BULLETIN DE LA S. M. F.

CHARLES DELORME

Sur les modules des singularités des courbes planes

Bulletin de la S. M. F., tome 106 (1978), p. 417-446

<http://www.numdam.org/item?id=BSMF_1978__106__417_0>

Bull. Soc. math. France,
106, 1978, p. 417-446

SUR LES MODULES DES SINGULARITÉS DES COURBES PLANES

PAR

CHARLES DELORME

[Université Paris-Sud, Orsay]

RÉSUMÉ. — Dans cet article, on étudie l'espace des modules des singularités unibranches de courbes planes, ayant un monoïde caractéristique donné. On montre que cet espace comporte des parties isomorphes à des ouverts d'espaces projectifs anisotropes. Dans le cas où la singularité a une seule paire de Puiseux, on calcule la dimension de la partie générique, ce qui répond à une question posée par ZARISKI dans son cours à l'École Polytechnique.

Introduction

On considère l'anneau local complet d'une branche analytique intègre et singulière d'une courbe plane sur $\mathbf{C}$; on peut le décrire à l'aide de développements de Puiseux.

On indique comment voir si deux tels développements décrivent des anneaux isomorphes (§ 3), et on introduit des invariants analytiques discrets, faisant intervenir les valuations des éléments de l'anneau et de ses formes différentielles dans son normalisé (§ 4). A partir de ces invariants, on obtient des conditions, qui lorsqu'elles sont réalisées, permettent de construire des développements ultra-courts, ayant le plus possible de coefficients nuls (§ 6). Certaines composantes de l'espace des modules apparaissent alors comme des parties constructibles d'espaces projectifs anisotropes (§ 8).

Quand l'anneau n'a qu'une paire de Puiseux, on peut préciser les relations entre les invariants, et les coefficients des développements de Puiseux (§ 14 et 15). On dégage une notion de généricité (§ 16), et on montre que l'espace des modules des anneaux génériques est un ouvert d'un espace anisotrope (§ 18), dont on arrive à expliciter la dimension en fraction continue de la paire de Puiseux (§ 32) ce qui répond dans ce cas à une question posée par ZARISKI en novembre 1973.

1. Définition des anneaux de Puiseux

Soient m et n deux entiers tels que $1 < n < m$, et n ne divise pas m. Soit $a = (a_i,\ i > m)$ une suite de nombres complexes, telle que le pgcd de m, n et des i, tels que $a_i \neq 0$, vaut 1.

On appelle $A\,(m, n, a)$ le sous-anneau complet de $B = \mathbf{C}\,[[t]]$ engendré pae $x = t^n$ et $y = t^m + \sum_{i>m} a_i\, t^i$.

Les anneaux ainsi obtenus sont dits de *Puiseux*.

2. Interprétation géométrique

L'anneau local complet d'une branche analytique intègre et singulière d'une courbe plane sur $\mathbf{C}$ est un anneau de Puiseux : il suffit de choisir un paramètre transverse x, puis une uniformisante convenable t du normalisé, puis un paramètre convenable y donnant le contact maximal. Inversement, un anneau de Puiseux définit une telle branche, dont la multiplicité est n, et dont l'ordre du contact maximal est m, car B est le normalisé de $A\,(m, n, a)$.

3. Lemme

Deux anneaux de Puiseux $A = A\,(m, n, a)$ et $A' = A\,(m', n', a')$ sont isomorphes si, et seulement si, les deux conditions suivantes sont réalisées :

(i) $m = m'$ *et* $n = n'$;

(ii) *il existe* $\xi \in A$, $v(\xi) > n$ *et* $\eta \in A$, $v(\eta) > m$, *et* $\gamma \in \mathbf{C}$, $\gamma \neq 0$, *tels que*

$$t' = \gamma\, t \sqrt[n]{1 + x^{-1}\gamma^{-n}\xi},$$

$$y' = \gamma^m y + \eta = t'^m + \sum_{i<m} a'_i\, t'^i,$$

où v est la valuation naturelle de B, et où $\sqrt[n]{1+z} = 1 + (z/n) + \ldots$ *pour tout* $z \in B$, $v(z) > 0$.

D'après le paragraphe 2, m et n ne dépendent pas du développement choisi. Un isomorphisme $A' \to A$ se prolonge de manière unique en un isomorphisme des corps de fractions et des normalisés. L'uniformisante, qui sert à définir A', a pour image t' dans B, de valuation 1, ce qui permet de définir γ, et les deux générateurs de définition de A' ont pour images x' et y', qui permettent de définir ξ et η satisfaisant les conditions indiquées.

Inversement, les conditions indiquées permettent de définir un monomorphisme $A' \to A$, et c'est un isomorphisme, car x' et y' engendrent encore A comme anneau complet, puisque les conditions $v(\xi) > n$ et $v(\eta) > m$ impliquent $\eta \in (x, y)^2$ et $\xi \in (y, x^2)$, ce qui permet d'écrire x et y sous forme de séries entières en x' et y'.

Dans la suite, on ne considère plus que des changements de paramètres du type indiqué.

4. Invariants des anneaux de Puiseux

A un anneau de Puiseux $A(m, n, a) = A$, on associe les objets suivants :

Le monoïde caractéristique $\Gamma = v(A)$: Les deux plus petits générateurs de Γ sont n et m; on pose $c = \inf\{u \in \Gamma, \mathbf{N}+u \subset \Gamma\}$, c est un nombre fini.

L'ensemble $\Delta = v(A+A(dy/dx))$: on voit que Γ opère par addition sur Δ, qui contient donc Γ et $\Gamma+m-n$. On pose

$$\nu = \inf\{u \in \Delta, u \notin \Gamma \cup \Gamma+m-n\} \qquad \text{et} \qquad \delta = \inf\{u \in \Delta, \mathbf{N}+u \cup \Delta\}.$$

pose aussi $\Delta' = \{u \in \Delta, u \neq \nu, m < u < \infty\}$.

La fonction $w : \Delta \to \Gamma$, définie par

$$w(r) = \sup\{v(p)\}, \quad p \in A, \quad q \in A, \qquad v\left(q - p\frac{dy}{dx}\right) = r.$$

Le nombre $\varepsilon = \inf\{v(p)\}, p \in A, q \in A, v(q-p(dy/dx)) = \infty$.

On a évidemment $\delta \leqslant c$ et $\varepsilon \leqslant c$.

Montrons que ces objets sont des invariants de A, autrement dit, qu'un changement de paramètres ne les modifie pas.

C'est clair pour Γ, dont la définition est indépendante du développement choisi.

On interprète Δ à l'aide de formes différentielles. A un anneau complet R sur C, on associe le R-module $I/I^2 = \Omega_R$, où I est le noyau de la surjection diagonale $R \hat{\otimes}_C R \to R$ d'anneaux complets. L'injection $A \to B$ fournit un morphisme de A-modules $\Omega_A \to \Omega_B$. Le B-module Ω_B est libre de rang 1, de base $dt = t \otimes 1 - 1 \otimes t$, et le A-module image de Ω_A a deux générateurs, savoir

$$dx = nt^{n-1} \qquad \text{et} \qquad dy = (mt^{m-1} + \textstyle\sum_{i>m} i a_i t^{i-1})\, dt.$$

Le sous-B-module de Ω_B, engendré par cette image, est libre de base dx.

On voit que Δ est l'ensemble des valuations des éléments de l'image Ad A rapportés à une base du module Bd A engendré par Ad A dans Ω_B, ce qui ne fait pas intervenir le choix du développement.

Voyons l'invariance de w.

Si $r \in \Gamma$, alors $w(r) = \infty$. Si $r \notin \Gamma$ et $r \in \Gamma + m - n$, $w(r) = r + m - n$.

Si $r \in \Delta$ et $r \notin \Gamma \cup \Gamma + m - n$, il existe p et q dans A tels que

$$v\left(q - p\frac{dy}{dx}\right) = r;$$

alors

$$v(q) = v(p) + m - n < r \qquad \text{et} \qquad v(p) \leqslant w(r),$$

l'égalité $v(p) = w(r)$ pouvant être atteinte par un choix convenable de p et q. On regarde l'effet d'un changement de paramètres $x' = \gamma^n x + \xi$, $y' = \gamma^m y + \eta$ et $t' = \gamma t$ modulo t^2. On peut écrire $\xi = P(x, y)$, avec $P \in (X^2, Y)\mathbf{C}[[X, Y]]$, et $\eta = Q(x, y)$ avec $Q \in (X, Y)^2\mathbf{C}[[X, Y]]$. Il existe p' et q' dans A avec $v(q' - p'(dy'/dx')) = r$ et $w'(r) = v(p')$, où w' est la fonction attachée au générateur x', y' de A. On a l'égalité, où figurent les dérivées partielles de P et Q,

$$\frac{dx'}{dx}\left(q' - p'\frac{dy'}{dx'}\right) = (q'\gamma^n + q' P'_X(x, y) - p' Q'_X(x, y)) - (p'\gamma^m - q' P'_Y(x, y) + p' Q'_Y(x, y))\frac{dy}{dx}.$$

La valuation de $dx'/dx = \gamma^n + P'_X(x, y) + P'_Y(x, y)\, dy/dx$ est 0, car

$$v(\gamma^n) = 0 \qquad \text{et} \qquad v(P'_X(x, y)) > 0$$

et

$$v\left(P'_Y(x, y)\frac{dy}{dx}\right) \geqslant m - n > 0.$$

La valuation de $p'\gamma^m - q' P'_Y(x, y) + p' Q'_Y(x, y)$ est $v(p')$, puisque

$$v(p'\gamma^m) = v(p'), \qquad v(p' Q'_Y(x, y)) > v(p')$$

et

$$v(q' P'_Y(x, y)) \geqslant v(q') > v(p').$$

On en tire $w(r) \geqslant v(p') = w'(r)$, et vice-versa, en utilisant le changement de paramètres inverse, donc $w(r) = w'(r)$.

On montre de la même façon que ε ne dépend pas du choix des paramètres.

Quand aux autres objets introduits, ils sont tous directement déduits de Γ et Δ, donc insensibles aux changements de paramètres.

5. Lemme

L'effet du changement de paramètres $x' = \gamma^n x$, $y' = \gamma^m y$, $t' = \gamma t$ *est* $a'_i = a_i \gamma^{m-i}$.

L'effet du changement de paramètres $x' = x+p$, $y' = y+q$, $t' = t\sqrt[n]{1+x^{-1}p}$ *est donné par*

$$\Phi(a', t') - \Phi(a, t') = q - p\frac{dy}{dx} \text{ modulo } t^{2v(p)-2n+m},$$

en posant $\Phi(a, t) = t^m + \sum_{i>m} a_i t^i$.

La première partie est évidente. Pour la seconde, on notera que $t'^i = t^i + (ip/nx)\, t^i$ modulo $t^{2v(p)-2n+i}$.

On en déduit, puisque $\Phi(a, t) = y$,

$$\Phi(a, t') = y + \Phi'_t(a, t)\frac{pt}{nx} \text{ modulo } t^{2v(p)-2n+m},$$

$$y' = y+q = \Phi(a', t') = \Phi(a, t') + q - p\frac{dy}{dx} \text{ modulo } t^{2v(p)-2n+m}.$$

6. Proposition

On introduit les conditions (CE) *et* (CU) :

(CE) $\forall\, r \in \Delta'$, $r < 2w(r) - 2n + m$;

(CU) $\delta \leqslant 2\varepsilon - 2n + m$;

en vue des résultats suivants :

(i) *si un anneau de Puiseux* $A = A(m, n, a)$ *vérifie* (CE), *il existe une suite ultra-courte* a', *c'est-à-dire* $a'_r = 0$ *pour tout* $r \in \Delta'$, *telle que* $A(m, n, a')$ *soit isomorphe à* A;

(ii) *si en outre* A *vérifie* (CU), *cette suite ultra-courte est unique à homothétie près, c'est-à-dire que si* a' *et* a'' *sont deux suites ultra-courtes donnant un anneau isomorphe à* A, *il existe un nombre complexe* $\gamma \neq 0$ *tel que* $a'_i = a''_i \gamma^{i-m}$ *pour tout* $i > m$.

D'après le lemme (§ 5), si $r \in \Delta'$ vérifie $2w(r) - 2n + m > r$, il existe un changement de paramètres $x' = x+p$, $y' = y+q$, avec $v(p) = w(r)$,

dont l'effet est d'annuler le coefficient de t^r sans changer les coefficients des t^i, $m \leqslant i < r$. On fera donc successivement des changements de paramètres convenables pour annuler les a_i, $i \in \Delta'$, $i < c$, i croissant de proche en proche. A ce moment, $\sum_{i \geqslant c} a_i t^i$ est un élément de A, qu'on peut annuler par un changement de paramètres évident, sans rien changer aux a_i, $i < c$.

Ceci prouve (i), et donne la manière de construire un développement ultra-court de A si A vérifie (CE).

Supposons que a et a' sont deux développements ultra-courts de A, et que A vérifie (CE) et (CU). Le deuxième développement se déduit du premier par un changement de paramètres : $x' = \gamma^n x + p$, $y' = \gamma^m y + q$ et $v(t' - \gamma t) \geqslant 2$. Le changement $x' = \gamma^n x$, $y' = \gamma^m y$, $t' = \gamma t$ donnant une modification homothétique, on se ramène au cas $\gamma = 1$.

Si a est ultra-court, on a $\nu = v(my - nx\,(dy/dx)) = \inf\{i, i > m, a_i \neq 0\}$ [2]. De la sorte on est assuré que $v(q - p\,(dy/dx))$ est différent de ν, ou bien infini, $v(q) > m$ et $v(p) > n$. D'après le paragraphe 5, on a

$$v\left(q - p\frac{dy}{dx}\right) \geqslant 2v(p) - 2n + m,$$

sinon le changement perdrait la nullité du coefficient du terme de degré $v(q - p\,(dy/dx))$. On prouve au lemme (§ 7) ci-après que $v(p) \geqslant \varepsilon$ dans ces conditions. Le changement ne modifie donc pas les a_i, $m < i < \delta \leqslant 2\varepsilon - 2n + m$, ni les a_i, $i \geqslant \delta$ qui restent nuls.

C.Q.F.D.

7. Lemme

Si A vérifie (CE), *l'inégalité* $v(q - p\,(dy/dx)) \geqslant 2v(p) - 2n + m$, *avec p et q dans A, implique* $v(p) \geqslant \varepsilon$.

Si $v(q - p\,(dy/dx)) = r$ est supérieur ou égal à c, c'est gagné car alors $p\,(dy/dx) \in A$, donc $v(p) \geqslant \varepsilon$, par définition de ε.

Sinon, on peut trouver p' et q', avec $v(p) = v(p')$ et $v(q' - p'\,(dy/dx)) > r$. En effet, il existe p'' et q'', avec $v(p'') = w(r)$, et $v(q'' - p''\,(dy/dx)) = r$ par définition de w, et on a $v(p'') > v(p)$, car

$$2v(p'') - 2n + m > r \geqslant 2v(p) - 2n + m \quad \text{d'après (CE).}$$

Il suffit de prendre $p' = p + \lambda p''$ et $q' = q + \lambda q''$, où λ est un nombre complexe convenable. Bien sûr, on a encore

$$v\left(q' - p'\frac{dy}{dx}\right) \geqslant 2v(p') - 2n + m.$$

En recommençant un nombre fini de fois cette construction, on se ramène au cas $r \geqslant c$ déjà traité.

8. Proposition

L'ensemble des classes d'isomorphisme des anneaux de Puiseux, ayant des invariants Γ_0, Δ_0, w_0, ε_0 *fixés, est isomorphe à un quotient d'un ensemble algébrique constructible. Si en outre les invariants vérifient* (CE) *et* (CU), *l'ensemble des classes est lui-même naturellement en bijection avec une partie constructible d'un espace projectif anisotrope.*

Tout d'abord, on sait comment $\Gamma(A(m, n, a))$ se calcule à partir des exposants caractéristiques (définis en [3], § 3). On a $\Gamma = \sum_{0 \leqslant i \leqslant g} \mathbf{N}\,\bar{\beta}_i$ avec $\bar{\beta}_0 = n = e_0$, $\bar{\beta}_1 = m$, $e_1 = \operatorname{pgcd}(m, n)$, $e_i = \operatorname{pgcd}(e_{i-1}, \beta_i)$ et $\bar{\beta}_i = \beta_i - \beta_{i-1} + \bar{\beta}_{i-1}\, e_{i-2}/e_{i-1}$ pour $1 < i \leqslant g$ [4].

La condition $\Gamma = \Gamma_0$ se traduit donc par un nombre fini de conditions $a_i = 0$ ou $a_i \neq 0$.

Comme une modification des a_i, $i \geqslant c$, ne change pas $A(m, n, a)$, on peut toujours supposer que $a_i = 0$ pour $i \geqslant c$ (c étant le conducteur).

On trouve ainsi un espace constructible, dont l'ensemble des classes d'anneaux de Puiseux, de monoïde caractéristique Γ_0, est un quotient. Soit E cet espace; on a $E \subset \mathbf{C}^{]m,c[}$.

Pour connaître Δ, w, ε, il suffit de connaître $\Delta \cap\,]m, c[$, et la restriction de w à $\Delta \cap\,]m, c[$, et ε.

On considère l'espace produit de E par l'espace L^2 des couples (p, q) de polynômes de $\mathbf{C}[X, Y]$ dont les monômes $X^i\, Y^j$ à coefficient non nuls vérifient $ni + mj < c$. On considère les fonctions α et β de $E \times L^2$ dans $\mathbf{N} \cup \{\infty\}$, définies par

$$\alpha(a, p, q) = v(p(x, y)) \qquad \text{et} \qquad \beta(a, p, q) = v\left(q(x, y) - p(x, y)\frac{dy}{dx}\right),$$

où v, x, y ont la signification déjà utilisée.

Ces deux fonctions sont évidemment semi-continues supérieurement pour la topologie de Zariski. On en déduit que $\beta^{-1}(r) \cap \alpha^{-1}(s)$ est une partie constructible de $E \times L^2$, et, puisque L^2 est de présentation finie sur $\mathbf{C}$, la projection sur E d'une partie constructible de $E \times L^2$ est une partie constructible de E.

Il en ressort que la partie de E, où $\Delta = \Delta_0$, $w = w_0$, $\varepsilon = \varepsilon_0$, est constructible, car elle s'interprète comme intersection de projections sur E de parties constructibles du produit $E \times L^2$.

En effet, $r \in \Delta$ s'écrit $a \in \pi\beta^{-1}(r)$, et $s = w(r)$ s'écrit :

$$a \in \pi(\beta^{-1}(r) \cap \alpha^{-1}(s) \cap \complement\, \alpha^{-1}(]s, r[)),$$

enfin $s = \varepsilon$ s'écrit

$$a \in \pi(\beta^{-1}(\infty) \cap \alpha^{-1}(s) \cap \complement\, \alpha^{-1}([n, s[)),$$

où π est la projection sur E.

La première affirmation est ainsi démontrée.

Si les invariants donnent lieu aux conditions (CE) et (CU), on obtient une bijection entre les classes d'isomorphisme des anneaux de Puiseux, dont les invariants ont les valeurs voulues, et le quotient par la relation d'homothétie de l'intersection F de la partie de E, où Δ, w, ε prennent les valeurs voulues, et du fermé défini par les équations $a_i = 0$, $i \in \Delta' \cap]m, c[$ en mettant en correspondance la classe de a, $a \in F$, et la classe de l'anneau $A(m, n, a)$ correspondant (tout ceci ne fait que répéter autrement la proposition (§ 6).

On a ainsi justifié la seconde affirmation.

9. Le cas des anneaux à une seule paire de Puiseux

Dans ce qui suit, m et n sont premiers entre eux, et $1 < n < m$. Pour toute suite $(a_i, i > m)$, l'anneau $A(m, n, a)$ est de Puiseux, et son monoïde caractéristique est $\Gamma = (\mathbf{N}m + \mathbf{N}n) \cup \{\infty\}$, et on a $c = (m-1)(n-1)$.

On va préciser les valeurs possibles pour Δ, w, ε, et en déduire que pour certaines valeurs de Δ, et en particulier pour la valeur générique de Δ, l'espace des classes d'anneaux est isomorphe à un ouvert d'un espace projectif anisotrope.

On écrira $A(a)$, ou seulement A, au lieu de $A(m, n, a)$ si aucune confusion n'est à craindre.

On étudie d'abord les propriétés des parties de $\mathbf{Z} \cup \{\infty\}$ sur lesquelles Γ opère par addition, à deux générateurs sur Γ.

10. Lemme

Soient p et q deux éléments de $\mathbf{Z}$ tels que $|p-q| \notin \Gamma$.

On pose

$$u = \inf(\Gamma+p)\cap(\Gamma+q) \qquad et \qquad \bar{u} = u+c-mn.$$

On définit v par $u+v = p+q+mn$ *et* $\bar{v} = v+c-mn$. *Les relations suivantes ont lieu :*

(i) $(\Gamma+p)\cap(\Gamma+q) = (\Gamma+u)\cup(\Gamma+v)$,

(ii) $(\Gamma+p)\cup(\Gamma+q) = (\Gamma+u-mn)\cap(\Gamma+v-mn)$,

(iii) $\mathbf{N}+\bar{v} \subset (\Gamma+p)\cup(\Gamma+q)$,

(iv) $(\mathbf{N}+\bar{u})\cap((\Gamma+p)\cup(\Gamma+q)) = (\Gamma+v-mn)\cap(\mathbf{N}+\bar{u})$.

On peut calculer u et v à partir de p et q comme suit : si $|p-q| \notin \Gamma$, *il existe un, et un seul, couple* $(\alpha, \beta) \in]0, n[\times]0, m[$ *tel que* $q-p = \alpha m-\beta n$; *alors u et v sont, à l'ordre près, les deux nombres* $p+\alpha m$ *et* $q+(n-\alpha)m$.

Si r est un élément de $\mathbf{Z}$ hors de $-\Gamma\cup\Gamma$, il se met de manière unique sous la forme $\alpha m-\beta n$, avec $\alpha \in [0, n[$ et $\beta \in \mathbf{Z}$. De plus, on a $\alpha \neq 0$, sinon r serait multiple de n, et $\beta > 0$, sinon r appartiendrait à $+\Gamma$, et $\beta < m$, sinon r appartiendrait à $-\Gamma$: en effet,

$$r = \alpha m-\beta n = (\alpha-n)m-(\beta-m)n.$$

Inversement, un élément $r \in \mathbf{Z}$ de la forme $\alpha m-\beta n$, avec $(\alpha,\beta) \in]0,n[\times]0,m[$ est hors de $\Gamma\cup(-\Gamma)$. S'il était égal à $\alpha' m+\beta' n$, avec α' et β' positifs ou nuls, on aurait $n(\beta'+\beta) = m(\alpha-\alpha') = kmn$, et $k \geqslant 1$ car $\beta+\beta' > 0$, et $k \leqslant 0$ car $\alpha-\alpha' < n$, ce qui est absurde. De même, on ne peut avoir α' et β' simultanément $\leqslant 0$ avec $r = \alpha' m+\beta' n = \alpha m-\beta n$.

Si donc $|p-q| \notin \Gamma$, il existe un, et un seul, couple

$$(\alpha, \beta) \in]0, n[\times]0, m[\qquad \text{tel que} \quad p+\alpha m = q+\beta n.$$

Alors on a aussi $p+(m-\beta)n = q+(n-\alpha)m$. Montrons que les deux nombres ainsi trouvés engendrent $(\Gamma+p)\cap(\Gamma+q)$. Bien évidemment, ils sont dans cette intersection, et on note que leur somme est $p+q+mn$. Si r est un élément de l'intersection, on a les relations

$$r = p+\lambda m+\mu n, \qquad 0 \leqslant \lambda < n, \quad 0 \leqslant \mu,$$

$$r = q+\lambda' m+\mu' n, \qquad 0 \leqslant \lambda' < n, \quad 0 \leqslant \mu',$$

d'où l'on tire

$$q-p = \alpha m-\beta n = (\lambda-\lambda')m+(\mu-\mu')n \qquad \text{avec} \quad |\lambda-\lambda'| < n.$$

Alors de deux choses l'une :

ou bien $\lambda-\lambda' = \alpha$, et donc $\mu \geqslant 0$ et $\lambda \geqslant \alpha$, donc $r \in \Gamma+p+\alpha m$;

ou bien $\lambda-\lambda' = \alpha-n$, et donc $\mu' \geqslant 0$ et $\lambda' \geqslant n-\alpha$, donc

$$r \in \Gamma+q+(n-\alpha)m.$$

On a ainsi prouvé (i), et justifié le calcul de u et v. Comme

$$v-u = |\alpha m-(m-\beta)n| \notin \Gamma,$$

on peut encore appliquer (i) à u et v au lieu de p et q, ce qui donne (ii) en translatant de $-mn$ les deux membres de l'égalité obtenue.

On trouve alors (iii) et (iv) en intersectant les deux membres de (ii) avec $\mathbf{N}+\bar{v}$ et $\mathbf{N}+\bar{u}$, compte tenu des inclusions

$$\mathbf{N}+\bar{v} \subset \mathbf{N}+\bar{u} \quad \text{et} \quad \mathbf{N}+\bar{u} \subset \Gamma+u-mn \quad \text{et} \quad \mathbf{N}+\bar{v} \subset \Gamma+v-mn.$$

Remarque. — On a vu en passant qu'il existe une bijection de $]0, n[\times]0, m[$ vers le complémentaire dans $\mathbf{Z}$ de $\Gamma \cup -\Gamma$, définie par $(\alpha, \beta) \to \alpha m-\beta n$. Ceci permet de retrouver la formule du conducteur : $c = (m-1)(n-1)$, et la formule d'Apéry : le complémentaire de Γ dans $\mathbf{N}$ possède $c/2$ éléments, dans ce cas particulier.

Précisons maintenant les propriétés de Δ et ses rapports avec w et ε.

11. Notations

Soit $g_{-1} < g_0 < g_1 < \ldots < g_J$ le générateur minimal du Γ-ensemble Δ. On pose

$$E_i = \bigcup_{-1 \leqslant j \leqslant i} (\Gamma+g_j) \qquad \text{pour} \quad -1 \leqslant i \leqslant J.$$

On a donc $\Delta = E_J$ et $g_i \notin E_{i-1}$, pour $0 \leqslant i \leqslant J$. On pose aussi

$$u_i = \inf(\Gamma+g_i) \cap E_{i-1} \qquad \text{pour} \quad 0 \leqslant i \leqslant J.$$

On a évidemment $g_{-1} = 0$ et $g_0 = m-n$.

On choisit des éléments ω_i de $Ad\, A$, tels que $v(\omega_i) = g_i$, en particulier $\omega_0 = dy/dx$ et $\omega_{-1} = 1$.

On pose en outre $g_{J+1} = \infty$ et $\omega_{J+1} = 0$.

12. Lemme

Pour tout entier $l \in [0, J]$, *on a, en posant* $\bar{u}_l = u_l + c - mn$;

(*a*) *il existe un nombre* $c_l \in \mathbf{Z}$ *tel que*

$$(\mathbf{N} + \bar{u}_l) \cap E_l = (\mathbf{N} + \bar{u}_l) \cap (\Gamma + c_l),$$

(*b*) *il existe une relation* $\omega_{l+1} = \sum_{-1 \leqslant j \leqslant l} F_{j,\,l}\, \omega_j$, *où les* $F_{j,\,l}$ *sont des éléments de* A, *avec* $u_l = v(F_{l,\,l}) + g_l = \inf \{ v(F_{j,\,l}) + g_j \}$.

On procède par récurrence sur l de la façon suivante :

1er *point :* (*a*) est vrai pour $l = 0$;

2e *point :* (*a*) est vrai pour $l = i+1$ si (*a*) et (*b*) sont vrais pour $l = i$;

3e *point :* (*b*) est vrai pour $l = i$ si (*a*) et (*b*) sont vrais pour tout $l < i$.

Si les trois points sont démontrés, le lemme est visiblement établi aussi.

Preuve du 1er *point.* — C'est le lemme (§ 10), avec $p = 0$ et $q = m - n$. On a $u_0 = m = u$ et $c_0 = -n = v - mn$.

Preuve du 2e *point.* — On sait, par hypothèse, que

$$(\mathbf{N} + \bar{u}_i) \cap E_i = (\mathbf{N} + \bar{u}_i) \cap (\Gamma + c_i),$$

et aussi que g_{i+1} est au moins égal à u_i, donc $g_{i+1} \in (\mathbf{N} + \bar{u}_i)$. Comme $g_{i+1} \notin E_i$, on en déduit $g_{i+1} \notin (\Gamma + c_i)$. Comme de plus on a $g_{i+1} \geqslant u_i \geqslant c_i$, on peut appliquer le lemme (§ 10) avec p et q égaux à g_{i+1} et c_i, ce qui donne $c_{i+1} = c_i + g_{i+1} - u_{i+1}$.

Preuve du 3e *point.* — Elle peut se faire en 3 étapes.

1ere *étape :* On sait *a priori* que ω_{i+1} peut se mettre sous la forme $\sum_{-1 \leqslant j \leqslant 1} f_j\, \omega_j$, par exemple $q - p\ (dy/dx)$. Montrons qu'on peut se ramener au cas où $g_j + v(f_j) \geqslant v(f_i) + g_i \geqslant u_i$ et même, si $i < J$, $v(f_i) + g_i \in (\Gamma + u_i)$. On dit alors que la décomposition de ω_{i+1} sur les ω_j, $-1 \leqslant j \leqslant i$ est améliorée.

De l'égalité $\omega_{i+1} = \sum_{-1 \leqslant j \leqslant i} f_j\, \omega_j$, on tire, ou bien $i = J$ et $f_j = 0$ pour tout j, ce qui convient, ou bien l'inégalité stricte

$$v(\omega_{i+1}) > e(f) = \inf \{ v(f_j \omega_j),\ -1 \leqslant j \leqslant i \}.$$

Dans cette occurrence, on appelle $h(f)$ et $k(f)$ les deux plus grands indices j tels que $v(f_j) + g_j = e(f)$, avec $h < k$ (il y a certainement plusieurs valeurs de j où $v(f_j\, \omega_j)$ prend sa valeur minimale). Alors on a $v(f_k) + g_k \in E_h \subset E_{k-1}$.

En appliquant le lemme (§ 10), on voit que, ou bien $v(f_k)+g_k \in (\Gamma+c_k+mn)$, ou bien $v(f_k)+g_k \in (\Gamma+u_k)$.

La première possibilité implique $g_{k+1} \in (\mathbf{N}+g_k+v(f_k)) \cup \{\infty\} \subset E_k$, ce qui est absurde si $k \neq J$, mais convient sinon.

La deuxième possibilité convient si $k = i$. Si $k < i$, il existe une fonction $z \in A$ telle que $v(f_k+z F_{k,k}) > v(f_k)$. On a alors :

$$\omega_{i+1} = \sum_{-1 \leqslant j \leqslant i} f'_j \omega_j,$$

où $f'_j = f_j$ si $j > k+1$, et $f'_j = f_j+z F_{j,k}$ si $j \leqslant k$ et $f'_{j+1} = f_{k+1}-z$. On constate que, ou bien $e(f') > e(f)$, ou bien $e(f') = e(f)$, et $k(f') < k(f)$. Par conséquent, un nombre fini d'opérations semblables à celle qui fait passer de f à f' fournit une décomposition améliorée.

2e *étape :* On sait *a priori* qu'il existe un élément θ de $Ad\,A$, de valuation $v(\theta) > u_i$, tel que $\theta = \sum_{-1 \leqslant j \leqslant i} \Phi_j \omega_j$, avec

$$u_i = \inf\{v(\Phi_j)+g_j\} = v(\Phi_i)+g_i,$$

par exemple $z' \omega_j + z \omega_i$, avec $v(z) = u_i-g_i$ et $v(z') = u_i-g_j$, si $u_i \in (\Gamma+g_j)$, $j < i$. Montrons qu'on peut toujours supposer $v(\theta) \geqslant g_{i+1}$. Alors θ sera dit extrême.

Si $v(\theta) \in E_i$, il existe $\theta' = z'' \omega_k + \theta$, avec $v(\theta') > v(\theta)$, et

$$\theta' = \sum_{-1 \leqslant j \leqslant i} \Phi'_j \omega_j \qquad \text{avec} \quad \Phi'_k = z''+\Phi_k$$

et $\Phi'_j = \Phi_j$, si $j \neq k$. On constate que la condition sur les valuations est encore vérifiée. On peut recommencer jusqu'à obtenir $v(\theta) \geqslant g_{i+1}$ si $i < J$, ou $v(\theta) \geqslant c$ si $i = J$; dans ce dernier cas, une modification du même genre portant sur Φ_{-1} permet de ramener en un coup à $v(\theta) = \infty = g_{J+1}$.

3e *étape :* Il faut maintenant montrer que si θ est extrême, alors $v(\theta)$ est g_{i+1}, et que si $i < J$ et si f est améliorée, alors $v(f_i) = u_i-g_i$. Comme fonctions $F_{j,i}$, on prendra donc les f_j si $i < J$, et on prendra les Φ_j si $i = J$.

Le cas $i = J$ est, en fait, déjà traité dans la 2e étape.

Dans le cas $i < J$, on procède par l'absurde. Si θ est extrême et si f est améliorée, on a $v(\theta) \geqslant g_{i+1}$ et $v(f_i)+g_i \geqslant u_i$. Supposons que l'une au moins de ces deux inégalités est stricte. Comme $v(f_i)+g_i \in (\Gamma+u_i)$, il existe $z \in A$ avec $v(f_i+z\Phi_i) > v(f_i)$. Soit

$$\omega'_{i+1} = \omega_{i+1}+z\theta = \sum_{-1 \leqslant j \leqslant i} f''_j \omega_j \qquad \text{où} \quad f''_j = f_j+z\Phi_j.$$

D'après l'hypothèse à démentir, on a $v(z\theta) > v(\omega_{i+1})$, et donc $v(\omega'_{i+1})$ est encore égal à g_{i+1}. On constate aussi que $v(f''_j)+g_j \geqslant v(f_i)+g_i$. Comme $v(f''_i) > v(f_i)$, on a soit $e(f'') > e(f)$, soit $e(f'') = e(f)$, et $k(f'') < i$. En améliorant la décomposition de ω'_{i+1}, on trouvera

$$\omega'_{i+1} = \sum f'_j \omega_j \qquad \text{avec} \quad e(f') > e(f).$$

L'hypothèse à démentir sur θ et ω_{i+1} est encore vraie sur θ et ω'_{i+1}. On peut recommencer. Comme le nombre e croît strictement chaque fois, mais ne devrait pas dépasser g_{i+1}, on trouve une contradiction.

C.Q.F.D.

13. Remarques

Au cours de cette démonstration, on a vu que le calcul des éléments extrêmes permet en fait de trouver les générateurs g_j de Δ et de construire des éléments ω_j de valuation convenable, de proche en proche à partir de ω_0 et ω_{-1}.

On a pu observer aussi l'inégalité $g_{i+1} > u_i$, et l'égalité

$$c_i+u_i = m-n+\sum_{0\leqslant j<i}(g_{j+1}-u_j).$$

On pose

$$s_{k+1} = \sum_{0\leqslant j\leqslant k}(g_{j+1}-u_j) \qquad \text{pour} \quad 0 \leqslant k < J \quad \text{et} \quad s_0 = 0.$$

14. Proposition

Dans le cas où il n'y a qu'une paire de Puiseux, les invariants w et ε ne dépendent que de Δ et Γ.

Explicitement, on a les formules suivantes, avec les notations déjà utilisées :

si $r \in \Gamma$, $w(r) = \infty$;

si $r \in E_k$ *et* $r \notin E_{k-1}$, *avec* $0 \leqslant k \leqslant J$,

$$w(r) = r-s_k-m+n = r-c_k-u_k, \qquad \varepsilon = u_J-s_J-m+n = -c_J.$$

Les décompositions améliorées $\omega_{i+1} = \sum F_{j,i}\,\omega_j$, $0 \leqslant i \leqslant J$, vont donner des égalités $\omega_{i+1} = q_{i+1}-p_{i+1}\,(dy/dx)$, avec $p_{-1}=q_0=0$ et $q_{-1}=1=-p_0$, les autres p_i et q_i étant donnés par récurrence, selon la règle $p_{i+1} = \sum F_{j,i}\,p_j$ et $q_{i+1} = \sum F_{j,i}\,q_j$.

Montrons que, pour $l \geqslant 0$, on a $v(p_{l+1}) = v(p_l)+u_l-g_l$, et que $v(p_0) = 0$. La deuxième égalité est triviale, montrons la première par récurrence : Si elle est vérifiée pour $0 \leqslant i < l$, est-elle vraie pour $i = l$?

Il s'agit de voir que $v(F_{j,l})+v(p_j)$ atteint son minimum une seule fois, pour $j = l$, car on sait que $v(F_{l,l}) = u_l-g_l$.

Pour $j = -1$, $v(F_{j,l})+v(p_j) = \infty$. Pour $0 \leqslant j < l$, on a

$$g_j+v(F_{j,l}) \geqslant g_l+v(F_{l,l}),$$

donc

$$v(F_{j,l})+v(p_j)-(v(F_{l,l})+v(p_l))$$

est au moins égal à $v(p_j)-v(p_l)+g_l-g_j$ qui vaut, d'après l'hypothèse de récurrence,

$$g_l-g_j-\textstyle\sum_{j\leqslant i<l}(u_i-g_i) = \sum_{j<i\leqslant l} g_i-u_{i-1},$$

ce qui est strictement positif.

C. Q. F. D.

Ceci prouve déjà que $\varepsilon \leqslant v(p_{J+1}) = u_J-s_J+n-m = -c_J$, et que

$$w(g_i) \geqslant v(p_i) = g_i-s_i+n-m = -c_{i-1}, \qquad 0 \leqslant i \leqslant J,$$

en posant $c_{-1} = 0$.

On en déduit $w(r) \geqslant r-s_k+n-m$ si $r \in E_k$, compte tenu de l'inégalité évidente $w(r+\gamma) \geqslant w(r)+\gamma$, si $\gamma \in \Gamma$.

Soit $\lambda = \sum_{-1\leqslant i\leqslant J+1} f_i\,\omega_i$ un élément de $Ad\,A$, et soit $P = \sum f_i p_i$. On ne modifie ni λ ni P si on change f en f', avec $f_j-f'_j = 0$ si $j > k+1$, avec $f_j-f'_j = z\,F_{j,k}$ si $-1 \leqslant j \leqslant k$, et $f'_{k+1}-f_{k+1} = z$.

Si $v(f_k)+g_k \in E_{k-1}$, alors ou bien $v(f_k)+g_k \in (\Gamma+u_k)$, ou bien $v(f_k)+g_k \in (\Gamma+c_k+mn)$ et, dans ce cas,

$$v(f_k)+g_k \geqslant c_k+mn \geqslant c_J+mn > u_J.$$

Donc si $e(f) < u_J$, et si $e(f) = \inf\{\, v(f_i)+g_i \,\}$ est atteint plusieurs fois, l'indice le plus grand pour lequel ce minimum est atteint étant appelé $k(f)$, on peut, sans changer λ ni P, trouver une décomposition f' telle que ou bien $e(f') > e(f)$, ou bien $e(f') = e(f)$, et $k(f') < k(f)$.

Si $\lambda = 0$, on peut se ramener de la sorte à $e(f) \geqslant u_J$. Alors

$$v(f_i)+v(p_i) \geqslant e(f)-g_i+v(p_i) = e(f)-s_i+n-m \geqslant u_J-s_J+n-m$$

si $0 \leqslant i \leqslant J$,

$$v(f_{-1})+v(p_{-1}) = \infty > -c_J \qquad \text{et} \qquad v(f_{J+1})+v(p_{J+1}) \geqslant v(p_{J+1}) = -c_J.$$

Ceci termine le calcul de ε.

On veut montrer maintenant la formule pour w. On la connaît déjà pour $r \in E_0$. On procède encore par étapes pour les autres valeurs de r.

1ere *étape :* on se ramène au cas $r = c_{K-1}+c-1$, $0 \leqslant K \leqslant J$.

Avec les notations du lemme (§ 10), si on pose $\sigma = q+c-1$, alors $r \in \complement(\Gamma+q) \cap (\Gamma+p)$ implique $\sigma \in (\Gamma+r)$. En effet, la condition sur r implique $r-p = \rho m+\mu n$, avec $\rho < \alpha$ et $\mu < m-\beta$, et on a

$$\sigma-p = (\alpha-1)m+(m-\beta-1)n.$$

On observe encore que $\sigma \in \complement(\Gamma+q) \cap (\Gamma+p)$ et $(\mathbf{N}+1+\sigma) \subset (\Gamma+q)$.

On applique ceci avec $p = g_K$ et $q = c_{K-1}$. Si on démontre l'égalité cherchée pour $c_{K-1}+c-1$, elle sera prouvée pour les autres éléments de E_K hors de E_{K-1}, compte tenu de l'inégalité $w(r+\gamma) \geqslant w(r)+\gamma$, si $\gamma \in \Gamma$.

2e *étape :* si $v(P) > (c_{K-1}+c-1)-s_K+n-m = c-g_K-1$, alors

$$v\left(Q-P\frac{dy}{dx}\right) \in E_{K-1}.$$

Ceci assure en effet que $w(c_{K-1}+c-1)$ a bien la valeur souhaitée $c-g_K-1$.

Soit donc $\lambda = Q-P(dy/dx) \in \mathrm{Ad}\, A$. Nous allons construire de proche en proche des décompositions $\lambda = \sum f_i \omega_i$ avec $P = \sum f_i p_i$, et

(1) $j(f) \leqslant K$, $v(f_{j(f)})+g_{j(f)} = v(P)+s_{j(f)}+m-n$;

(2) Si $j(f) > 0$ et $j(f) > k(f)$, les inégalités $j(f) \geqslant k(f)+1$ et $e(f) \geqslant v(f_{j(f)})+u_{j(f)-1}$ ont lieu, l'une au moins étant stricte. $j(f)$, $e(f)$, $k(f)$ sont le plus petit indice i tel que $f_i \neq 0$, la plus petite valuation $v(f_i)+g_i$, le plus grand indice i tel que $v(f_i)+g_i = e(f)$.

La première décomposition est $\lambda = Q-P(dy/dx)$, qui convient. Si on a une décomposition vérifiant (1) et (2), dans chacun des cas (*a*), (*b*), (*c*), on a la conclusion et dans le cas (*d*) on modifie la décomposition comme il sera dit. Comme alors $e(f)$ croît ou $k(f)$ décroît, et comme $k(f) \geqslant -1$ et $e(f) \leqslant v(\lambda)$, on ne peut faire qu'un nombre fini de modifications. Ce qui prouve bien la deuxième étape.

(*a*) $k(f) = K$; alors :

$$v(\lambda) \geqslant v(f_K)+g_K = v(P)+s_K+m-n \geqslant c_{K-1}+c,$$

donc $v(\lambda) \in E_{K-1}$;

(*b*) $k(f) < K$ et $e(f)$ n'est atteint qu'une fois; alors :

$$v(\lambda) = v(f_{k(f)}) + g_{k(f)} \in E_{k(f)} \subset E_{K-1};$$

(*c*) $k(f) < K$ et $e(f)$ est atteint deux fois, et $e(f) \in \Gamma + mn + c_{k(f)}$, alors $v(\lambda) \geqslant e(f)$ appartient à E_{K-1};

(*d*) Si aucune de ces conditions n'est vérifiée, on a $k = k(f) < K$, $e(f)$ est atteint deux fois, et $e(f) \in \Gamma + u_k$. On remplace f par

$$f' = f + z(\omega_{k+1} - \sum F_{ki}\omega_i)$$

(*cf.* § 12), où $z \in A$ est choisi de façon que $v(f'_k) > v(f_k)$, donc

$$v(z) = v(f_k) + g_k - u_k.$$

On a encore $P = \sum f'_i p_i$. Si $k(f) = j(f)$, alors $j(f') = j(f) + 1 = k+1$ et $f'_{k+1} = z$, d'où (1) et (2), car

$$s_{k+1} = s_k + g_{k+1} - u_k \qquad \text{et} \qquad e(f') \geqslant e(f) = u_k + v(z),$$

et

$$v(f'_k) + g_k > u_k + v(z).$$

Si $k(f) + 1 < j(f)$, on a $j(f) = j(f')$ et $f'_{j(f)} = f_{j(f)}$, donc encore (1) et (2). Enfin si $k(f) + 1 = j(f)$, on a, par (2), $v(z) > v(f_{j(f)})$, donc $j(f) = j(f')$, et $v(f_{j(f)}) = v(f_{j(f)})$, d'où encore (1) et (2).

On va maintenant donner des précisions sur les espaces signalés à la proposition (§ 8), dans le cas où il n'y a qu'une paire de Puiseux. L'espace E est l'espace des suites $(a_i,\ m < i < c)$.

15. Proposition

La partie de E où Δ (*et aussi w et* ε) *prend une valeur constante est donnée par un nombre fini de conditions* $a_i = \psi_{i,\Delta}(a_j,\ m < j < i)$ *et de conditions* $a_i \neq \psi_{i,\Delta}(a_j,\ m < j < i)$, *où* $\psi_{i,\Delta}$ *est une fraction rationnelle homogène dont le dénominateur est inversible sur la partie considérée.*

Si Δ *est tel que* (CE) *et* (CU) *sont vérifiées, l'ensemble des classes d'isomorphisme des anneaux ayant pour invariants* Γ *et* Δ *est en bijection avec un ouvert d'un espace projectif anisotrope.*

On considère l'anneau de polynômes $\mathbf{C}[X_1, \ldots, X_b, T]$, où $b = c - m - 1$. On le munit de la graduation où les X_i sont homogènes de degré i et où T est homogène de degré -1.

On définit les polynômes homogènes particuliers $Y = T^m(1+\sum X_i T^i)$, $\Omega_{-1} = 1$ et $\Phi_0 = (1/n)\, T^{m-n}(m+\sum (m+i)\, X_i T^i)$ et $R(\gamma)$; si $\gamma \in (0, mn(\cap \Gamma$, il existe un unique couple $(\alpha, \beta) \in \mathbf{N}\times\mathbf{N}$ tel que $\gamma = \alpha m+\beta n$; alors $R(\gamma) = T^{\beta n}\, Y^{\alpha}$.

On définit un morphisme d'anneaux $\mathbf{C}[X, T] \to B$, $X_i \to a_{i+m}$ et $T \to t$. L'image de $P \in \mathbf{C}[X, T]$ est appelée $P(a)$.

On suppose maintenant qu'un ensemble Δ est donné, compatible avec la condition nécessaire $g_{i+1} > u_i$. On cherche pour quelles valeurs de a on a $\Delta(A(a)) = \Delta$.

On va définir des classes de polynômes homogènes :

$$\mathscr{P}(i, s) \subset \mathbf{C}[X_1, \ldots, X_s] \quad \text{pour} \quad 1 \leqslant i \leqslant J+1 \quad \text{et} \quad s \leqslant b,$$
$$\mathscr{S}(i, s) \subset \mathbf{C}[X_1, \ldots, X_b, \mathrm{T}] \quad \text{pour} \quad 1 \leqslant i \leqslant J+1 \quad \text{et} \quad s \leqslant b.$$

On va définir des polynômes homogènes :

$$\Omega_i \in \mathscr{S}(i, s_i) \quad 1 \leqslant i \leqslant J \qquad \text{avec} \quad v(\Omega_i(a)) = g_i,$$
$$K_{i,s} \in \mathscr{P}(i, s) \qquad 1 \leqslant i \leqslant J+1,$$
$$L_i \in \mathscr{P}(i, s_i) \quad -1 \leqslant i \leqslant J,$$

avec déjà

$$L_{-1} = 1 \qquad \text{et} \qquad L_0 = \frac{m}{n}.$$

On va montrer que la relation $\Delta(A(a)) = \Delta$ est équivalente à

$$K_{l,s}(a) = 0 \qquad \textit{pour} \quad 1 \leqslant l \leqslant J+1$$

et

$$s \in]s_{l-1}, \qquad s_l[\cap \complement(E_{l-1}-h_l),$$

où on a posé $h_i = v(p_i)+m-n$ *et* $s_{J+1} = s_J+c_J+mn-u_J$,

$$L_l(a) \neq 0 \qquad \textit{pour} \quad 1 \leqslant l \leqslant J.$$

Pour cela, on procède par récurrence sur l.

On sait déjà que $g_{-1} = 0 = v(\Omega_{-1}(a))$ et $g_0 = m-n = v(\Omega_0(a))$, et que L_{-1} et L_0 sont les coefficients des termes de plus bas degré en T de Ω_{-1} et Ω_0. Ceci est le point de départ de la récurrence. Pour faire avancer la récurrence, on va prouver que si on a défini les objets annoncés pour i, $0 < i < l \leqslant J$, si les L_i sont les coefficients des termes de plus bas degré en T des Ω_i pour $-1 \leqslant i < l$, et si les conditions $g_i(a) = g_i$ équivalent aux conditions $K_{l,s}(a) = 0$, $L_i(a) \neq 0$ pour $i \in]-1, l[$ et s appartenant à l'ensemble indiqué, alors on peut en faire autant pour $i = l$.

On appelle $\mathscr{P}(l, s)$ la classe des polynômes homogènes de $\mathbf{C}[X_1, \ldots, X_s]$ de la forme UX_s+V, où $V \in \mathbf{C}[X_1, \ldots, X_{s-1}]$, et où U est un produit de puissances des L_k, $k \in]-1, l[$ et d'une constante non nulle.

On appelle $\mathscr{S}(l, s)$ la classe des polynômes homogènes de $\mathbf{C}[X, T]$, dont le coefficient de T^q est nul si $q < h_l+s$ appartient à $\mathscr{P}(l, q-h_l)$ si $q \in [h_l+s, b]$, et est quelconque si $q > b$.

On forme, par récurrence sur α, $s_{l-1} \leqslant \alpha \leqslant s$, des polynômes U_α appartenant à $\mathscr{S}(l, \alpha)$.

Pour $\alpha = s_{l-1}$, on prend $U_\alpha = R(u_{l-1}-g_{l-1})\,\Omega_{l-1}$. C'est un élément de $\mathscr{S}(l, s_{l-1})$.

Pour passer de U_α à $U_{\alpha+1}$ si $\alpha < s_l$, il y a deux possibilités :

si $\beta = h_l+\alpha \in E_k \cap \complement E_{k-1}$, $-1 \leqslant k < l$, on prend

$$U_{\alpha+1} = L_k U_\alpha - K_{l,\alpha} R(\beta-g_k)\Omega_k,$$

où $K_{l,\alpha}$ est le coefficient de T^β dans U_α. Il est facile de vérifier que si $U_\alpha \in \mathscr{S}(l, \alpha)$, alors $U_{\alpha+1} \in \mathscr{S}(l, \alpha+1)$;

si $\beta \notin E_{l-1}$, alors $K_{l,\alpha}(a)$ est nul, sinon β serait $g_l(a)$. On prend

$$U_{\alpha+1} = U_\alpha - K_{l,\alpha} T^\beta.$$

C'est évidemment un élément de $\mathscr{S}(l, \alpha+1)$.

On arrive ainsi à U_α, avec $\alpha = s_l$. Si $l = J+1$, c'est terminé, car $s_{J+1}+h_{J+1} = c_J+mn$, donc $(\mathbf{N}+s_{J+1}+h_{J+1}) \subset E_J$. Si $l \leqslant J$, on a $K_{l,\alpha}(a) \neq 0$, car alors $\beta = g_l(a)$. On prend donc $K_{l,\alpha} = L_l$ et $\Omega_l = U_\alpha$. Evidemment U_l et L_l satisfont les relations voulues.

On vient également de voir que si les $g_k(a)$, $-1 \leqslant k < l$ sont égaux aux g_k donnés, pour que $g_l(a)$ soit bien le g_l donné, il faut et il suffit que les $K_{l,s}(a)$, $s \in]s_{l-1}, s_l[\cap \complement(E_{l-1}-h_l)$ soient nuls et, si $l \leqslant J$, que $L_l(a)$ ne soit pas nul.

C. Q. F. D.

Compte tenu de la forme particulière des polynômes $K_{l,s}$ et L_l qui interviennent, la première affirmation est justifiée.

Soit H le complémentaire dans $\mathbf{N}$ de

$$(\Delta'-m) \cup \left(\bigcup_{1 \leqslant i \leqslant J+1}]s_{l-1}, s_l[\cap \complement(E_{l-1}-h_l)\right),$$

et soit $\mathbf{P}$ le quotient de $\mathbf{C}^H$ par l'homothétie anisotrope (c'est-à-dire $(b_i, i \in H)$ et $(b_i, i \in H)$ sont homothétiques s'il existe $\gamma \in \mathbf{C}$, $\gamma \neq 0$ avec $b_i = \gamma^i b'_i$ pour tout $i \in H$).

On met naturellement en bijection les classes d'isomorphisme des anneaux de Puiseux ayant Γ et Δ comme invariants, tels que (CE) et (CU) soient vérifiées, et les classes d'homothétie des suites $(a_i,\ m < i < c,\ i \notin \Delta')$ vérifiant les relations $K_{l,\,s}(a) = 0$ et $L_l(a) \neq 0$ pour les valeurs convenables de l et s : la bijection est obtenue en associant la classe de $(a_i,\ m < i < c,\ i \notin \Delta')$ et la classe de l'anneau $A(a)$, étant entendu que $a_i = 0$ si $i \in \Delta'$.

Compte tenu de la forme particulière des polynômes K et L intervenant, l'espace des classes d'homothétie des suites décrites est lui-même en bijection avec l'ouvert de $\mathbf{P}$ défini par $\prod_{s \in S} b_s \neq 0$, où $S = \{ s_l,\ 1 \leqslant l \leqslant J \}$; on prend $b_s = a_{m+s}$ si $s \in H$ et $s \notin S$, et on prend $b_s = a_{m+s} - (V_i(a)/U_i(a))$ si $s = s_i$ et $L_i = U_i X_s + V_i$. L'ensemble S est vide si, et seulement si, $J = 0$, c'est-à-dire $\Delta = E_0$, ce qui est compatible avec (CE), mais est compatible avec (CU) si, et seulement si, $2\varepsilon - 2n + m \geqslant \delta$, ce qui est ici tout calculé : $-2n - 2n + m \geqslant c - n$, ou encore $(n-2)(m-2) \leqslant 3$. Ceci se produit dans 3 cas seulement : $n = 2$ et m impair $\geqslant 3$, $n = 3$ et $m = 4$, $n = 3$ et $m = 5$.

Dans chacun de ces 3 cas, toutes les singularités sont isomorphes, d'anneau isomorphe à $\mathbf{C}[[t^n, t^m]] = A(m, n, 0)$.

Dans les autres cas, S n'est pas vide, et l'ouvert de P est un ouvert affine d'un espace projectif anisotrope (singulier parfois). C'est un espace dont la dimension est le nombre d'éléments de H, diminué de 1 (on note que H n'est pas vide, car $S \subset H$).

16. Définition

On définit un ensemble $\Delta(m, n) \subset \mathbf{N} \cup \{ \infty \}$, sur lequel

$$\Gamma = (\mathbf{N}n + \mathbf{N}m) \cup \{ \infty \}$$

opère par addition, de la manière suivante :

On pose $g_{-1} = 0$ et $g_0 = m - n$, et $E_{-1} = \Gamma$, puis par récurrence,

$$u_i = \inf((\Gamma + g_i) \cap E_{i-1}),$$

$$E_i = E_{i-1} \cup (\Gamma + g_i) \qquad \text{et} \qquad g_{i+1} = \inf((\mathbf{N} + u_i) \cap E_i)$$

pour $i \geqslant 0$. On appelle J le plus petit indice i tel que $\mathbf{N} + u_i \subset E_i$, ou, ce qui revient au même, tel que $g_{i+1} = \infty$. Alors $\Delta(m, n) = E_J$.

On dit que $A(m, n, a)$ est générique si son invariant $\Delta(A(m, n, a))$ est égal à $\Delta(m, n)$.

17. Lemme

Tout anneau générique vérifie (CE) *et* (CU).

Si $r \in \Gamma$, alors $w(r) = \infty$, et $r < 2w(r) - 2n + m$ ou $r = \infty \notin \Delta'$.

Si $r \notin \Gamma$ et $r \in (\Gamma + m - n)$ et $r > m$, alors $2w(r) - 2n + m = 2r - m > r$.

Montrons que $(g_i - s_i, g_i) \subset \Delta = \Delta(m, n)$ pour $0 \leqslant i \leqslant J$. C'est vrai pour $i = 0$, car $s_0 = 0$. Si c'est vrai pour $i < J$, c'est vrai pour $i+1$, car l'addition de $u_i - g_i \in \Gamma$ donne $(u_i - s_i, u_i) \subset \Delta$, et $u_i - s_i = g_{i+1} - s_{i+1}$, et la définition de g_{i+1} « générique » donne $(u_i, g_{i+1}) \subset \Delta$.

On en déduit aisément $s_J < n$; sinon $g_J - n$ serait dans Δ et non dans $\Gamma + g_J$, donc dans E_{J-1}, et g_J serait aussi dans E_{J-1}.

On voit aussi que $u_i - g_i \in \Gamma$, et $u_i - g_i > 0$ implique $u_i - g_i \geqslant n$, pour $0 \leqslant i \leqslant J$. Donc $g_k - s_k - m + n \geqslant nk$ si $0 \leqslant k \leqslant J$, et $u_J - s_J - m + n \geqslant n(J+1)$.

Si $r \in \Delta$, $r \notin E_0$, $r \neq v = g_1$, montrons que l'on a (CE), c'est-à-dire $E = 2w(r) - 2n + m - r > 0$. Soit k le plus petit entier tel que $r \in E_k$. On a

$$E = r - 2s_k - m = (r - g_k) - s_k + (g_k - s_k - m + n) - n > (r - g_k) + (k-2)n.$$

Si $k \geqslant 2$, on a $E > 0$, si $k = 1$, on a $0 \neq r - g_1 \in \Gamma$, donc $r - g_1 \geqslant n$, donc $E > 0$.

On voit aussi que $\mathbf{N} + u_J \subset \Delta$, donc aussi $\mathbf{N} + u_J - s_J \subset \Delta$, c'est-à-dire $u_J - s_J \geqslant \delta$. En outre, $u_J - s_J - m \geqslant nJ$. On en tire l'inégalité :

$$2\varepsilon - 2n + m = 2u_J - 2s_J - m \geqslant \delta + u_J - s_J - m \geqslant \delta + nJ \geqslant \delta,$$

c'est-à-dire (CU).

18. Proposition

Il existe un ouvert non vide $U \subset E$, tel que la condition « $a \in U$ » soit équivalente à « $A(a)$ est générique » (ce qui justifie l'appellation générique).

L'espace des modules des singularités génériques, c'est-à-dire l'espace des classes d'isomorphisme des anneaux génériques, est un ouvert affine d'un espace projectif anisotrope, dont la dimension est le nombre d'éléments du complémentaire dans $\mathbf{N} + m$ de Δ.

On applique la proposition 15. Comme les ensembles

$$]s_{l-1}, s_l[\cap \complement(E_{l-1} - h_l),\ 1 \leqslant l \leqslant J+1$$

sont vides, la partie de E, où Δ prend la valeur générique, est donnée par $0 \neq \prod_{1 \leqslant l \leqslant J} L_l(a)$. Autrement dit, chacun des a_{s+m}, $s \in S$, doit être différent d'une valeur particulière qui se calcule à partir des a d'indice plus petit.

L'espace des modules s'obtient, d'après le paragraphe 8, en coupant U par le fermé $a_i = 0$ pour tout $i \in \Delta'$ et en passant au quotient par l'homothétie (où a_i est affecté du degré $i-m$). D'où la conclusion, aisément obtenue, en traitant séparément les cas particuliers $n = 2$ et m entier impair > 2, $n = 3$ et $m = 4$, $n = 3$ et $m = 5$, déjà examinés au cours de la démonstration du paragraphe 15.

On s'attache maintenant au calcul de la dimension de cet espace.

19. Définition

A un couple d'entiers $\geqslant 2$ premiers entre eux, on associe le monoïde $\Gamma_{m,n} = (\mathbf{N}\,m+\mathbf{N}\,n) \cup \{\infty\}$, la fonction $f_{m,n} : \mathbf{N} \to \mathbf{Z}$, définie par

$$f_{m,n}(k) = k - \mathrm{card}\,([m,\ m+k[\cap \Gamma_{m,n}) - \mathrm{card}\,([n,\ n+k[\cap \Gamma_{m,n}),$$

et le nombre $D_{m,n} = \sup_{k \in \mathbf{N}} f_{m,n}(k)$.

Evidemment $D_{m,n} = D_{n,m} \geqslant 0 = f_{m,n}(0)$ et $D_{m,n}$ est fini, car $k \geqslant c$ implique $f_{m,n}(k+1) = f_{m,n}(k) - 1$ (avec $c = (m-1)(n-1)$).

On omettra parfois la mention de m et n si aucune confusion n'est à craindre.

20. Proposition

Le nombre d'éléments du complémentaire $\Delta(m, n)$ dans $\mathbf{N}+m$ est $D_{n,m}$, pour tout couple d'entiers m, n premiers entre eux, tels que $2 \leqslant n < m$.

Soit A un anneau générique, et soit B son normalisé.

On considère des $\mathbf{C}$-espaces vectoriels A, B, avec la filtration donnée par la valuation de B, c'est-à-dire $B_k = B\,t^k$ et $A_k = A \cap B_k$.

On a un morphisme $A \times A \to B$, de noyau R et d'image C, défini par $(p, q) \to q - p\,(dy/dx)$. On pose $C_k = C \cap B_k$.

On a alors une suite exacte $0 \to C_m \to B_m \to Q \to 0$, où la dimension de Qest égale au cardinal du complémentaire de $\Delta(m, n)$ dans $\mathbf{N}+m$ (car $v(C) = \Delta(m, n)$ si A est générique).

On a aussi une suite exacte $0 \to R \to A_n \times A_m \to C_m \to 0$, car un élément de $A \times A$ hors de $A_n \times A_m$ donne par le morphisme un élément de C hors de C_m, sa valuation ne pouvant être que $m-n$ ou un multiple de n inférieur à m.

On en déduit des suites exactes :

$$0 \to R_k \to (A_n/A_{n+k}) \times (A_m/A_{m+k}) \to C_m/C_{m+k} \to 0,$$

$$0 \to C_m/C_{m+k} \to B_m/B_{m+k} \to Q_k \to 0.$$

Il est clair que les dimensions de B_m/B_{m+k}, A_m/A_{m+k} et A_n/A_{n+k} sont respectivement k, card ($[m, m+k[\cap \Gamma$) et card ($[n, n+k[\cap \Gamma$).

On en déduit aisément

$$f_{m,n}(k) = \dim Q_k - \dim R_k .$$

Comme Q_k est isomorphe à un quotient de Q, on a $f_{m,n}(k) \leqslant \dim Q$.

Pour montrer que $D_{m,n} = \dim Q$, il suffit de prouver le lemme :

21. Lemme

Si $k = u_J - s_J - m$, *alors* $\dim Q_k = \dim Q$ *et* $\dim R_k = 0$.

On reprend les notations définies aux paragraphes 11 et 13.

On a vu que $\delta \leqslant u_J - s_J$. Donc $C_{m+k} = B_{m+k}$, ce qui assure un isomorphisme entre Q et Q_k. On a bien $\dim Q = \dim Q_k$.

On remarque aussi que, pour $0 \leqslant i < J$, on a $[u_J - s_J + s_i, u_J - s_J + s_{i+1}[\subset E_i$, et que $\mathbf{N} + u_J \subset E_J$. La formule de w (*cf.* § 14) montre que, pour $r \geqslant u_J - s_J$, on a $w(r) \geqslant u_J - s_J - m + n$.

On en déduit que tout élément ω de C_{m+k} est de la forme $q - p\,(dy/dx)$, avec $q \in A_{m+k}$ et $p \in A_{n+k}$. En effet, c'est vrai si $v(\omega) \geqslant c$, car on peut prendre $q = \omega$ et $p = 0$, et si $v(\omega) < c$, il existe $p \in A_{n+k}$ et $q \in A_{m+k}$ tels que $v(\omega - q + p\,(dy/dx)) > v(\omega)$, par définition de w. Un nombre fini « d'approximations successives » conduit au résultat voulu.

On peut maintenant prouver que $R_k = 0$; autrement dit, que $q - p\,(dy/dx) \in C_{m+k}$ implique $q \in A_{m+k}$ et $p \in A_{n+k}$. En effet, si $q - p\,(dy/dx) \in C_{m+k}$, il existe $p' \in A_{n+k}$ et $q' \in A_{m+k}$ avec

$$(q - q') - (p - p')\frac{dy}{dx} = 0,$$

donc

$$v(p - p') \geqslant \varepsilon = u_J - s_J - m + n = k + n \quad (\S\ 14)$$

et

$$v(q-q') = v(p-p')+m-n \geqslant k+m.$$

Les valuations de p et q vérifient bien les inégalités voulues.

Remarque. — Grâce à la symétrie de $D_{m,n}$, on pourra chercher à le calculer sans se préoccuper de savoir si $n < m$ ou si $n > m$.

22. Rappel sur les fractions continues

A une suite S de k nombres entiers positifs ou nuls, on associe un couple $\psi(S)$ d'entiers positifs ou nuls, avec les règles suivantes :

1° si $k = 0$, alors $\psi(S) = (1, 0)$. Si $k \geqslant 1$, S s'écrit (p, T), et si $\psi(T) = (u, v)$, alors :

$$\psi(S) = (pu+v, u).$$

Cette règle permet de définir ψ par récurrence sur k. Les autres règles en découlent;

2° si $\psi(S) = (c, d)$, si $\psi(S, p) = (a, b)$ et si $\psi(I) = (u, v)$, alors :

$$\psi(S, p, T) = (au+cv, bu+dv);$$

3° si $\psi(T) = (u, v)$, alors $\psi(0, T) = (v, u)$. On a les égalités

$$\psi(S, p, 0) = \psi(S),$$

$$\psi(S, p, 1) = \psi(S, p+1),$$

$$\psi(S, p, 0, q, T) = \psi(S, p+q, T);$$

4° si $\psi(S) = (c, d)$, si $\psi(S, p) = (a, b)$ et si $\psi(S, p, q) = (m, n)$, on a

$$bm-an = bc-ad = (-1)^k \quad \text{où k est la longueur de } S,$$

$$m = c+qa,$$

$$n = d+qb;$$

5° $\psi(S)$ est composé de deux nombres premiers entre eux, et, pour tout couple de nombres premiers entre eux, il existe une suite S dont l'image par ψ est ce couple;

6° en utilisant les règles 3° et 5°, on peut mettre un couple d'entiers premiers entre eux sous la forme $\psi(S)$, où les éléments r_i de S vérifient

$r_i \geqslant 1$ si $1 < i < k$. Si le couple n'a pas 1 parmi ses éléments, on peut supposer $r_k \geqslant 2$. Quitte à remplacer le couple par son symétrique, on peut supposer que k est pair (k étant la longueur de S).

Les preuves sont dans [1] (chap. X).

23. Définitions

Désormais, m et n sont deux entiers positifs, premiers entre eux, et (S, p, q) une suite de longueur paire, telle que $\psi(S, p, q) = (m, n)$, avec $p \geqslant 1$. On pose $(a, b) = \psi(S, p)$ et $(c, d) = \psi(S)$. On a alors

$$m = qa + c, \qquad n = qb + d,$$

$$bc - ad = bm - an = 1 \qquad \text{et} \qquad cn - dm = q.$$

On a

$$b \geqslant pd \geqslant d \qquad \text{et} \qquad b \geqslant 1 \quad \text{et} \quad a \geqslant pc \geqslant c \geqslant 1.$$

(Le nombre c n'a rien à voir avec le conducteur $(m-1)(n-1)$.)

On définit une suite de triplets appartenant à $\mathbf{Z} \times [0, a[\times [0, b[$ par récurrence. Le premier triplet est $\theta_0 = (\lambda_0, u_0, v_0) = (0, 0, 0)$, et $u_{z+1} = u_z + c \bmod a$, $v_{z+1} = v_z - d \bmod b$, et λ_{z+1} est déterminé à partir de λ_z par la condition $h_z \leqslant h_{z+1} < h_z + na$, en posant $h_z = (\lambda_z a + u_z) n + v_z m$. On appelle h_z la valeur de θ_z. On peut vérifier que $h_{z+1} - h_z$ vaut q si $v \geqslant d$, vaut $q-1$ si $v < d$. Comme b et d sont premiers entre eux, la suite v_z est périodique de période b, d'image $[0, b[$, donc $h_{z+b} = h_z + n$. Il y a dans la suite des triplets de valeur arbitrairement grande.

24. Lemme

Si $h = h_z$ et $h' = h_{z+1}$, on a

$$[h, h'[\cap \Gamma = [h, h'[\cap [h, h + \lambda_z).$$

L'image de la suite θ est formée des (λ, u, v) tels que $(\lambda a + u) n + vm > 0$, et de θ_0.

Si la suite θ comporte le triplet (λ, u, v) de valeur h, elle comporte également les triplets suivants :

$(\lambda, u+1, v)$, de valeur $h+n$, pourvu que $u < a-1$;

$(\lambda+1, 0, v)$, de valeur $h+n$, pourvu que $u = a-1$;

$(\lambda, u, v+1)$, *de valeur* $h+m$, *pourvu que* $v < b-1$;

$(\lambda+1, u, 0)$, *de valeur* $h+m-1$, *lorsque* $v = b-1$.

Si $h \leqslant h+\alpha < h'$, on a $h+\alpha = a(\lambda-\alpha)n+un+vm+\alpha bm$. Si donc $0 \leqslant \alpha \leqslant \lambda$, $h+\alpha \in \Gamma$, et si $\lambda < \alpha < h'-h$, le coefficient de n est négatif, et celui de m inférieur à n, donc $h+\alpha \notin \Gamma$.

Si $0 < \alpha < h'-h$, le coefficient $(v+\alpha b)$ de m n'appartient pas à $\mathbf{N}+n+[0, b[$, et $h+\alpha$ n'est donc pas une valeur d'un triplet de θ. Si deux triplets θ_z et θ'' ont même valeur > 0, ils sont égaux si $q \neq 0$, et si $q = 0$, on a $n = d$ et $m = c$, et $v-v''$ est multiple de $n = d$ (car m et n sont premiers entre eux). Si par exemple $v'' = v+\mu d$, on a $\theta_{z-\mu} = \theta''$. La seconde assertion est ainsi prouvée.

Le calcul de la valeur des triplets, indiqués dans la troisième assertion, est trivial, et on vient de voir que cette valeur assure qu'ils sont dans l'image de la suite θ.

25. Corollaire

La fonction $f_{m,n}$ *atteint son maximum* $D_{m,n}$ *sur l'image de la suite des valeurs.*

Si $k \leqslant k'$, on a

$$f(k')-f(k) = k'-k-\operatorname{card}([k+m, k'+m[\cap \Gamma)-\operatorname{card}([k+n, k'+n[\cap \Gamma).$$

Soit $h \leqslant k < h'$ un encadrement d'un nombre k par les valeurs de deux triplets consécutifs.

Si $k+n \in \Gamma$, alors $[k+n, k+n[\subset \Gamma$, donc

$$f(k)-f(h) = -\operatorname{card}([h+m, k+m[\cap \Gamma).$$

Si $k+n \notin \Gamma$, alors $[k+n, h'+n[\cap \Gamma = \emptyset$, donc $f(h')-f(k)$ est égal à

$$h'-k-\operatorname{card}([k+m, h'+m[\cap \Gamma) \geqslant 0.$$

Ainsi, si $D_{m,n} = f_{m,n}(k)$, l'une des valeurs de triplets qui encadrent k réalise aussi le maximum de $f_{m,n}$.

26. Lemme

Si $h_z < (m-1)(n-1)$, *on a* $f(h_{z+1})-f(h_z) = g_z$, *où* g_z *est la fonction de* λ_z, u_z, v_z *donnée par le tableau suivant* :

		g
$d=0,\ v=0$.....	$u<a-1$	$q-2\lambda-3$
	$u=a-1$	$q-2\lambda-4$
$d>0,\ v<d-1$..	$u<a-1$	$q-2\lambda-1$
	$u=a-1$	$q-2\lambda-2$
$v\geqslant d-1$.....	$u<a-1$	$q-2\lambda-2$
	$u=a-1$	$q-2\lambda-3$

Si $h_z \geqslant (m-1)(n-1)$, $f(h_{z+1})-f(h_z)$ et g_z sont tous deux des nombres $\leqslant 0$.

En effet, $h_{z+1}-h_z$ vaut $q+1$ ou q suivant que $v_z < d$ ou $v_z \geqslant d$. L'intersection $[h_z+n,\ h_{z+1}+n[\cap \Gamma$ compte λ_{z+1} éléments si $u_z < a-1$, ou λ_z+2 si $u_z = a-1$, à moins que $h_{z+1}+n \geqslant mn$, auquel cas les expressions indiquées majorent card $([h_z+n,\ h_{z+1}+n[\cap\Gamma)$. De même,

$$\operatorname{card}([h_z+m,\ h_{z+1}+m[\cap\Gamma)$$

vaut au plus λ_z+1 si $v_{z+1} < b-1$, ou λ_z+2 si $v_z = b-1$, l'égalité étant assurée si $h_{z+1}+m < mn$.

On a donc bien $f(h_{z+1})-f(h_z) = g_z$ si $h_z \leqslant (m-1)(n-1)$, et pour $h_z \geqslant (m-1)(n-1)$, on a

$$g_z \leqslant f(h_{z+1})-f(h_z) = h_z - h_{z+1} \leqslant 0.$$

27. Corollaire

$D_{m,n}$, qui est le maximum de la suite $f(h_z)$, est aussi le maximum de la suite $\sum_{0\leqslant i<z} g_i = f_z^*$.

28. Lemme

On a $f_{ab}^* = (q-1)ab-2a-2b+bc = bm-2a-2b-ab$.

On sépare les cas $d=0$ et $d\neq 0$ pour la démonstration. Pour $d=0$, on a $b=c=1$, donc $v_i=0$, $u_i=i$ et $\lambda_i=0$ pour $0\leqslant i<a$. Donc $f_0^* = (a-1)(q-3)+q-4$, ce qui convient.

Pour $d>0$, comme a et c, b et d, a et b sont premiers entre eux, $(c,\ -d)$ est un générateur du groupe $(\mathbf{Z}/a\,\mathbf{Z})\times(\mathbf{Z}/b\,\mathbf{Z})$, donc la suite $(u_i,\ v_i)$, $0\leqslant i<ab$ a pour image $[0,\ a[\times[0,\ b[$. Comptons les λ_i égaux à -1 : ils correspondent aux $(u_i,\ v_i)$ tels que $u_i n+v_i m > an$, ce qui impose $u_i \geqslant 1$ et $v_i \geqslant 1$. Si $un+vm > an$, avec $0<u<a$ et $0<v<b$, on a

$$(a-u)n+(b-v)m = 2an+1-un-vm \leqslant an,$$

et vice versa. Ceci montre qu'il y a $(a-1)(b-1)/2$ fois $\lambda_i = -1$ pour $0 \leqslant i < ab$. Les autres λ_i sont évidemment nuls.

Le tableau des valeurs de g donne donc

$$f^*_{ab} = qab-(a-1)(d-1)-2(d-1)$$
$$-2(a-1)(b-d+1)-3(b-d+1)+(a-1)(b-1).$$

Toute simplification faite, on voit que $f^*_{ab} = (q-1)\,ab-2\,a-2\,b+ad+1$. Ce qui convient aussi.

29. Théorème

Si m et n sont deux entiers $\geqslant 2$ premiers entre eux, si S est une suite de longueur paire, si $(m, n) = \psi(S, p, q)$, avec $p \geqslant 1$ et $q \geqslant 2$ (et on sait qu'une telle suite existe, quitte à intervertir m et n), si $(a, b) = \psi(S, p)$, et si $(c, d) = \psi(S)$, on a

si $q = 2$ et $d = 0$, $D_{m,n} = 0$;

si $q = 3$ et $d = 0$, $D_{m,n} = 0$;

si $q = 2$, $c = 1$, $d > 0$, $D_{m,n} = f^*_{ab}+2$;

si $q = 2$, $d = 1$, $c > 1$, $D_{m,n} = f^*_{ab}+1$;

sinon $D_{m,n} = f^*_{ab}+D_{m-2a,\,n-2b}$.

On constate que $(m-2\,a, n-2\,b) = (\bar{m}, \bar{n}) = \psi(S, p, q-2)$. On remarque que si $q > 2$ ou $d > 0$, on peut encore définir $\bar{f}^*$ et $\bar{g}$ comme précédemment en vue de calculer $D_{\bar{m},\bar{n}}$. On notera que $\bar{g}_z = g_{z+ab}$, et que par conséquent $\bar{f}^*_z + f^*_{ab} = f^*_{z+ab}$.

Le cas $q = 2$, $d = 0$, qui donne $n = 2$ et $m = 2\,a+1$ se traite aisément : comme $g_z \leqslant 0$ pour tout z, $f^*_0 = 0$ est le maximum de f^*.

Le cas $d = 0$ et $q = 3$ se traite de la même façon.

Dans les autres cas, deux éventualités apparaissent; la première est : $g_z \geqslant 0$ pour tout $z \in [0, ab[$, la seconde est : il existe z dans $[0, ab[$ avec $g_z < 0$.

La première éventualité a lieu si $d = 0$ et $q \geqslant 4$, et aussi si $d > 0$ et $q \geqslant 3$. Elle implique que le maximum de f^*_i se réalise avec $i \geqslant ab$, donc $D_{m,n} = f^*_i = \bar{f}^*_{i-ab} + f^*_{ab}$, et $\bar{f}^*_{i-ab}$ réalise le maximum de $\bar{f}^*$, qui est $D_{\bar{m},\bar{n}}$.

On voit que $g_z \geqslant 0$, sauf si $u_z = a-1$, $v_z \geqslant d-1$, et $\lambda_z = 0$. De tels triplets ne peuvent être obtenus que si $(a-1)\,n+(d-1)\,m < an$, c'est-à-dire $(d-1)\,m-n = (c-1)\,n-m-q < 0$, ou encore $(d-2)\,m+(c-2)\,n-2 < 0$

(cette expression est la somme des deux précédentes). Si $c \geqslant 2$ et $d \geqslant 2$, l'un des deux nombres c et d est $\geqslant 3$, car c et d sont premiers entre eux. L'expression est donc au moins $m-2$ ou au moins $n-2$, donc positive. Si donc $c \geqslant 2$ et $d \geqslant 2$, la première éventualité a lieu.

Si $c \geqslant 2$ et $d = 1$, on a $(d-1)\,m-n < 0$, mais $dm-n = (c-2)\,n+n-2 \geqslant 0$, il n'y a qu'une valeur de $z \in [0, ab[$ qui donne $g_z = -1$, les autres donnent $g_z \geqslant 0$.

Si $c = 1$ et $d \geqslant 1$, on a $(d-1)\,m-n = -m-2 < 0$, $dm-n = -2 < 0$, mais $(d+1)\,m-n \geqslant 0$. Il n'y a que deux valeurs de $z \in [0, ab[$ qui donnent $g_z = -1$, les autres donnent $g_z \geqslant 0$. (On a bien $d < b$, car $b = ad+1$ et $a \geqslant c \geqslant 1$.)

Montrons que dans les deux cas, on a $g_z \leqslant 0$ si $h_z \geqslant an$. L'inégalité $h_z \geqslant an$ implique $\lambda_z \geqslant 0$. Si $\lambda_z \geqslant 1$, la question est réglée; de même si $\lambda_z = 0$ et si $u_z = a-1$ ou $v_z < d-1$. Si $u_z < a-1$, $v_z < d-1$ et $\lambda_z = 0$, on a

$$u_z n+v_z m+\lambda_z an < (d-1)\,m+(a-1)\,n < an.$$

Montrons que dans les deux cas, si $g_z = -1$ et si $z \leqslant i < ab$, alors $g_i \leqslant 0$. Si $(d-1)\,m+(a-1)\,n \leqslant an+un+vm < an$, on a sûrement $\lambda = 0$, car $\lambda = 1$ ne donne que des valeurs $\geqslant an$ et $\lambda = -1$ ne donne que des valeurs plus petites que $(b-1)\,m-n = (a-1)\,n+1-m < (a-1)\,(d-1)\,m$ (car $m \geqslant 2$ et $d \geqslant 1$). Si $u = a-1$ et $v \geqslant d-1$, on a $g = -1$, et si $u < a-1$, on a $v > d-1$, et $g = 0$.

Ces valeurs de g donnent les variations de f^*, ce qui donne la valeur du maximum de f^* comme on le voulait.

30. Corollaire

Avec les mêmes notations que ci-dessus, on a les formules, où x/y est la partie entière du quotient :

si $d = 0$, $D_{n,m} = (p-1)\,((q-2)^2/4)+((q-3)^2/4)$ (on retrouve le résultat de [4]);

si $d > 0$, $D_{n,m} = ab\,(q^2/4)+(bc-2a-2b)\,(q/2)+F$, où F est donné par le tableau :

			F
q impair			$D_{a+c,b+d}$
q pair.....	$c \geqslant 2$	$d \geqslant 2$	$D_{c,d}$
		$d = 1$	1
	$c = 1$	$d \geqslant 1$	2

On obtient ceci à partir du théorème précédent, en utilisant l'expression de f_{ab}^{*} (lemme 28) et les formules sommatoires des progressions arithmétiques.

31. Notations

Soit $R = (e_1, e_2, \ldots, e_k)$, avec $k \geqslant 2$, $e_1 > 0$ et $e_2 > 0$, telle que $(M, N) = \psi(R)$, vérifie $\mathbf{N} \geqslant 2$ (on a $M > N$). On définit des nombres σ_i et τ_i, $0 \leqslant i \leqslant k$ de la manière suivante :

$$\sigma_k = 0 \qquad \text{et} \qquad \tau_k = 1,$$

si $0 < i \leqslant k$, $\sigma_{i-1} = \sigma_i + \tau_i e_i$, et $\tau_{i-1} = 0$ si $\tau_i = 1$ et σ_{i-1} pair, et $\tau_{i-1} = 1$ si $\tau_i = 0$ ou si σ_{i-1} impair.

32. Théorème

Avec les notations ci-dessus, on a

(i) $4\,D_{M,N} = (M-4)(N-4) + \sigma_0 + (4-2\tau_1)(e_1-2) - 2\tau_1\tau_2$;

(ii) $(M-4)(N-4)/4 \leqslant D_{M,N} \leqslant (M-2)/2 \times (N-2)/2$;

(iii) $D_{M+N,N} - D_{M,N} = (N-2)^2/4$;

(iv) $D_{M+N,M} - D_{M,N}$ *est donné par le tableau.*

	$4\,(D_{M+N,M} - D_{M,N})$
$\tau_1 = 0$	$M^2 - 4M + 7 - 4e_1$
$\tau_1 = 1$	$M^2 - 4M - 2e_1 + \tau_0 + 2\tau_2$

(v) $(M-3)^2/4 \leqslant D_{M+N,N} - D_{M,N} \leqslant (M-2)^2/4$.

Commentaire. — Les formules (iii) et (iv) décrivent le comportement de D sous l'effet d'un éclatement de l'idéal maximal de A; le cas (iii) concernant le cas où la multiplicité ne change pas.

(i) La preuve se fait « par récurrence sur R ».

On constate qu'une modification de R, dans les limites permises pour R, effectuée selon les règles 3° du rappel (§ 22), ne change aucun des deux membres de l'égalité à démontrer, mais permet de se ramener au cas où le dernier élément de R est $\geqslant 2$, en diminuant la longueur de R.

On observe aussi qu'alors le théorème 29 permet, soit de vérifier l'égalité voulue (dans les cas

$$R = (e_1, 2), \qquad R = (e_1, 3), \qquad R = (e_1, e_2, 2)$$

et

$$R = (e_1, 1, e_3, 2)),$$

soit de se ramener au cas $\overline{R} = (e_1, \ldots, e_{k-1}, e_k - 2)$, compte tenu de l'égalité (lemme 28)

$$4 f_{ab}^{*} = (m-4)(n-4) - (m-2a-4)(n-2b-4) + 2;$$

alors la longueur de R ne change pas, mais la somme de ses termes diminue si on remplace R par $\overline{R}$.

Comme la longueur de R et la somme de ses termes ne peuvent diminuer indéfiniment, on arrive à se ramener au bout d'un nombre fini de diminutions à l'un des cas de vérification directe.

(iv) se déduit de (i),

(ii), (iii), (v) peuvent se déduire de (i) et (iv), mais on peut également les montrer par récurrence sur R.

Les vérifications à effectuer sont toutes obtenues au terme de calculs simples et fastidieux.

BIBLIOGRAPHIE

[1] HARDY (G.) and WRIGHT (E.). — *Introduction to the theory of numbers* 3 rd edition. — Oxford, Clarendon Press, 1954.

[2] ZARISKI (O.). — Characterization of plane algebroid curves whose module of differentials has maximum torsion. *Proc. Nat. Ac. Sc. U.S.A.*, t. 56, 1966, p. 781-786.

[3] ZARISKI (O.). — Studies in equisingularity, III., *Amer. J. Math.*, t. 90, 1968, p. 961-1023.

[4] ZARISKI (O.). — Cours à l'École Polytechnique, 1973.

(Texte reçu le 16 novembre 1977).

Charles DELORME
Mathématiques Bâtiment 425,
Université de Paris-Sud,
91405 Orsay.