^n : les idéaux $\mathcal{U}_n$ forment un système fondamental des voisignages de 0 dans une topologie sur $\mathcal{J}$ compatible avec la structure d'anneau de $\mathcal{J}$; cette topologie est la topologie usuelle des séries formelles. Soit $\mathrm{Der}_{K_n} K$ l'ensemble des dérivations de K nulles sur $K_n = k(\rho_1, \ldots, \rho_n)$. Par constructions, le noyau de D^{p^n} est exactement K_n : un raisonnement analogue à celui fait pour démontrer la partie (1) du théorème montre que $\mathcal{U}_n$ coïncide avec $\mathrm{Der}_{K_n} K$.

Sur $\mathcal{J} = \mathrm{Der}_k K$, nous pouvons aussi définir la topologie de Krull : c'est la topologie obtenue en prenant comme base de voisinages de 0 dans $\mathcal{J}$ les sous espaces $\mathrm{Der}_L K$ (c'est-à-dire l'ensemble des dérivations de K nulles sur L), où L est une extension finie de k. La relation $\mathcal{O}_n = \mathrm{Der}_{Kn} K$ montre que la topologie de Krull est plus fine que la topologie des séries formelles.

Soit maintenant L une extension finie de k : il existe q tel que K_q contienne L (où $K_q = k(\rho_1, \ldots, \rho_q)$. Alors $\mathrm{Der}_{Kq} K * \mathcal{O}_q$ est contenu dans $\mathrm{Der}_L K$, ce qui montre que la topologie des séries formelles est plus fine que la topologie de Krull: en résumé, ces deux topologies sur $\mathcal{J}$ sont identiques.

(3) Soit $\mathcal{J}_D$ le plus petit sous espace de $\mathcal{J}$ contenant D et stable par élévation à la puissance p : montrons que tout élément Δ de $\mathcal{J}$ peut être considéré comme limite d'éléments de $\mathcal{J}_D$:

$$\Delta \in \mathcal{J} \Longrightarrow \Delta = \sum_{i=0}^{\infty} a_i D^{p^i} \qquad a_i \in K$$

Les $\Delta + \mathcal{O}_q$ constituent une base de voisinage de Δ dans $\mathcal{J}$. Pour tout q, la dérivation $\sum_{i=0}^{q-1} a_i D^{p^i}$ appartient à $(\Delta + \mathcal{O}_q) \cap \mathcal{J}_D$, ce qui montre bien que $\mathcal{J}_D$ est partout dense dans $\mathcal{J}$.

REMARQUE : Cette partie (3) du théorème 5 est un cas particulier d'un théorème dû à Gerstenhaber [7] : en effet, celui-ci a démontré que, si K est un corps de caractéristique p, tout sous espace fermé de Der K est de la forme $\overline{\mathcal{J}_\Delta}$ pour un certain élément Δ de Der K.

CHAPITRE IV

ETUDE DE TOUTES LES DERIVATIONS DE K DE NOYAU k LORSQUE $[K : k]$ EST FINI

Dans tout ce chapitre, nous nous intéresserons à un corps K extension purement inséparable d'exposant 1 de k de degré fini sur k:

$$[K : k] = p^n$$

A - CARACTERISATION DES DERIVATIONS DE K DE NOYAU k

LEMME 3

Soit Δ une dérivation de K de noyau k. Si les applications $\Delta, \Delta^2, \ldots, \Delta^q$ sont linéairement dépendantes sur K, elles le sont sur k.

Soit m le plus petit entier tel qu'il existe une relation du type :

$$\Delta^m = \alpha_{m-1}\ \Delta^{m-1} + \alpha_{m-2}\ \Delta^{m-2} + \ldots + \alpha_1\Delta$$

où les α_i appartiennent à K. Pour tout x dans K, calculons $\Delta^{m+1}(x)$ de deux manières différentes :

$$\Delta^{m+1}(x) = \Delta^m(\Delta x) = \alpha_{m-1}\ \Delta^m(x) + \alpha_{m-2}\ \Delta^{m-1}(x) + \ldots + \alpha_1\Delta^2(x)$$

$$\Delta^{m+1}(x) = \Delta(\Delta^m x) = \alpha_{m-1}\Delta^m(x) + \ldots + \alpha_1\Delta^2(x) + \Delta(\alpha_{m-1})\Delta^{m-1}(x) + \ldots + \Delta\alpha_1\ \Delta x$$

Par soustraction, nous en déduisons :

$$\Delta(\alpha_{m-1})\Delta^{m-1}(x) + \Delta(\alpha_{m-2})\Delta^{m-2}(x) + \ldots + \Delta(\alpha_1)\ \Delta x = 0$$

$$\Delta(\alpha_{m-1})\Delta^{m-1} + \Delta(\alpha_{m-2})\ \Delta^{m-2} + \ldots + \Delta(\alpha_1)\Delta = 0$$

Etant donné le caractère minimal de m, nous avons nécessairement :

$$\Delta(\alpha_{m-1}) = \Delta(\alpha_{m-2}) = \ldots = \Delta(\alpha_1) = 0$$

Les coefficients α_i appartiennent donc à k.

Soient $D_1, \ldots, D_n$ des dérivations éléments de $\mathrm{Der}_k K$ et $\rho_1, \ldots, \rho_n$ des éléments de K. Considérons le déterminant $A(D_1, D_2, \ldots, D_n ; \rho_1, \rho_2, \ldots, \rho_n)$ défi-

ni par :

$$A(D_1, \ldots, D_n; \rho_1, \ldots, \rho_n) = \begin{vmatrix} D_1(\rho_1) & D_2(\rho_1) & \ldots & D_n(\rho_1) \\ D_1(\rho_2) & D_2(\rho_2) & \ldots & D_n(\rho_2) \\ \vdots & & & \vdots \\ D_1(\rho_n) & D_2(\rho_n) & \ldots & D_n(\rho_n) \end{vmatrix}$$

LEMME 4

Soit $(D_1, \ldots, D_n)$ une base de $\mathrm{Der}_k K$ sur K. Pour que n éléments $\rho_1, \ldots, \rho_n$ de K forment une p-base de K sur k, il faut et il suffit que $A(D_1, \ldots, D_n ; \rho_1, \ldots, \rho_n)$ soit différent de 0.

- Montrons tout d'abord que, pour que n éléments $\rho_1, \ldots, \rho_n$ de K forment une p-base de K sur k, il faut et il suffit qu'il existe n dérivations Δ_i dans $\mathrm{Der}_k K$ telles que $\Delta_i(\rho_j) = \delta_{ij}$: si $\rho_1, \ldots, \rho_n$ forment une p-base de K sur k nous pouvons définir n dérivations Δ_i nulles sur k en posant $\Delta_i(\rho_j) = \delta_{ij}$ (δ_{ij} désigne le symbole de Kronecker) puisque nous savons que, pour déterminer une dérivation de K, il suffit de choisir arbitrairement les images des éléments d'une p-base. Inversement, considérons n éléments $\rho_1, \ldots, \rho_n$ de K tels qu'il existe n dérivations de K nulles sur k vérifiant $\Delta_i(\rho_j) \neq \delta_{ij}$. Les dérivations Δ_i sont linéairement indépendantes sur K et en nombre égal à la dimension de $\mathrm{Der}_k K$ donc elles constituent une base de $\mathrm{Der}_k K$.

L'élément ρ_1 n'appartient pas à k (sinon $\Delta_1(\rho_1)$ serait nul). Si ρ_2 appartenait à $k(\rho_1)$, nous aurions $\Delta_2(\rho_2)$ égal à 0 car la dérivation Δ_2 nulle sur k et sur ρ_1 est nulle sur $k(\rho_1)$. Comme ρ_2^p appartient à k, le degré de $k(\rho_1, \rho_2)$ sur k est p^2. De proche en proche, nous pouvons ainsi démontrer que le degré de $k(\rho_1, \rho_2, \ldots, \rho_n)$ sur k est p^n. Or le degré de K sur k est p^n donc les corps emboîtés $k(\rho_1, \ldots, \rho_n)$ et K sont égaux : les éléments $\rho_1, \ldots, \rho_n$ forment une p-base de K sur k.

Ces dérivations Δ_i sont appelées dérivations partielles relativement à la p-base ρ_i.

- Si $\rho_1, \ldots, \rho_n$ forment une p-base de K sur k, considérons les n dérivations partielles Δ_i : elles peuvent s'exprimer comme combinaison linéaire à coefficients dans K des éléments $D_1, \ldots, D_n$ de la base de $\mathrm{Der}_k K$:

$$\Delta_i = a_1^i D_1 + a_2^i D_2 + \ldots + a_n^i D_n$$

Pour un i fixé, les n éléments $a_1^i, \ldots, a_n^i$ sont déterminés d'une façon unique par les conditions :

$$\Delta_i(\rho_j) = \delta_{ij}$$

Le déterminant du système, qui n'est autre que $A(D_1, /.., D_n ; \rho_1, \ldots, \rho_n)$ est donc bien différent de 0.

- Si $A(D_1, \ldots, D_n ; \rho_1, \ldots, \rho_n)$ est différent de 0, les n systèmes :

$$\sum_{m=1}^{n} a_m^i D_m (\rho_j) = \delta_{ij}$$

permettent de déterminer d'une manière unique n dérivations Δ_i telles que $\Delta_i (\rho_j) = \delta_{ij}$ donc $(\rho_1, \ldots, \rho_n)$ est une p-base de K sur k.

LEMME 5

Soit $(\rho_1, \ldots, \rho_n)$ une p-base de K sur k. Pour que n dérivations $D_1, \ldots, D_n$ appartenant à $\mathrm{Der}_k K$ constituent une base de $\mathrm{Der}_k K$ sur K, il faut et il suffit que le déterminant $A (D_1, \ldots, D_n ; \rho_1, \ldots, \rho_n)$ soit différent de zéro.

- Si $D_1, \ldots, D_n$ constituent une base de $\mathrm{Der}_k K$, il suffit d'appliquer le lemme 4.

- Supposons le déterminant $A (D_1, \ldots, D_n ; \rho_1, \ldots, \rho_n)$ différent de 0. Considérons les n dérivations partielles Δ_i relatives à la p-base (ρ_i) : elles constituent une base de $\mathrm{Der}_k K$ sur K donc les n dérivations D_i sont des combinai-

sons linéaires à coefficients dans K des dérivations Δ_i :

$$D_i = \alpha_1^i \Delta_1 + \ldots + \alpha_n^i \Delta_n$$

$$D_i (\rho_j) = \alpha_j^i$$

La matrice construite à partir des α_j^i est régulière (car son déterminant est l'inverse de $A (D_1, \ldots, D_n ; \rho_1, \ldots, \rho_n)$ donc les dérivations $D_1, \ldots, D_n$ forment une base de $Der_k K$.

THEOREME 5

Pour qu'une dérivation Δ de K nulle sur k admette exactement k comme noyau, il faut et il suffit que $\Delta, \Delta^p, \ldots, \Delta^{p^{n-1}}$ soient linéairement indépendantes sur K.

- Si $\Delta, \Delta^p, \ldots, \Delta^{p^{n-1}}$ sont linéairement indépendantes sur K, elles constituent une base de $Der_k K$ sur K. Toute "bonne dérivation" D de K est combinaison linéaire à coefficients dans K de $\Delta, \Delta^p, \ldots, \Delta^{p^{n-1}}$:

$$D = \alpha_o \Delta + \alpha_1 \Delta^p + \ldots + \alpha_{n-1} \Delta^{p^{n-1}}$$

Soit x un élément du noyau de Δ :

$$\Delta^{p^j}(x) = 0 \qquad j = 0, \ldots, n-1$$
$$D(x) = 0$$

Comme le noyau de D est k, l'élément x est dans k : le noyau de Δ est exactement k.

- Soit Δ une dérivation de K de noyau k. Appelons i le plus grand entier tel que $\Delta, \Delta^p, \ldots, \Delta^{p^i}$ soient linéairement indépendantes sur K : alors, $\Delta^{p^{i+1}}$ est combinaison linéaire à coefficients dans K des dérivations $\Delta, \Delta^p, \ldots, \Delta^{p^i}$:

$$\Delta^{p^{i+1}} = a_i \Delta^{p^i} + \ldots + a_1 \Delta^p + a_o \Delta$$

D'après le théorème de Jacobson rappelé au chapitre III, les applications k-linéaires $1, \Delta, \ldots, \Delta^{p^{i+1}-1}$ sont linéairement indépendantes sur K : les applications $1, \Delta, \ldots, \Delta^{p^{i+1}}$ sont linéairement dépendantes sur K, donc aussi sur k d'après le lemme 2 : la dérivation $\Delta^{p^{i+1}}$ apparaît alors comme combinaison linéaire à coefficients dans k de $1, \Delta, \ldots, \Delta^{p^{i+1}-1}$. D'après l'unicité de la décomposition de $\Delta^{p^{i+1}}$ suivant la base $1, \Delta, \ldots, \Delta^{p^{i+1}-1}$ nous en déduisons que $\Delta^{p^{i+1}}$ est combinaison linéaire à coefficients dans k de $\Delta^{p^i}, \Delta^{p^{i-1}}, \ldots, \Delta^p, \Delta$.

D'après le lemme 3, la dimension du noyau de l'application $\Delta^{p^{i+1}} - a_i\Delta^{p^i} - \ldots - a_1\Delta^p - a_o\Delta$ est au plus p^{i+1}. Or, cette application doit être nulle sur K tout entier, donc nous avons :

$$i + 1 = n$$

Les dérivations $\Delta, \Delta^p, \ldots, \Delta^{p^{n-1}}$ sont linéairement indépendantes sur K.

COROLLAIRE 1

Si Δ est une dérivation de K de noyau k, les dérivations Δ^{p^j} sont combinaisons linéaires à coefficients dans k de $\Delta, \Delta^p, \ldots, \Delta^{p^{n-1}}$ pour tout j supérieur ou égal à n.

Au cours de la démonstration du théorème 5, nous avons vu que Δ^{p^n} pouvait se mettre sous la forme :

$$\Delta^{p^n} = a_{n-1}\Delta^{p^{n-1}} + \ldots + a_1\Delta^p + a_o\Delta$$

où les a_i sont des éléments de k.

Les termes intervenant dans l'expression de Δ^{p^n} sont deux à deux permutables, donc $\Delta^{p^{n+1}}$ s'écrit :

$$\Delta^{p^{n+1}} = a^p_{n-1}\Delta^{p^n} + \ldots + a^p_1\Delta^{p^2} + a^p_o\Delta^p$$

$$\Delta^{p^{n+1}} = \sum_{i=1}^{n-1} (a^p_{n-1}\, a_i + a^p_{i-1})\, \Delta^{p^i} + a^p_{n-1}\, a_o\Delta$$

Le résultat s'établit ensuite de proche en proche.

COROLLAIRE 2

L'ensemble des dérivations de K dont le noyau est k définit un k-ouvert (de Zariski) dans $\mathrm{Der}_k K$.

Pour que Δ ait pour noyau k, il faut et il suffit que $\Delta, \Delta^p, \ldots, \Delta^{p^{n-1}}$ soient linéairement indépendantes, c'est-à-dire que $A(\Delta, \Delta^p, \ldots, \Delta^{p^{n-1}} ; \rho_1, \ldots, \rho_n)$ soit différent de 0, pour une p-base quelconque de K.

CAS PARTICULIER

Etudions le cas où K est de caractéristique 2 et est une extension de degré 4 de k. Soient (ρ_1, ρ_2) une 2-base de K et Δ_1 et Δ_2 les dérivations partielles relatives à cette 2-base. Soit Δ une dérivation de K nulle sur k :

$$\Delta = x_1\Delta_1 + x_2\Delta_2$$

Pour que le noyau de Δ soit k, il faut et il suffit que Δ et Δ^2 soient linéairement indépendantes, c'est-à-dire que $A(\Delta, \Delta^2 ; \rho_1, \rho_2)$ soit non nul. Cela donne la condition simple $\Delta(x_1x_2)$ différent de 0.

B - CARACTERISATION DES DERIVEES LOGARITHMIQUES POUR UNE DERIVATION DE NOYAU k

Soit $\mathcal{L}$ l'espace vectoriel des applications k-linéaires de K dans K. Pour toute dérivation Δ de K de noyau k, les dérivations $\Delta, \Delta^p, \ldots, \Delta^{p^{n-1}}$ constituent une base de la p-algèbre de Lie $\mathrm{Der}_k K$ donc, d'après le théorème de Jacobson rappelé au chapitre III, les applications $1, \Delta, \Delta^2, \ldots, \Delta^{p^n - 1}$ constituent une base

de $\mathfrak{L}$ sur K.

Pour tout élément ρ de K, introduisons la notation suivante :

$$\rho[p^i] = \rho p^i + (\Delta^{p-1}\rho)p^{i-1} + (\Delta^{p^2-1}\rho)p^{i-2} + \ldots + \Delta^{p^i-1}\rho$$

LEMME 6

Soit Δ une dérivation de K de noyau k

(1) L'application K-linéaire Φ de $\mathfrak{L}$ dans $\mathfrak{L}$ définie par :

$\Phi(\Delta^i) = (\Delta + \rho.1)^i \quad (i = 0, \ldots, p^n - 1)$
est bijective pour tout ρ dans K

(2) L'application Φ est un homomorphisme d'anneaux si et seulement si $\rho[p^n]$ vérifie la relation :

$$\rho[p^n] = a_o\rho + a_1\rho[p] + \ldots + a_{n-1}\rho[p^{n-1}]$$

où les a_i sont les composantes de Δ^{p^n} relativement à la base $\Delta, \Delta^p, \ldots, \Delta^{p^{n-1}}$:

$$\Delta^{p^n} = a_o\Delta + a_1\Delta^p + \ldots + a_{n-1}\Delta^{p^{n-1}}$$

(1) Chaque $(\Delta + \rho.1)^i$ est combinaison linéaire à coefficients dans K de $1, \Delta, \ldots, \Delta^i$, la coefficient de Δ^i étant 1 ; la matrice de Φ relativement à la base $1, \Delta, \ldots, \Delta^{p^n-1}$ de $\mathfrak{L}$ est une matrice triangulaire n'ayant que des 1 sur la diagonale principale donc elle est inversible ; les $(\Delta + \rho.1)^i$ $(i = 0, \ldots, p^n - 1)$ constituent alors une base de $\mathfrak{L}$, ce qui montre que l'application Φ est bijective.

(2) Si Φ est un homomorphisme d'anneaux, $\Phi(\Delta^{p^n})$ est égal à $(\Phi(\Delta))^{p^n}$. Or, d'après une formule établie par Jacobson [6], nous avons :

$$(\Delta + \rho.1)^{p^i} = \Delta^{p^i} + \rho^{[p^i]}.1$$

$$\Delta^{p^n} = a_o\Delta + \ldots + a_{n-1}\Delta^{p^{n-1}}$$

(Le corollaire 1 du théorème 6 montre que les a_j appartiennent à k)

Comme Φ est K-linéaire, nous avons :

$$\Phi(\Delta^{p^n}) = a_o(\Delta + \rho.1) + a_1(\Delta^p + \rho^{[p]}.1) + \ldots + a_{n-1}(\Delta^{p^{n-1}} + \rho^{[p^{n-1}]}.1$$

$$= \Delta^{p^n} + (a_o\rho + a_1\rho^{[p]} + \ldots + a_{n-1}\rho^{[p^{n-1}]}).1$$

$$(\Phi(\Delta))^{p^n} = (\Delta + \rho.1)^{p^n}$$

$$= \Delta^{p^n} + \rho^{[p^n]}.1$$

L'égalité $(\Phi(\Delta))^{p^n} = \Phi(\Delta^{p^n})$ entraîne :

$$\rho^{[p^n]} = a_o\rho + a_1\rho^{[p]} + \ldots + a_{n-1}\rho^{[p^{n-1}]}$$

- Supposons vérifiée la relation ci-dessus. En reprenant le calcul précédent en sens inverse, nous en déduisons que :

$$\Phi(\Delta^{p^n}) = (\Phi(\Delta))^{p^n}$$

Nous avons donc, d'après la définition de $\Phi(\Delta^i)$ pour $i < p^n - 1$

$$\Phi(\Delta^m) = (\Phi(\Delta))^m$$

pour m inférieur ou égal à p^n. Supposons cette relation vraie jusqu'à ℓ, nombre supérieur à p^n. D'après le lemme 3, nous avons :

$$\Delta^\ell = \alpha_o + \alpha_1\Delta + \ldots + \alpha_{p^n-1}\Delta^{p^n-1}$$

où les α_i sont dans k.

$$\Delta^{\ell+1} = \alpha_o \Delta + \alpha_1 \Delta^2 + \ldots + \alpha_{p^n-1} \Delta^{p^n}$$

$$\Phi(\Delta^{\ell+1}) = \alpha_o \Phi(\Delta) + \alpha_1 (\Phi(\Delta))^2 + \ldots + \alpha_{p^n-1} (\Phi(\Delta))^{p^n}$$

$$= \Phi(\Delta) \left\{ \alpha_o + \alpha_1 \Phi(\Delta) + \ldots + \alpha_{p^n-1} (\Phi(\Delta))^{p^n-1} \right\}$$

Or, par hypothèse, nous avons :

$$\Phi(\Delta^{\ell}) = (\Phi(\Delta))^{\ell}$$

$$= \alpha_o + \alpha_1 \Phi(\Delta) + \ldots + \alpha_{p^n-1} (\Phi(\Delta))^{p^n-1}$$

Nous en déduisons :

$$\Phi(\Delta^{\ell+1}) = (\Phi(\Delta))^{\ell+1}$$

Cette égalité est donc valable pour tout ℓ.
En raison de la K-linéarité de Φ, pour démontrer que Φ est un homomorphisme d'anneaux, il suffit de vérifier que :

$$\Phi(\Delta^i) \Phi (a\Delta^j) = \Phi(\Delta^i (a\Delta^j))$$

pour i et j inférieurs à p^n et a appartenant à K.

Etudions le cas où i vaut 1 :

$$\Phi(\Delta) = (\Delta + \rho.1)$$

$$\Phi(a\Delta^j) = a (\Delta + \rho.1)^j$$

$$\Phi(\Delta) . \Phi(a\Delta^j) = (\Delta + \rho.1) \left\{ a(\Delta + \rho.1)^j \right\}$$

$$= a(\Delta + \rho.1)^{j+1} + \Delta a.(\Delta + \rho.1)^j$$

$$\Delta(a\Delta^j) = \Delta a . \Delta^j + a \Delta^{J+1}$$

$$\Phi(\Delta(a\Delta^j)) = \Delta a(\Delta + \rho.1)^j + a(\Delta + \rho.1)^{j+1}$$

La relation est donc vérifiée par $i = 1$. Supposons-la vérifiée pour tout i inférieur à m. Etudions alors :

$$\Phi(\Delta^m) \cdot \Phi(a\Delta^j)$$

$$\Phi(\Delta^m)\ \Phi\ (a\Delta^j) = \Phi(\Delta)\ \Phi(\Delta^{m-1})\ \Phi(a\Delta^j)$$

D'après l'hypothèse de récurrence, nous avons :

$$\Phi(\Delta^{m-1})\ \Phi(a\Delta^j) = \Phi(\Delta^{m-1}\ (a\Delta^j))$$

Calculons alors $\Delta^{m-1}\ (a\Delta^j)$ grâce à la formule de Leibnitz :

$$\Delta^{m-1}\ (a\Delta^j) = \sum_{\ell=o}^{m-1} (^{m-1}_{\ell})\ \Delta^{m-1-\ell}(a)\ .\ \Delta^{j+\ell}$$

$$\Phi(\Delta^{m-1}\ (a\Delta^j)) = \sum_{\ell=o}^{m-1} (^{m-1}_{\ell})\ \ ^{m-1-\ell}(a)\ \Phi(\Delta^{j+\ell})$$

$$\Phi(\Delta^m)\ \Phi(a\Delta^j) = \sum_{\ell=o}^{m-1} (^{m-1}_{\ell})\ \Phi(\Delta)\ \ \Delta^{m-1-\ell}(a)\ .\ \Phi(\Delta^{j+\ell})$$

Appliquons à nouveau l'hypothèse de récurrence :

$$\Phi(\Delta^m)\ \Phi(a\Delta^j) = \sum_{\ell=o}^{m-1} (^{m-1}_{\ell})\ \Phi(\Delta\ \ \Delta^{m-1-\ell}(a)\ .\ \Delta^{j+\ell}\ )$$

$$= \sum_{\ell=o}^{m-1} (^{m-1}_{\ell})\ \Phi(\Delta^{m-\ell}(a)\ .\ \Delta^{j+\ell} + \Delta^{m-1-\ell}(a)\ \Delta^{j+\ell+1})$$

$$= \sum_{\ell=1}^{m-1} (^{m-1}_{\ell}) + (^{m-1}_{\ell-1})\ \ \Delta^{m-\ell}(a)\ \Phi\ (\Delta^{j+\ell})$$

$$+ \Delta^m(a)\ \Phi(\Delta^j) + a\ \Phi(\Delta^{m+j})$$

Utilisons la relation :

$$(^{m-1}_{\ell}) + (^{m-1}_{\ell-1}) = (^{m}_{\ell})$$

Nous obtenons alors :

$$\Phi(\Delta^m)\ \Phi(a\Delta^j) = \Phi \sum_{\ell=0}^{m} \binom{m}{\ell} \Delta^{m-\ell}(a)\ \Delta^{j+\ell}$$

$$= \Phi\ \Delta^m\ (a\Delta^j)$$

L'égalité annoncée est ainsi vérifiée. Pour tout i, nous avons donc :

$$\Phi(\Delta^i)\ \Phi(a\Delta^j) = \Phi(\Delta^i(a\Delta^j))$$

L'application Φ est un homomorphisme d'anneaux.

Remarque : La méthode précédente m'a été inspirée par un exercice de Jacobson [6].

LEMME 7 - (GENERALISATION DE LA FORMULE DE BARSOTTI-CARTIER)

Si K est un corps de caractéristique p et si Δ est une dérivation de K, nous avons :

$$\frac{\Delta^{p^j}(x)}{x} = \left(\frac{\Delta x}{x}\right)^{\lceil p^j \rceil}$$

pour tout x de K et tout entier j supérieur ou égal à 1.

Calculons tout d'abord $\rho^{\lceil p^{j+1} \rceil}$ à partir de $\rho^{\lceil p^j \rceil}$ pour élément quelconque ρ de K :

$$\rho^{\lceil p^j \rceil} = \rho^{p^j} + \sum_{i=1}^{j} (\Delta^{p^i-1}\rho)^{p^{j-i}}$$

$$\rho^{\lceil p^{j+1} \rceil} = \rho^{p^{j+1}} + \sum_{i=1}^{j+1} (\Delta^{p^i-1}\rho)^{p^{j+1-i}}$$

$$\rho^{\lceil p^{j+1} \rceil} = (\rho^{\lceil p^j \rceil})^p + \Delta^{p^{j+1}-1}(\rho)$$

Pour j = 1, la formule annoncée n'est autre que la formule de Barsotti-Cartier [4] :

$$\frac{\Delta^p(x)}{x} = \left(\frac{\Delta x}{x}\right)^p + \Delta^{p-1}\left(\frac{\Delta x}{x}\right)$$

Supposons la formule vraie à l'ordre j et appliquons la formule de Barsotti-Cartier

à la dérivation Δ^{p^j} :

$$\frac{\Delta^{p^{j+1}}(x)}{x} = \left(\frac{\Delta^{p^j}(x)}{x}\right)^p + \Delta^{p^{j+1}-1}\left(\frac{\Delta x}{x}\right)$$

D'après l'hypothèse de récurrence, nous avons :

$$\frac{\Delta^{p^j}(x)}{x} = \left(\frac{\Delta x}{x}\right)^{\left[p^j\right]}$$

Nous en déduisons :

$$\frac{\Delta^{p^{j+1}}(x)}{x} = \left\{\left(\frac{\Delta x}{x}\right)^{\left[p^j\right]}\right\}^p + \Delta^{p^{j+1}-1}\left(\frac{\Delta x}{x}\right)$$

$$= \left(\frac{\Delta x}{x}\right)^{\left[p^{j+1}\right]}$$

THEOREME 6

Soit Δ une dérivation de K de noyau k ; alors Δ^{p^n} peut s'écrire :

$$\Delta^{p^n} = a_o\Delta + a_1\Delta^p + \ldots + a_{n-1}\Delta^{p^{n-1}} \qquad a_i \in k$$

Dans ces conditions, pour qu'un élément ρ de K soit la dérivée logarithmique d'un élément de K, il faut et il suffit que ρ soit solution de l'équation :

$$\rho^{\left[p^n\right]} = a_o\rho + a_1\rho^{[p]} + \ldots + a_{n-1}\rho^{\left[p^{n-1}\right]}$$

- Supposons que ρ soit la dérivée logarithmique d'un élément σ de K. Appliquons le lemme 7 :

$$\frac{\Delta^{p^n}(\sigma)}{\sigma} = \rho^{\left[p^n\right]}$$

$$\Delta^{p^n}(\sigma) = a_o\Delta\sigma + a_1\Delta^p\sigma + \ldots + a_{n-1}\Delta^{p^{n-1}}(\sigma)$$

$$\frac{\Delta^{p^n}(\sigma)}{\sigma} = a_o \rho + a_1 \rho^{[p]} + \ldots + a_{n-1} \rho^{[p^{n-1}]}$$

L'élément ρ est bien solution de l'équation

$$\rho^{[p^n]} = a_o \rho + a_1 \rho^{[p]} + \ldots + a_{n-1} \rho^{[p^{n-1}]}$$

- Réciproquement, supposons ρ solution de cette équation. Nous pouvons alors considérer l'automorphisme Φ de $\mathfrak{L}$ défini dans le lemme 6. Il est nécessairement de la forme [9] :

$$\Phi(X) = C^{-1} X C \qquad \forall X \in \mathfrak{L}$$

où C est un élément inversible de $\mathfrak{L}$. Prenons pour X l'homothétie H_x définie par un élément x quelconque de K :

$$\Phi(H_x) : C^{-1} (H_x) C = H_x$$
$$H_x . C = C . H_x$$

Comme C commute avec toutes les homothéties de rapport un élément de K, c'est une homothétie : il existe un élément σ non nul dans K tel que C soit l'homothétie de rapport σ. Etudions alors $\Phi(\Delta-\rho.1)$: par définition de Φ, c'est Δ ; d'autre part nous avons :

$$\Phi(\Delta-\rho.1) = \sigma^{-1} (\Delta-\rho.1)\sigma$$
$$\Delta = \sigma^{-1} (\Delta-\rho.1)\sigma$$

Appliquons la transformation $\sigma^{-1} (\Delta-\rho.1)$ à un élément quelconque x de K :

$$\sigma^{-1}\ (\Delta-\rho.1)\ \sigma(x) = \sigma^{-1}\ (\Delta-\rho.1)\ (\sigma x)$$
$$= \sigma^{-1}\ .\ \left(\ \Delta(\sigma x) - \rho.\sigma x\ \right)$$
$$= \sigma^{-1}\ \left(\sigma\Delta x + x\Delta\sigma - \rho\sigma x\ \right)$$
$$= \Delta x + x\,\frac{\Delta\sigma}{\sigma} - \rho x$$

$$\Delta x = \Delta x + x\,\frac{\Delta\sigma}{\sigma} - \rho x$$

Choisissant x non nul, nous en déduisons :

$$\rho = \frac{\Delta\sigma}{\sigma}$$

L'élément ρ apparaît comme la dérivée logarithmique de σ.

BIBLIOGRAPHIE

1. BOURBAKI : Algèbre commutative - VII - § 1 - n° 7 - théorème 4

2. BOURBAKI : Algèbre commutative - V - § 2 - n° 3 - lemme 4

3. P. SAMUEL : Classes de diviseurs et dérivées logarithmiques - Topology - 3 - p. 81-96

4. BARSOTTI : Répartitions on abelian varieties - Illinois - J. Math. 2 (1958), p. 43-70

5. ZARISKI-SAMUEL : Commutative Algebra - II

6. JACOBSON : Lectures in Abstract Algebra - Volume III : Theory of fields and Galois theory - IV - § 8 - théorème 19

7. GERSTENHABER : Bulletin of the American Mathematical Society ; Volume 71 - nber 6 november 1965

8. P. SAMUEL : On unique factorization domains ; Illinois - J. Math. - t. 5 - 1961 - p. 1-17

9. JACOBSON : Lectures in Abstract Algebra - Volume II : Linear Algebra - III - § 17

10. SALMON : Su un problema posto da P. Samuel
Rendiconti dell' Accademia dei Lincei - Genova

11. D. SHANKS : Number theory - II - § 28 - theorem 35

12. D. SHANKS : Number theory - I - § 11 - theorem 18

13. D. SHANKS : Number theory - II - § 32.

Joseph FLOCH, Maître-Imprimeur à Mayenne - 5-10-1967 - n°2915