Approche effective des résidus algébriques

Mohamed Elkadi, Bernard Mourrain

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Approche Effective des Résidus Algébriques

Mohamed Elkadi & Bernard Mourrain

N° 2884

Mai 1996

THÈME 2

ISSN 0249-6399

Approche Effective des Résidus Algébriques

Mohamed Elkadi* & Bernard Mourrain**

Thème 2 — Génie logiciel
et calcul symbolique
Projet SAFIR

Rapport de recherche n° 2884 — Mai 1996 — 67 pages

Résumé : Dans ce rapport, nous nous intéressons aux propriétés du dual des polynômes et leurs connections avec la théorie algébrique des résidus. En particulier, nous voulons éclaircir le rôle que jouent les Bézoutiens dans la théorie des résidus et dans la résolution de systèmes polynomiaux. Nous rappelons donc les propriétés du dual des polynômes et des systèmes inverses. Nous montrons dans le cas local (point isolé) comment ces systèmes inverses peuvent être calculés par intégration. Puis nous détaillons les travaux de G. Scheja et U. Storch [29], et E. Kunz [19], où les fondements de la théorie algébrique des résidus sont établis. Nous étudions ensuite le comportement du résidu sous l'action de certaines transformations polynomiales, et le lien avec les bases de Gröbner. Nous donnons enfin des preuves élémentaires de résultats classiques tels que le théorème de Macaulay, la formule d'Euler-Jacobi, le théorème de Bézout, la formule de Weil, et des algorithmes pour le calcul du résidu, dans certains cas, en utilisant les bases de Gröbner ou en résolvant des systèmes linéaires de tailles raisonnables.

Mots-clé : dualité, résidus, systèmes inverses, algèbre de Gorenstein, intersection complète, Bézoutiens, systèmes polynomiaux

(Abstract: pto)

∗. UNSA, Lab. J-A. Dieudonné, Parc Valrose, B.P. 71, 06108 Nice, elkadi@hera.unice.fr
∗∗. INRIA, SAFIR, 2004 route des Lucioles, B.P. 93, 06902 Sophia Antipolis, mourrain@sophia.inria.fr

Unité de recherche INRIA Sophia-Antipolis
2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS Cedex (France)
Téléphone : (33) 93 65 77 77 – Télécopie : (33) 93 65 77 65

Effective Approach of Algebraic Residues

Abstract: In this report, we are interested by the dual of the polynomials and its connections with the theory of algebraic residues. We specially focus of the Bezoutians and their role in the theory of residues and in polynomial systems solving. We recall the main properties of the dual and of inverse systems of ideals. We show in the local 0-dimensional case, how inverse systems can be computed by *integration*. The next part is devoted to the work of G. Scheja and U. Storch [29], E. Kunz [19], where the foundations of the algebraic theory of residues are settled. Then, we study the properties of residues under polynomial transformations, and some connections with Gröbner Bases. Finally, we give some elementary proofs of classical results such as Macaulay's theorem, Bezout's theorem, Weil's formula, Euler-Jacobi's formula, and we proposed (in some cases) algorithms for the computations of residues.

Key-words: duality, residues, inverse systems, Gorentsein algebra, complete intersection, Bezoutians, polynomial systems

Table des matières

Ces notes ont été rédigées à la suite d'exposés au séminaire « Formes & Formules» 1994-1995. Ce séminaire commun au laboratoire J-A. Dieudonné de Mathématiques de l'Université de Nice et au projet SAFIR, INRIA, Sophia-Antipolis, avait pour thème, cette année-là, « *Polynômes et Résidus*».

Dans une première partie, nous y avons présenté les travaux de Scheja, Storch et Kunz sur les résidus algébriques; puis nous avons abordé les aspects analytiques et leurs applications en géométrie algébrique effective. Ces approches avaient été illustrées par quelques applications à la résolution de systèmes polynomiaux, à l'étude locale de points isolés, à l'étude locale de courbes et à leur traces réelles[1]. Nous remercions tous les intervenants au séminaire « Formes & Formules », ainsi que tous les participants.

1 Introduction

L'ingrédient principal de la construction algébrique des résidus est le Bézoutien (que l'on appellera aussi « jacobien discret »). Nous allons rappeler rapidement sa définition, ainsi que certains domaines où il apparaît. Considérons deux paquets de variables $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n)$ et les points $X_{(0)} = (x_1, \ldots, x_n)$, $X_{(1)} = (y_1, x_2 \ldots, x_n), \ldots, X_{(n)} = (y_1, \ldots, y_n)$. Pour tout polynôme $P \in \mathbb{K}[\mathbf{x}]$ ($\mathbb{K}$ est un corps commutatif unitaire), on note $\theta_i(P) = \frac{P(X_{(i)}) - P(X_{(i-1)})}{y_i - x_i}, 1 \leq i \leq n$, les différences *finies* de P. Ce sont des polynômes en $x_1, \ldots, x_n, y_1, \ldots, y_n$, de degrés au plus $\deg(P) - 1$. Construisons le polynôme de $\mathbb{K}[\mathbf{x}, \mathbf{y}]$,

$$\Phi(P_0, P_1, \ldots, P_n) = \begin{vmatrix} P_0(X_{(0)}) & \theta_1(P_0) & \cdots & \theta_n(P_0) \\ \vdots & \vdots & & \vdots \\ P_n(X_{(0)}) & \theta_1(P_n) & \cdots & \theta_n(P_n) \end{vmatrix},$$

où $P_0, \ldots, P_n \in \mathbb{K}[\mathbf{x}]$. Nous allons voir que cet objet apparaît quand on s'intéresse à l'étude des systèmes polynomiaux.

E. Bézout a utilisé cet outil pour construire le résultant de deux polynômes P et Q en une variable, en calculant le déterminant d'une matrice de taille $\max(\deg P, \deg Q)$ (voir [5]). Nous pouvons comparer la méthode de Bézout à celle proposée ultérieurement par Sylvester qui consiste à calculer le déterminant d'une matrice de taille $\deg P + \deg Q$ en considérant des multiples des polynômes initiaux P et Q. Cette comparaison peut se faire aussi dans le cas d'un système de $n+1$ polynômes en n variables. Les formulations du résultant par Macaulay (voir [21] ou [30]), ou encore

1. pour plus de détails, voir `http://www.inria.fr/safir/MEETING/seminaires.html`

les résultants de « Newton» (voir [6]), peuvent être vues comme une généralisation de la méthode de Sylvester alors que les formulations obtenues à partir « des jacobiens discrets » généralisent la méthode de Bézout.

Les Bézoutiens apparaissent aussi dans les travaux de A. Dixon [9], qui a construit le résultant de trois polynômes, en deux variables, du même degré, en suivant la méthode introduite par Bézout pour deux polynômes en une variable.

Les polynômes Φ sont aussi à la base de méthodes numériques de localisation des zéros d'un système polynomial, comme la méthode des sécantes en une et plusieurs variables, que l'on présentera dans la section 4.2 (voir [17], [31], [25]).

La fonction Φ apparaît également dans les travaux de J.P. Jouanolou [18], où elle est appelée *forme de Morley*. Elle sert à construire le résultant de n polynômes homogènes en n variables.

Les « jacobiens discrets » apparaissent inévitablement en théorie analytique des résidus, par exemple dans la formule de Weil ou dans les lois de transformations (voir [15], [4] ou [3]). Ils sont utilisés en particulier pour trouver des formules de représentation dans des idéaux de polynômes et obtenir des versions effectives économiques du Nullstellensatz ([3], [4], [11], [12]).

Depuis quelques temps, les aspects effectifs des Bézoutiens ont suscité un regain d'intérêt comme le montre les travaux [7], [28, 14], [27] ou encore [2] pour ce qui concerne la géométrie algébrique réelle. Signalons également qu'une approche algorithmique du calcul des résidus est proposée dans [8], dans le cas très spécial où l'application polynomiale $(P_1, \ldots, P_n)$ est une déformation plate de $(x_1^{d_1}, \ldots, x_n^{d_n})$.

Le but de ce rapport est de donner les principales propriétés des Bézoutiens et surtout d'éclaircir le rôle qu'ils peuvent jouer dans la théorie algébrique des résidus et dans la résolution de systèmes polynomiaux. Dans une première partie, nous rappellerons les propriétés du dual de l'algèbre des polynômes et du système inverse d'un idéal. Nous montrerons dans le cas local (point isolé) comment ces systèmes inverses peuvent être calculés par *intégration*. Nous utiliserons ces résultats pour calculer le résidu local d'une application polynomiale. Dans un deuxième temps, nous détaillerons les travaux de G. Scheja et U. Storch [29], et E. Kunz [19], où les fondements de la théorie algébrique des résidus sont établis. En suite, nous étudierons le comportement du résidu sous l'action de certaines transformations polynomiales, et le lien avec les bases de Gröbner. Nous donnerons des preuves élémentaires de résultats classiques tels que le théorème de Macaulay, la formule d'Euler-Jacobi, le théorème de Bézout, la formule de Weil, et des algorithmes pour le calcul du résidu, dans certains cas, en utilisant les bases de Gröbner ou en résolvant des systèmes linéaires de tailles raisonnables.

Notations générales :

- $\mathbb{K}$ est un corps de caractéristique quelconque, sauf mention du contraire.
- $R = \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\mathbf{x}]$ est l'anneau des polynômes en les variables $x_1, \ldots, x_n$ et à coefficients dans $\mathbb{K}$.
- Si $A \subset B$ sont deux anneaux et I un idéal de A, on notera $I\,B$ l'idéal de B engendré par les éléments de I.
- L'**annulateur** d'un idéal I dans un anneau A, noté $Ann_A(I)$, est par définition $\{x \in A : x\,g = 0\,, \forall g \in I\}$. C'est un idéal de A.
- Si M et N sont deux A-modules, l'ensemble des A-**homomorphismes** de M dans N est noté $Hom_A(M, N)$.
- Pour tout $\mathbb{K}$-espace vectoriel B, l'ensemble $Hom_{\mathbb{K}}(B, \mathbb{K})$ des formes linéaires sur B sera noté $\hat{B}$.
- Si A est une $\mathbb{K}$-algèbre, on peut munir l'espace $\hat{A}$ d'une structure naturelle de A-module de la façon suivante: $\forall \lambda \in \hat{A}, \forall a \in A, a \cdot \lambda$ est l'élément de $\hat{A}$ défini par

$$\begin{array}{rccl} a \cdot \lambda & : A & \to & \mathbb{K} \\ & b & \mapsto & (a \cdot \lambda)(b) = \lambda(a\,b). \end{array}$$

- Pour toute $\mathbb{K}$-algèbre A, on note μ la multiplication interne

$$\begin{array}{rccl} \mu & : A \otimes A & \to & A \\ & a \otimes b & \mapsto & a\,b. \end{array}$$

  Son noyau est noté $\mathcal{D}$; c'est un idéal bilatère de $A \otimes A$ engendré par les éléments de la forme $a \otimes 1 - 1 \otimes a, a \in A$.
- Pour tout élément a de A, on note μ_a la multiplication par a

$$\begin{array}{rccl} \mu_a & : A & \to & A \\ & b & \mapsto & a\,b. \end{array}$$

- Une suite $f_1, \ldots, f_n$ d'éléments d'un anneau A est dite **régulière** si pour tout $i \in \{0, \ldots, n-1\}$, f_{i+1} n'est pas un diviseur de zéro dans $A/(f_1, \ldots, f_i)$ (i.e. $Ann_{A/(f_1,\ldots,f_i)}(f_{i+1}) = \{0\}$).

– La suite $f_1, \ldots, f_n$ est dite **quasi-régulière** si elle est régulière dans toute localisation de A par un idéal maximal m contenant $(f_1, \ldots, f_n)$. Rappelons que la notion de quasi-régularité est indépendante de l'ordre des éléments $f_1, \ldots, f_n$, tandis que la notion de régularité en dépend (voir [24]).

2 Dualité et Systèmes Inverses

Dans cette section, nous allons nous intéresser aux formes linéaires sur l'anneau des polynômes. Les objets que nous étudierons seront donc des éléments du dual de $\mathbb{K}[\mathbf{x}]$. Un thème de recherche connaissant depuis quelques temps des développements intéressants consiste à représenter les polynômes comme des « algorithmes» calculant une valeur en un point. On s'intéresse donc à l'évaluation des polynômes en un point. Cette évaluation est une forme linéaire particulière. Nous voulons étendre ce point de vue en nous intéressant systématiquement aux propriétés des formes linéaires sur les polynômes.

2.1 Le dual de $R = \mathbb{K}[\mathbf{x}]$

La forme linéaire non nulle la plus simple est l'*évaluation en un point* $\zeta \in \mathbb{K}^n$,

$$\begin{aligned} \partial_\zeta^{\mathbf{0}} : R &\to \mathbb{K} \\ p &\mapsto \partial_\zeta^{\mathbf{0}}(p) = p(\zeta). \end{aligned}$$

Pour tout multi-indice $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$, on peut considérer la forme linéaire

$$\begin{aligned} \partial_\zeta^{\mathbf{a}} : R &\to \mathbb{K} \\ p &\mapsto \partial_\zeta^{\mathbf{a}}(p) = d_{x_1}^{a_1} \cdots d_{x_n}^{a_n}(p)(\zeta), \end{aligned}$$

où d_{x_i} désigne la dérivation par rapport à la variable x_i. Nous notons, $\partial_{i,\zeta} = \partial_\zeta^{\mathbf{a}}$, avec $a_i = 1$ et $a_j = 0, j \neq i$. Avec ces notations, $\partial_\zeta^{\mathbf{a}} = \partial_{1,\zeta}^{a_1} \ldots \partial_{n,\zeta}^{a_n}$.

Via ce formalisme, *l'algèbre* $\mathbb{K}[[\partial_{1,\zeta}, \ldots, \partial_{n,\zeta}]]$ *des séries formelles* (*ou opérateurs différentiels « en* ζ *» à coefficients dans* $\mathbb{K}$) *s'identifie à* $\hat{R}$. Cette identification est réalisée par le développement de Taylor en ζ. En effet, étant donné $f \in \mathbb{K}[x_1, \ldots, x_n]$,

$$f(x) = \sum_{\mathbf{a} \in \mathbb{N}^n} f_{\mathbf{a}}(\zeta)(x - \zeta)^{\mathbf{a}}, f_{\mathbf{a}} \in \mathbb{K}[x_1, \ldots, x_n],$$

où $(x - \zeta)^{\mathbf{a}} = \prod_{i=1}^n (x_i - \zeta_i)^{a_i}$. Par conséquent, pour toute forme linéaire Λ sur R,

$$\Lambda(f) = \sum_{\mathbf{a} \in \mathbb{N}^n} \Lambda((x - \zeta)^{\mathbf{a}}) f_{\mathbf{a}}(\zeta) = \sum_{\mathbf{a} \in \mathbb{N}^n} \Lambda((x - \zeta)^{\mathbf{a}}) \mathbf{d}_\zeta^{\mathbf{a}}(f).$$

Si la caractéristique de $\mathbb{K}$ est nulle, $\mathbf{d}_\zeta^{\mathbf{a}} = \frac{1}{\prod_{i=1}^n a_i!}\partial_\zeta^{\mathbf{a}}$. Lorsque $\zeta = 0, \mathbf{d}_\zeta^{\mathbf{a}}$ sera noté $\mathbf{d}^{\mathbf{a}}$.

On vérifie facilement que

$$\mathbf{d}_\zeta^{\mathbf{a}}((x-\zeta)^{\mathbf{b}}) = \begin{cases} 1 \text{ si } \mathbf{a} = \mathbf{b}, \\ 0 \text{ sinon.} \end{cases}$$

La base $(\mathbf{d}_\zeta^{\mathbf{a}})_{\mathbf{a}\in\mathbb{N}^n}$ de $\hat{R}$ est donc la base duale de la base monomiale $((x-\zeta)^{\mathbf{a}})_{\mathbf{a}\in\mathbb{N}^n}$ de R. Cette notation n'est pas multiplicative : $\mathbf{d}_\zeta^{\mathbf{a}}\,\mathbf{d}_\zeta^{\mathbf{a}'} \neq \mathbf{d}_\zeta^{\mathbf{a}+\mathbf{a}'}$. Voir [13] pour plus de détail.

Remarquons que l'on peut aussi choisir comme base de $\hat{R}$, $(\partial_\zeta^{\mathbf{0}})_{\zeta\in\mathcal{P}}$ où $\mathcal{P}$ est un ensemble infini de points convenablement choisis.

A partir de maintenant, nous allons identifier $\hat{R}$ avec $\mathbb{K}[[\partial_{1,\zeta},\ldots,\partial_{n,\zeta}]]$. Les formes linéaires seront donc vue *comme des opérateurs différentiels au point* ζ. On notera aussi leur espace $\mathbb{K}[[\partial_\zeta]]$. Lorsque $\zeta = 0, \mathbb{K}[[\partial_0]]$ sera noté $\mathbb{K}[[\partial_1,\ldots,\partial_n]]$ ou $\mathbb{K}[[\partial]]$.

L'espace vectoriel $\hat{R}$ est muni d'une structure de R-module de la façon suivante : $\forall p \in R$, $\forall \Lambda \in \hat{R}$, on définit $p\cdot\Lambda$ par

$$\begin{aligned} p\cdot\Lambda : R &\to \mathbb{K} \\ q &\mapsto \Lambda(p\,q). \end{aligned}$$

Cette opération correspond dans $\mathbb{K}[[\partial_\zeta]]$ à des dérivations. En effet, on montre par récurrence sur $a \in \mathbb{N}^*$,

$$d_{x_i}^a((x_i-\zeta_i)\,p) = a\,d_{x_i}^{a-1}(p) + (x_i-\zeta_i)\,d_{x_i}^a(p).$$

Ce qui montre que

$$\begin{aligned} (x_i-\zeta_i)\cdot\partial_\zeta^{\mathbf{a}}(p) &= \partial_\zeta^{\mathbf{a}}((x_i-\zeta_i)\,p) \\ &= a_i\partial_{1,\zeta}^{a_1}\cdots\partial_{i-1,\zeta}^{a_{i-1}}\partial_{i,\zeta}^{a_i-1}\partial_{i+1,\zeta}^{a_{i+1}}\cdots\partial_{n,\zeta}^{a_n}(p) \\ &= d_{\partial_{i,\zeta}}(\partial_\zeta^{\mathbf{a}})(p). \end{aligned}$$

Donc la multiplication par $x_i-\zeta_i$ dans $\hat{R}$ agit sur les éléments de $\mathbb{K}[[\partial_\zeta]]$ comme une dérivation par rapport à la variable $\partial_{i,\zeta}$.

Décrivons ici, comment on peut passer des opérateurs différentiels en ζ aux opérateurs différentiels en un autre point. Pour cela, nous notons

$$e^{(\zeta,\partial)} = \sum_{\mathbf{a}\in\mathbb{N}^n} \zeta^{\mathbf{a}}\mathbf{d}^{\mathbf{a}}.$$

Nous allons définir l'isomorphisme entre $\mathbb{K}[[\partial_\zeta]]$ et $\mathbb{K}[[\partial]]$. Tout autre changement de points induit le même type d'isomorphisme (à translation près).

Théorème 2.1.1 — *L'isomorphisme de passage de $\mathbb{K}[[\partial_\zeta]]$ à $\mathbb{K}[[\partial]]$ induit par l'isomorphisme entre $\hat{R}$ et $\mathbb{K}[[\partial_\zeta]]$ et celui entre $\hat{R}$ et $\mathbb{K}[[\partial]]$ est donné par*

$$\begin{array}{rcl} \mathbb{K}[[\partial_\zeta]] & \to & \mathbb{K}[[\partial]] \\ \partial_\zeta^{\mathbf{a}} & \mapsto & \partial^{\mathbf{a}}\, e^{(\zeta,\partial)}. \end{array}$$

Preuve. Pour tout $p = \sum_{\mathbf{a}\in\mathbb{N}^n} p_{\mathbf{a}}\, \mathbf{x}^{\mathbf{a}} \in R$ et tout $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{N}^n$, notons $p^{(\mathbf{b})} = d_{x_1}^{b_1} \cdots d_{x_n}^{b_n}(p) = \sum_{\mathbf{a}\in\mathbb{N}^n} p_{\mathbf{a}}^{(\mathbf{b})} \mathbf{x}^{\mathbf{a}}$. Comme $(\mathbf{d}^{\mathbf{a}})_{\mathbf{a}\in\mathbb{N}^n}$ est la base duale de $(\mathbf{x}^{\mathbf{a}})_{\mathbf{a}\in\mathbb{N}^n}$,

$$\begin{array}{rcl} \partial_\zeta^{\mathbf{b}}(p) & = & \displaystyle\sum_{\mathbf{a}\in\mathbb{N}^n} p_{\mathbf{a}}^{(\mathbf{b})}\, \zeta^{\mathbf{a}} = (\sum_{\mathbf{a}\in\mathbb{N}^n} \zeta^{\mathbf{a}}\, \mathbf{d}^{\mathbf{a}})(\sum_{\mathbf{a}\in\mathbb{N}^n} p_{\mathbf{a}}^{(\mathbf{b})} \mathbf{x}^{\mathbf{a}}) \\ & = & (\displaystyle\sum_{\mathbf{a}\in\mathbb{N}^n} \zeta^{\mathbf{a}}\, \mathbf{d}^{\mathbf{a}})(p^{(\mathbf{b})}) = \left(\partial^{\mathbf{b}}\, e^{(\zeta,\partial)}\right)(p). \end{array}$$

Ce qui montre que $\partial_\zeta^{\mathbf{b}} = \partial^{\mathbf{b}}\, e^{(\zeta,\partial)}$ dans $\mathbb{K}[[\partial]]$.

□

2.2 L'orthogonal d'un idéal et l'orthogonal d'un espace vectoriel

Définition 2.2.1 — *Pour tout idéal I de R, on définit le sous-espace vectoriel de $\hat{R}$*

$$I^\perp = \{\Lambda \in \hat{R};\ \forall p \in I,\ \Lambda(p) = 0\}.$$

Pour tout sous-espace vectoriel D de $\hat{R}$, on définit le sous-espace vectoriel de R

$$D^\perp = \{p \in R;\ \forall \Lambda \in D,\ \Lambda(p) = 0\}.$$

L'espace vectoriel $I^\perp$ est appelé dans la littérature le *système inverse* de I (voir [22]).
Remarque: L'orthogonal d'un idéal I de R n'est pas un idéal de $\mathbb{K}[[\partial]]$.

Ses éléments peuvent se voir comme des formes linéaires sur $B = R/I$. La projection $\pi : R \to B$ induit une application

$$\begin{array}{rcl} \pi_* : \hat{B} & \to & I^\perp \\ \lambda & \mapsto & \lambda \circ \pi \end{array}$$

Il est clair que

Proposition 2.2.2 — *L'application π_* est un isomorphisme entre $I^\perp$ et $\hat{B}$.*
Dans la suite on identifie $I^\perp$ avec $\hat{B}$.

2.2.1 Equation différentielle et système inverse

Proposition 2.2.3 — *Soit $I = (p_1, \ldots, p_s)$ un idéal de R; alors son système inverse*

$$I^\perp = \{\Lambda \in \mathbb{K}[[\partial_\zeta]];\ p_i(\zeta_1 + d_{\partial_{1,\zeta}}, \ldots, \zeta_n + d_{\partial_{n,\zeta}})(\Lambda) = 0, 1 \leq i \leq s\}.$$

Preuve. On a vu que si $\Lambda \in \mathbb{K}[[\partial_\zeta]], (x_i - \zeta_i).\Lambda = d_{\partial_{i,\zeta}}(\Lambda)$. Donc, pour tout $P \in R, P.\Lambda = P(\zeta_1 + d_{\partial_{1,\zeta}}, \ldots, \zeta_n + d_{\partial_{n,\zeta}})(\Lambda)$. Ceci montre que $\Lambda \in I^\perp$ ssi $\forall q \in R$, $\forall i = 1, \ldots, s$,

$$\Lambda(p_i\, q) = p_i \cdot \Lambda(q) = p_i(\zeta_1 + d_{\partial_{1,\zeta}}, \ldots, \zeta_n + d_{\partial_{n,\zeta}})(\Lambda)(q) = 0.$$

□

La proposition permet de voir la résolution de systèmes d'équations différentielles à coefficients constants et la réduction modulo un idéal de R comme le même problème. Voir [26] à propos de cette remarque.

Le système inverse $I^\perp$ est stable par dérivation. En fait, il y a une correspondance entre les idéaux de R et certains sous-espaces vectoriels de $\mathbb{K}[[\partial_\zeta]]$ stables par dérivation.

Théorème 2.2.4 — *Les idéaux de R sont en bijection avec les sous-espaces vectoriels de $\mathbb{K}[[\partial_\zeta]]$ stables par dérivation et fermés pour la topologie $(\partial_{1,\zeta}, \ldots, \partial_{n,\zeta})$-adique.*

Voir [13]. Cette bijection consiste à prendre l'orthogonal dans le dual et dans le bidual, c'est-à-dire l'espace lui-même. Pour tout idéal I de R et pour tout sous-espace vectoriel fermé D de $\hat{R}$, on a en effet les propriétés

$$I^{\perp\perp} = I,\ D^{\perp\perp} = D.$$

Nous donnons quelques propriétés des systèmes inverses.

Définition 2.2.5 — *Soient $\Lambda_1, \ldots, \Lambda_s \in \mathbb{K}[[\partial_\zeta]]$, on note*

$$\langle\langle \Lambda_1, \ldots, \Lambda_s \rangle\rangle$$

le sous-espace vectoriel de $\mathbb{K}[[\partial_\zeta]]$ *engendré par les éléments* Λ_i *et leurs dérivées.*

Proposition 2.2.6 — *Soient* I *et* J *deux idéaux de* R*, alors*

- $I \subset J \Leftrightarrow J^\perp \subset I^\perp$
- $(I \cap J)^\perp = I^\perp + J^\perp$
- $(I + J)^\perp = I^\perp \cap J^\perp$.

2.2.2 Division d'idéaux

Certaines propriétés des idéaux, difficiles à décrire ou à calculer dans R, se traduisent particulièrement bien sur les systèmes inverses. La division en est un exemple.

Proposition 2.2.7 — *Pour tout* $\Lambda_1, \ldots, \Lambda_s \in \mathbb{K}[[\partial_\zeta]]$*, et* $p_1, \ldots, p_t \in R$*,*

$$\langle\!\langle \Lambda_1, \ldots, \Lambda_s \rangle\!\rangle^\perp : (p_1, \ldots, p_t) = \langle\!\langle p_j \cdot \Lambda_i \rangle\!\rangle^\perp_{1 \le i \le s, 1 \le j \le t}$$

Preuve. Comme $\langle\!\langle \Lambda_1, \ldots, \Lambda_s \rangle\!\rangle^\perp$ est un idéal de R,

$$\begin{aligned} P \in \langle\!\langle \Lambda_1, \ldots, \Lambda_s \rangle\!\rangle^\perp : (p_1, \ldots, p_t) &\Leftrightarrow \forall j,\ p_j P \in \langle\!\langle \Lambda_1, \ldots, \Lambda_s \rangle\!\rangle^\perp \\ &\Leftrightarrow \forall i, j, \forall Q \in R,\ \Lambda_i(p_j P Q) = 0 \\ &\Leftrightarrow \forall i, j, \forall Q \in R, p_j \cdot \Lambda_i(P Q) = 0 \\ &\Leftrightarrow P \in \langle\!\langle p_j \cdot \Lambda_i \rangle\!\rangle^\perp. \end{aligned}$$

□

2.2.3 Elimination de variables

La projection ou l'élimination de variables est un deuxième exemple de propriétés qui se traduisent bien sur les systèmes inverses. Soit $r \in \{1, \ldots, n\}$; pour tout idéal I de R, $\sigma_r(I^\perp) = \{\sigma_r(\Lambda) = \Lambda(\partial_1, \ldots, \partial_r, 0, \ldots, 0); \Lambda \in I^\perp\}$. Pour tout idéal $I \subset R_r$, $I^{\perp_r} = I^\perp \cap \mathbb{K}[[\partial_1, \ldots, \partial_r]]$, où $I^\perp \subset \mathbb{K}[[\partial_1, \ldots, \partial_n]]$.

Proposition 2.2.8 — *Pour tout idéal I de R,*

$$(I \cap R_r)^{\perp_r} = \sigma_r(I^\perp).$$

Preuve. Comme $R_r^\perp = \langle\langle \partial_{r+1}, \ldots, \partial_n \rangle\rangle$,

$$\begin{aligned}(I \cap R_r)^{\perp_r} &= (I \cap R_r)^\perp \cap \hat{R}_r = (I^\perp + R_r^\perp) \cap \hat{R}_r \\ &= (I^\perp + \langle\langle \partial_{r+1}, \ldots, \partial_n \rangle\rangle) \cap \hat{R}_r = \sigma_r(I^\perp).\end{aligned}$$

□

2.2.4 Passage de l'homogène à l'affine

Soit $R_0 = \mathbb{K}[x_0, \ldots, x_n]$ l'anneau des polynômes en $n+1$ variables, à coefficients dans $\mathbb{K}$, et σ l'application

$$\begin{aligned}\sigma : R_0 &\to R \\ p(x_0, \ldots, x_n) &\mapsto p(1, x_1, \ldots, x_n).\end{aligned}$$

Cette dernière permet de passer d'un idéal homogène à l'idéal affine correspondant. Elle est surjective mais non injective, et définit une application injective

$$\begin{aligned}\sigma_* : \hat{R} &\to \hat{R}_0 \\ \lambda &\mapsto \sigma_*(\lambda) = \lambda \circ \sigma.\end{aligned}$$

Proposition 2.2.9 — *Pour tout idéal $J \subset R_0$,*

$$\sigma_*^{-1}(J^\perp) = (\sigma(J))^\perp,$$

où σ_*^{-1} est l'image réciproque par σ_*.
Preuve. Pour tout $\Lambda \in \hat{R}$,

$$\begin{aligned}&\Lambda \in (\sigma(J))^\perp \\ &\Leftrightarrow \quad \forall p \in J,\ \Lambda(\sigma(p)) = 0 \\ &\Leftrightarrow \quad \forall p \in J,\ \sigma_*(\Lambda)(p) = 0 \\ &\Leftrightarrow \quad \Lambda \in \sigma_*^{-1}(J^\perp).\end{aligned}$$

□

Posons $e^{\partial_0} = \sum_{a\in\mathbb{N}} \mathbf{d}_0^a$, avec $\mathbf{d}_0^a(p) = \mathbf{d}_{x_0}^a(p)(0)$. Alors l'image par l'application σ_* d'un élément $\mathbf{d}^{\mathbf{m}}, \mathbf{m} \in \mathbb{N}^n$, de la base duale des monômes est

$$\sigma_*(\mathbf{d}^{\mathbf{m}}) = \mathbf{d}^{\mathbf{m}} e^{\partial_0}.$$

En effet, $\sigma_*(\mathbf{d}^{\mathbf{m}})$ est de la forme $\sum_{\mathbf{a}\in\mathbb{N}^{n+1}} \lambda_{\mathbf{a}}\, \mathbf{d}^{\mathbf{a}}$; pour tout $\mathbf{a} = (a_0, \ldots, a_n) \in \mathbb{N}^{n+1}$,

$$\lambda_{\mathbf{a}} = \sigma_*(\mathbf{d}^{\mathbf{m}})(\mathbf{x}^{\mathbf{a}}) = \mathbf{d}^{\mathbf{m}}(x_1^{a_1}\cdots x_n^{a_n}) = \begin{cases} 0 \text{ si } (a_1, \ldots, a_n) \neq \mathbf{m}, \\ 1 \text{ sinon.} \end{cases}$$

Ceci montre que

$$\sigma_*(\mathbf{d}^{\mathbf{m}}) = \sum_{a\geq 0} \mathbf{d}_0^a \mathbf{d}^{\mathbf{m}} = \mathbf{d}^{\mathbf{m}} e^{\partial_0}.$$

L'application σ_* est donc juste la multiplication par e^{∂_0}. Pour tout idéal homogène J tel que $\sigma(J) = I$, l'image par σ_* de $I^\perp$ est $I^\perp e^{\partial_0} \subset\ J^\perp$ (car, si $\Lambda \in I^\perp$ et $p \in J$, $(e^{\partial_0}\Lambda)(p) = \sigma_*(\Lambda)(p) = \Lambda(\sigma(p)) = 0$).

En général, cette inclusion est stricte car $J^\perp$ est homogène (i.e. si $\Lambda \in J^\perp$ alors toutes les composantes homogènes de Λ sont dans $J^\perp$). Pour tout $\Lambda \in \hat{R}_0$, notons $[\Lambda]_d$ la composante homogène de degré d de cette série et $[\sigma_*(I^\perp)]_*$ le sous-espace vectoriel de $\hat{R}_0$ engendré par toutes les composantes homogènes des éléments de $\sigma_*(I^\perp)$.

Proposition 2.2.10 — *Pour tout idéal homogène J tel que $\sigma(J) = I$, on a $[\sigma_*(I^\perp)]_* = (J : x_0^*)^\perp$ avec $(J : x_0^*) = \{p \in R; \exists N \in \mathbb{N},\ x_0^N p \in J\}$.*

Preuve. L'espace vectoriel $[\sigma_*(I^\perp)]_*$ est stable par dérivation car pour $\Lambda \in \hat{R}_0, i \in \{0, \ldots, n\}, d \in \mathbb{N}$,

$$d_{\partial_i}([\Lambda]_d) = [d_{\partial_i}(\Lambda)]_{d-1}.$$

Comme $\sigma_*(I^\perp) = I^\perp e^{\partial_0}$, on a en particulier si $\Lambda \in I^\perp$,

$$d_{\partial_0}([e^{\partial_0}\Lambda]_d) = [d_{\partial_0}(e^{\partial_0}\Lambda)]_{d-1} = [e^{\partial_0}\Lambda]_{d-1}$$

et

$$d_{\partial_0}([e^{\partial_0} I^\perp]_*) = [e^{\partial_0} I^\perp]_*.$$

Notons $\tilde{J}$ l'idéal homogène de R_0 tel que $\tilde{J}^\perp = [e^{\partial_0} I^\perp]_*$, qui vérifie donc la propriété $\tilde{J}^\perp \supset e^{\partial_0} I^\perp$.

L'égalité précédente montre que $(\tilde{J} : x_0) = \tilde{J}$. Par construction, $\sigma_*(I^\perp) = e^{\partial_0} I^\perp \subset \tilde{J}^\perp$ et $\tilde{J}^\perp \subset J^\perp$ car $e^{\partial_0} I^\perp \subset J^\perp$ et $J^\perp$ est homogène donc engendré par les composantes homogènes de ses éléments. Par conséquent,

$$J \subset \tilde{J} \text{ et } \sigma(\tilde{J}) \subset I,$$

donc $\sigma(\tilde{J}) = I$ (car $\sigma(J) = I$). Alors $\tilde{J}$ est le plus petit idéal stable par division par x_0 et tel que $\sigma(\tilde{J}) = I$. Donc $\tilde{J} = (J : x_0^*)$. □

2.3 Points isolés

Nous nous plaçons dans le cas où l'idéal I définit un seul point $\zeta \in \mathbb{K}^n$, et nous notons $\mathbf{m}_\zeta$ l'idéal maximal définissant ζ.

2.3.1 Un idéal $\mathbf{m}_\zeta$-primaire

Proposition 2.3.1 — *Supposons que I soit $\mathbf{m}_\zeta$-primaire; alors $I^\perp \subset \mathbb{K}[\partial_\zeta]$.*
Preuve. Puisqu'il existe un entier N tel que $\mathbf{m}_\zeta^N \subset I \subset \mathbf{m}_\zeta, (\mathbf{x} - \zeta)^\mathbf{a} \in I$ dès que $|\mathbf{a}| = a_1 + \cdots + a_n \geq N$. Soit $\Lambda \in I^\perp$, alors

$$\Lambda = \sum_{\mathbf{a} \in \mathbb{N}^n : |\mathbf{a}| < N} \Lambda((\mathbf{x} - \zeta)^\mathbf{a})\, \mathbf{d}_\zeta^\mathbf{a}.$$

□

Dans ce cas, les éléments du système inverse de I sont des polynômes en ∂_ζ. De plus, $B = R/I$ est de dimension finie μ sur $\mathbb{K}$ (où μ est la multiplicité de la racine ζ), par suite $I^\perp$ est un espace vectoriel de dimension μ.

Ceci établit *une bijection entre les idéaux $\mathbf{m}_\zeta$-primaires et les sous-espaces vectoriels de $\mathbb{K}[\partial_\zeta]$, stables par dérivation et de dimension finie* (voir [13], [22][p. 65], [16]).

2.3.2 La composante $\mathbf{m}_\zeta$-primaire

Dans la pratique, il est rare de traiter directement un idéal $\mathbf{m}_\zeta$-primaire; on a souvent affaire à des idéaux dont une composante est $\mathbf{m}_\zeta$-primaire. Nous allons voir comment on peut isoler cette composante, c'est-à-dire oublier le reste de la variété.

Théorème 2.3.2 — *Soit I un idéal de R et Q_ζ sa composante $\mathbf{m}_\zeta$-primaire que l'on suppose isolée. Alors*

$$(I^\perp \cap \mathbb{K}[\partial_\zeta])^\perp = Q_\zeta.$$

Preuve. Notons $D_\zeta = I^\perp \cap \mathbb{K}[\partial_\zeta]$; nous allons montrer que $D_\zeta = Q_\zeta^\perp$. On a $Q_\zeta^\perp \subset I^\perp$ (car $I \subset Q_\zeta$) et $Q_\zeta^\perp \subset \mathbb{K}[\partial_\zeta]$ (d'après la proposition (2.3.1)), par suite, $Q_\zeta^\perp \subset I^\perp \cap \mathbb{K}[\partial_\zeta]$. Pour montrer l'inclusion inverse, nous utiliserons les deux propriétés suivantes

- La composante $\mathbf{m}_\zeta$-primaire Q_ζ de I est l'ensemble des polynômes f de R tels qu'il existe $g \in R$ avec $f\,g \in I$ et $g(\zeta) \neq 0$ (voir [1]).
- Pour tout $\Lambda \in \mathbb{K}[\partial_\zeta]$ et tout $g \in R$,

$$\begin{aligned}(g \cdot \Lambda)(f) &= g(\zeta_1 + d_{\partial_{1,\zeta}}, \ldots, \zeta_n + d_{\partial_{n,\zeta}})(\Lambda)(f) \\ &= g(\zeta)\Lambda(f) + (g - g(\zeta))(\zeta_1 + d_{\partial_{1,\zeta}}, \ldots, \zeta_n + d_{\partial_{n,\zeta}})(\Lambda)(f).\end{aligned} \tag{1}$$

Montrons par récurrence sur le degré de Λ (en $\partial_\zeta = (\partial_{1,\zeta}, \ldots, \partial_{n,\zeta})$) que $D_\zeta \subset Q_\zeta^\perp$.

Si $\Lambda \in D_\zeta$, est de degré 0, alors Λ est, à un scalaire près, l'évaluation en ζ. Pour tout $f \in Q_\zeta, g \in R$ tels que $g(\zeta) \neq 0$ et $f\,g \in I$, $\Lambda(f\,g) = 0 = f(\zeta)g(\zeta)$, donc $\Lambda(f) = f(\zeta) = 0$, et $\Lambda \in Q_\zeta^\perp$.

Supposons maintenant que tous les éléments de D_ζ de degré $< d$ sont dans $Q_\zeta^\perp$. Soit $\Lambda \in D_\zeta$ de degré d; d'après la formule (1), pour tout $f \in Q_\zeta$, $g \in R$ tels que $g(\zeta) \neq 0$ et $fg \in I$,

$$\begin{aligned}\Lambda(f\,g) = \; 0 = \; & g(\zeta)\Lambda(f) + (g - g(\zeta))(\zeta_1 + d_{\partial_{1,\zeta}}, \ldots, \zeta_n + d_{\partial_{n,\zeta}})(\Lambda)(f) \\ = \; & g(\zeta)\Lambda(f) + \rho(f),\end{aligned}$$

$\rho = (g - g(\zeta))(\zeta_1 + d_{\partial_{1,\zeta}}, \ldots, \zeta_n + d_{\partial_{n,\zeta}})(\Lambda)$ est de degré $< d$ en ∂_ζ et $\rho \in D_\zeta$ (car D_ζ est stable par dérivation). Par hypothèse de récurrence, $\rho(f) = 0$. Il en découle que $\Lambda(f) = 0$, et $\Lambda \in Q_\zeta^\perp$. □

Soit $N \in \mathbb{N}$ tel que $\mathbf{m}_\zeta^N \subset Q_\zeta$; alors le degré des éléments de D_ζ est au plus N.

Définition 2.3.3 — *On appelle l'indice de nil-potence de Q_ζ l'entier N_ζ égal au maximum des degrés des éléments de D_ζ.*

On vérifie facilement que N_ζ est le plus grand entier N tel que

$$\mathbf{m}_\zeta^N \not\subset Q_\zeta.$$

En effet, pour tout $\Lambda \in D_\zeta$ de degré N_ζ, il existe un monôme $m = (\mathbf{x} - \zeta)^{\mathbf{a}}$ de degré N_ζ tel que $\Lambda(m) \neq 0$, donc $\mathbf{m}_\zeta^{N_\zeta} \not\subset Q_\zeta$. Par contre, pour tout monôme $m = (\mathbf{x} - \zeta)^{\mathbf{a}}$ tel que $|\mathbf{a}| > N_\zeta$ et tout $\Lambda \in D_\zeta$, $\Lambda(m) = 0$, donc $(\mathbf{x} - \zeta)^{\mathbf{a}} \in Q_\zeta$, ce qui implique que $\mathbf{m}_\zeta^{N_\zeta + 1} \subset Q_\zeta$.

Théorème 2.3.4 — *Soient $I = (p_1, \ldots, p_s)$ un idéal de R ayant une composante isolée Q_0 en 0, et $q_1, \ldots, q_s$ des polynômes homogènes de degrés $> N_0 + 1$. Alors l'idéal*

$$\tilde{I} = (p_1 + q_1, \ldots, p_s + q_s)$$

a pour composante $\mathbf{m}_0$-primaire isolée Q_0.

Preuve. Notons $\tilde{p}_i = p_i + q_i, 1 \leq i \leq s$. Un élément $\Lambda \in \mathbb{K}[\partial_0]$ est dans $I^\perp$ (resp. $\tilde{I}^\perp$) ssi pour tout $\mathbf{a} \in \mathbb{N}^n$, $\Lambda(\mathbf{x}^\mathbf{a} p_i) = 0$ (resp. $\Lambda(\mathbf{x}^\mathbf{a} \tilde{p}_i) = 0), 1 \leq i \leq s$. Or si le degré de Λ est $\leq N_0 + 1$,

$$\Lambda(\mathbf{x}^\mathbf{a} \tilde{p}_i) = \Lambda(\mathbf{x}^\mathbf{a} p_i).$$

Donc $I^\perp$ et $\tilde{I}^\perp$ coïncident jusqu'au degré $N_0 + 1$. Par conséquent, il n'existe pas d'éléments de degré exactement $N_0 + 1$ dans $\tilde{I}^\perp$ (car N_0 est l'indice de nil-potence de Q_0), et a fortiori pas d'éléments de degré $> N_0$ (car $\tilde{I}^\perp$ est stable par dérivation). Il en résulte que

$$\tilde{I}^\perp \cap \mathbb{K}[\partial_0] = I^\perp \cap \mathbb{K}[\partial_0].$$

□

La composante primaire Q_0 en 0 reste inchangée par déformation en degré suffisamment élevé. Ceci est vrai par translation en tout autre point ζ de $\mathbb{K}^n$.

Théorème 2.3.5 — *Soit I un idéal de R définissant des points isolés $\zeta_1, \ldots, \zeta_s$; alors*

$$I^\perp = Q_1^\perp \oplus \cdots \oplus Q_s^\perp,$$

où Q_i est la composante $\mathbf{m}_{\zeta_i}$-primaire. De plus, pour tout élément Λ de $I^\perp$, il existe des polynômes en $\partial_1, \ldots, \partial_n$ uniques $\Lambda_1, \ldots, \Lambda_n$, tels que

$$\Lambda = \sum_{i=1}^{s} \Lambda_i(\partial)\, e^{(\zeta_i, \partial)}. \tag{2}$$

Preuve. Comme $I = Q_1 \cap \cdots \cap Q_s$, $I^\perp = Q_1^\perp + \cdots + Q_s^\perp$. De plus, pour $j_1, \ldots, j_p \in \{1, \ldots, n\}$ et $i \neq j_1, \ldots, j_p$, $Q_i + (Q_{j_1} \cap \ldots \cap Q_{j_p}) = R$, donc $Q_i^\perp \cap (Q_{j_1}^\perp + \ldots + Q_{j_p}^\perp) = R^\perp = \{0\}$ et la somme ci-dessus est directe. Un élément de $I^\perp$ est donc une somme de polynômes de dérivations aux points $\zeta_i, 1 \leq i \leq s$. En utilisant l'isomorphisme (2.1.1), on obtient la décomposition (2). □

2.4 Passage du système inverse au quotient

La construction d'une base de $I^\perp$ peut se faire facilement si on sait réduire tout polynôme en une forme normale modulo I. Le système inverse de I capture, d'une certaine manière, tous les éléments qui se réduisent à un même terme. Soient I un idéal de R et (b_i) une base de $B = R/I$. Alors pour tout monôme $\mathbf{x}^\mathbf{a}$, il existe des scalaires uniques $(\lambda_{\mathbf{a},i})_i$ presque tous nuls, tels que

$$\mathbf{x}^\mathbf{a} - \sum_i \lambda_{\mathbf{a},i}\, b_i \in I.$$

Proposition 2.4.1 — *La famille* $(\sum_{\mathbf{a}\in\mathbb{N}^n} \lambda_{\mathbf{a},i}\, \mathbf{d}^\mathbf{a})_i$ *forme une base du système inverse de* I.

Preuve. Soit $(\Lambda_i) \subset \hat{B}$ (que l'on identifie avec $I^\perp$) la base duale de $(b_i) \subset B$. Les éléments Λ_i s'écrivent sous la forme

$$\Lambda_i = \sum_{\mathbf{a}\in\mathbb{N}^n} \mu_{\mathbf{a},i}\, \mathbf{d}^\mathbf{a}, \mu_{\mathbf{a},i} \in \mathbb{K}.$$

D'après les relations ci-dessus,

$$\mu_{\mathbf{a},i} = \Lambda_i(\mathbf{x}^\mathbf{a}) = \sum_j \lambda_{\mathbf{a},j}\, \Lambda_i(b_j) = \lambda_{\mathbf{a},i}.$$

□

Cette construction peut se reformuler de la façon suivante. Soit

$$\Delta = \sum_{\mathbf{a}\in\mathbb{N}^n} \mathbf{x}^\mathbf{a} \otimes \mathbf{d}^\mathbf{a}$$

l'élément diagonale de $\mathbb{K}[[\mathbf{x}, \partial]]$. Pour $p \in R$, on définit $\Delta(p) = \sum_{\mathbf{a}\in\mathbb{N}^n} \mathbf{x}^\mathbf{a}\mathbf{d}^\mathbf{a}(p)$, et pour $\lambda \in \hat{R}, \lambda(\Delta) = \sum_{\mathbf{a}\in\mathbb{N}^n} \lambda(\mathbf{x}^\mathbf{a})\mathbf{d}^\mathbf{a}$. On vérifie que

$$\Delta(p) = p,\ \lambda(\Delta) = \lambda.$$

Nous nous plaçons dans le cas où B est un $\mathbb{K}$-espace vectoriel de dimension finie.

Proposition 2.4.2 — *Les propriétés suivantes sont équivalentes*

1. *Il existe une décomposition de* Δ *sous la forme*

$$\Delta = \sum_{i=1}^{\infty} a_i \otimes \beta_i$$

où les familles (a_i) *et* (β_i) *sont linéairement indépendantes sur* $\mathbb{K}$ *avec*

- $a_j \in I$ *pour* $j > \mu$,

– $\beta_i \in I^\perp$ *pour* $1 \leq i \leq \mu$.

2. $(a_i)_{1\leq i\leq \mu}$ *est une base de* B .

3. $(\beta_i)_{1\leq i\leq \mu}$ *est une base de* $I^\perp$.

Si ces points sont satisfaits, alors $(a_i)_{1\leq i\leq \mu}$ *et* $(\beta_i)_{1\leq i\leq \mu}$ *sont des bases duales .*
Preuve. Supposons que Δ se décompose suivant *1*. Puisque (a_i) engendre $\mathbb{K}[\mathbf{x}]$ (comme $\mathbb{K}$-espace vectoriel), $(a_i)_{1\leq i\leq \mu}$ engendre B.

Nous avons de plus $\beta_i(\Delta) = \beta_i = \sum_{j=1}^{\mu} \beta_i(a_j)\,\beta_j$; ceci implique

$$\beta_i(a_j) = \delta_{i,j} \text{ pour } 1 \leq i,j \leq \mu, \tag{3}$$

où $\delta_{i,j}$ est le symbole de Kronecker. Par conséquent, $(a_i)_{1\leq i\leq \mu}$ est libre dans B. En effet, si $\sum_{l=1}^{\mu} \lambda_l\, a_l \in I$, alors $\beta_i(\sum_l \lambda_l\, a_l) = 0$ et $\lambda_l = 0$ pour $1 \leq l \leq \mu$. Ainsi $(a_i)_{1\leq i\leq \mu}$ est une base de B. La relation (3) montre que $(\beta_i)_{1\leq i\leq \mu}$ est la base duale de $(a_i)_{1\leq i\leq \mu}$ et les points *2* et *3* sont vérifiés.

Supposons maintenant que *2* soit vérifié. Alors il existe une famille libre $(a_j)_{j>\mu} \subset I$ telle que l'espace vectoriel engendré par $(a_1, \ldots, a_\mu, a_{\mu+1}, \ldots)$ soit une base de $\mathbb{K}[\mathbf{x}]$. Ceci permet de réécrire Δ sous la forme

$$\Delta = \sum_{i=1}^{\mu} a_i \otimes \beta'_i + \sum_{j>\mu} a_j \otimes \beta'_j,$$

avec les (β'_j) linéairement indépendants. Soit $(\beta_i)_{1\leq i\leq \mu} \subset I^\perp$ la base duale de $(a_i)_{1\leq i\leq \mu}$. On a alors

$$\beta_i(\Delta) = \beta_i = \sum_{j=1}^{\mu} \beta_i(a_j)\beta'_j = \beta'_i\ , \quad 1 \leq i \leq \mu$$

ce qui montre *1*.

Si *3* est vérifié, alors on choisit pour (a_i) la base duale de (β_i) et on utilise le *2*.
□

Cette propriété peut être utilisée dans les deux sens. Si nous savons réduire à une forme normale tout monôme (par exemple, en utilisant une base de Gröbner) alors nous pouvons calculer une base du système inverse (au moins en tronquant à un certain degré). Inversement, si nous connaissons le système inverse alors nous pouvons construire les générateurs de l'idéal. Nous illustrons ceci sur deux exemples très simples, où les éléments du système inverse sont des polynômes.

Exemple 1 :
Nous considérons l'idéal I engendré par

$$p_1 := y - x^2,\ p_2 := y^2 - x^3,\ p_3 := x^4.$$

Pour construire $I^\perp$, nous utilisons les relations $x\,y \equiv x^3 \equiv y^2 \equiv x^4 \equiv 0$ modulo I et $x^2 = y - p_1$. On réécrit Δ sous la forme

$$\begin{aligned}\Delta &= \mathbf{d}^0 + x\,\mathbf{d}_1 + y\,\mathbf{d}_2 + x^2\,\mathbf{d}_1^2 + \cdots \\ &= \mathbf{d}^0 + x\,\mathbf{d}_1 + y\,\mathbf{d}_2 + (y - p_1)\,\mathbf{d}_1^2 + \cdots \\ &= \mathbf{d}^0 + x\,\mathbf{d}_1 + y\,(\mathbf{d}_2 + \mathbf{d}_1^2) + \cdots\end{aligned}$$

les points ... désignant des éléments de $I\,\hat{R} = I \otimes \hat{R}$. Les produits tensoriels sont implicites dans cette notation. Donc $I^\perp = \langle \mathbf{d}_2 + \mathbf{d}_1^2, \mathbf{d}_1, \mathbf{d}^0 \rangle = \langle\langle \mathbf{d}_2 + \mathbf{d}_1^2 \rangle\rangle$.

Exemple 2 :
Nous considérons le système inverse

$$\langle\langle \mathbf{d}_1^2 + \mathbf{d}_2^2 + \mathbf{d}_1\mathbf{d}_2 \rangle\rangle$$

qui est engendré (comme $\mathbb{K}$-espace vectoriel) par les éléments $\Lambda_2 = \mathbf{d}_1^2 + \mathbf{d}_2^2 + \mathbf{d}_1\mathbf{d}_2, \Lambda_1 = \mathbf{d}_1 + \mathbf{d}_2, \Lambda_0 = \mathbf{d}^0$, et nous voulons construire l'idéal I. On réécrit Δ sous la forme

$$\begin{aligned}\Delta &= \mathbf{d}^0 + x\,\mathbf{d}_1 + y\,\mathbf{d}_2 + x^2\,\mathbf{d}_1^2 + x\,y\,\mathbf{d}_1\,\mathbf{d}_2 + y^2\,\mathbf{d}_2^2 + \cdots \\ &= \Lambda_0 + x\,(\Lambda_1 - \mathbf{d}_2) + y\,\mathbf{d}_2 + x^2\,(\Lambda_2 - \mathbf{d}_2^2 - \mathbf{d}_1\,\mathbf{d}_2) + x\,y\,\mathbf{d}_1\,\mathbf{d}_2 + y^2\,\mathbf{d}_2^2 + \cdots \\ &= \Lambda_0 + x\,\Lambda_1 + x^2\,\Lambda_2 + (y - x)\,\mathbf{d}_2 + (x\,y - x^2)\,\mathbf{d}_1\,\mathbf{d}_2 + (y^2 - x^2)\,\mathbf{d}_2^2 + \cdots\end{aligned}$$

On voit que

$$\langle\langle \mathbf{d}_1^2 + \mathbf{d}_2^2 + \mathbf{d}_1\mathbf{d}_2 \rangle\rangle^\perp = (x - y) + (x, y)^3,$$

et que $(1, x, x^2)$ est une base du quotient B.

Dans le cas où B est un espace vectoriel de dimension finie, la structure multiplicative du quotient peut se retrouver directement, comme le montre la proposition suivante. Soit $(\beta_1, \ldots, \beta_\mu)$ une base de l'espace vectoriel $I^\perp$. Pour tout $k \in \{1, \ldots, n\}$,

$$d_{\partial_k}(\beta_i) = \sum_{j=1}^{\mu} \lambda_{i,j}^k \beta_j \quad , \quad \lambda_{i,j}^k \in \mathbb{K}.$$

Notons M_k la matrice $(\lambda_{i,j}^k)_{1\leq i,j\leq \mu}$.

Proposition 2.4.3 — *Les matrices $M_k, 1 \leq k \leq n$, sont les matrices de multiplication par x_k dans B dans la base duale de $(\beta_i)_{1\leq i\leq \mu}$.*
Preuve. Soit $(b_1, \ldots, b_\mu)$ la base duale de $(\beta_1, \ldots, \beta_\mu)$ dans B. Le coefficient d'indices i, j de la matrice de multiplication par x_k dans B dans la base (b_j) est donné par

$$\begin{aligned} \beta_i(x_k\, b_j) &= (x_k \cdot \beta_i)(b_j) \\ &= d_{\partial_k}(\beta_i)(b_j) = \sum_{l=1}^{\mu} \lambda_{i,l}^k \beta_l(b_j) = \lambda_{i,j}^k. \end{aligned}$$

□

2.5 Construction du système inverse dans le cas local

Soit I un idéal de R et $D = I^\perp \cap \mathbb{K}[\partial]$ le système inverse de la composante primaire isolée au point $\zeta = 0$. Notons $\mathbb{K}[\partial]_d$ l'ensemble des polynômes en ∂ de degré au plus d et $D_d = D \cap \mathbb{K}[\partial]_d$. Nous allons voir comment on peut construire D_d à partir de D_{d-1}. Ainsi si les éléments de I s'annulent en 0, D_0 est engendré par ∂^0 (∂^0 est la forme linéaire telle que $\partial^0(p) = p(0)$) et il sera alors possible de construire tous les D_j par récurrence.

Notons pour $p \in \mathbb{K}[\partial], p_{|\partial_i=0} = p(\partial_1, \ldots, \partial_{i-1}, 0, \partial_{i+1}, \ldots, \partial_n)$.

Définition 2.5.1 — *On appelle i-primitive de $p \in \mathbb{K}[\partial]$ (sans terme constant), le polynôme q, noté $\int_i p$, tel que $d_{\partial_i} q = p$ et $q_{|\partial_i} = 0$.*

2.5.1 Passage de D_{d-1} à D_d

Les éléments de D_{d-1} sont les dérivées des éléments de D_d; donc pour obtenir les éléments de D_d, l'idée est d'intégrer les éléments de D_{d-1}. La construction de D_d à partir de D_{d-1} est basée sur le théorème suivant.

Théorème 2.5.2 — *Supposons que l'idéal I soit engendré par $p_1, \ldots, p_m$ et $d > 1$. Soit $(\beta_1, \ldots, \beta_s)$ une base de D_{d-1}. Les éléments de D_d sans terme constant sont les Λ de la forme*

$$\Lambda = \sum_{j=1}^{s} \lambda_j^1 \int_1 \beta_j|_{\partial_2=0,\ldots,\partial_n=0} \tag{4}$$

$$+\sum_{j=1}^{s}\lambda_j^2\int_2\beta_j|_{\partial_3=0,\ldots,\partial_n=0}+\cdots+\sum_{j=1}^{s}\lambda_j^n\int_n\beta_j \quad , \quad \lambda_j^k\in\mathbb{K}\ ,$$

tels que

1. $\sum_{j=1}^{s}\lambda_j^k d_{\partial_l}\beta_j-\sum_{j=1}^{s}\lambda_j^l d_{\partial_k}\beta_j=0$ *pour* $1\le k<l\le n$,
2. $\Lambda(p_i)=0$ *pour* $1\le i\le m$.

Preuve. Soit $\Lambda\in D_d$ sans terme constant. Il se décompose de manière unique en

$$\Lambda=\Lambda_1(\partial_1,\ldots,\partial_n)+\Lambda_2(\partial_2,\ldots,\partial_n)+\cdots+\Lambda_n(\partial_n),$$

avec tous les monômes de $\Lambda_i\in\mathbb{K}[\partial_i,\ldots,\partial_n]\backslash\mathbb{K}[\partial_{i+1},\ldots,\partial_n]$. On a alors $\int_i d_{\partial_i}(\Lambda_i)=\Lambda_i, 1\le i\le n$.

Comme $d_{\partial_1}(\Lambda)=d_{\partial_1}(\Lambda_1)\in D_{d-1}=\langle\beta_1,\ldots,\beta_s\rangle$, il existe des scalaires $\lambda_j^1\in\mathbb{K}$ tels que

$$\Lambda_1=\int_1 d_{\partial_1}(\Lambda_1)=\sum_{j=1}^{s}\lambda_j^1\int_1\beta_j.$$

Considérons maintenant $d_{\partial_2}(\Lambda)=d_{\partial_2}(\Lambda_1)+d_{\partial_2}(\Lambda_2)$ qui est dans D_{d-1}. Il existe alors $\lambda_j^2\in\mathbb{K}, 1\le j\le s$, tels que

$$\begin{aligned}\Lambda_2=\int_2 d_{\partial_2}(\Lambda_2) &= \sum_{j=1}^{s}\lambda_j^2\int_2\beta_j-\int_2 d_{\partial_2}(\Lambda_1)\\ &= \sum_{j=1}^{s}\lambda_j^2\int_2\beta_j-(\Lambda_1-\Lambda_1|_{\partial_2=0}),\end{aligned}$$

car $\int_2 d_{\partial_2}(\Lambda_1)$ est la partie de Λ_1 qui *dépend* de ∂_2. Par suite

$$\Lambda_1+\Lambda_2=\sum_{j=1}^{s}\lambda_j^1\int_1\beta_j|_{\partial_2=0}+\sum_{j=1}^{s}\lambda_j^2\int_2\beta_j.$$

Posons $\sigma_2=\Lambda_1+\Lambda_2$. Le même calcul appliqué à $d_{\partial_3}(\Lambda)$ donne

$$\Lambda_3=\sum_{j=1}^{s}\lambda_j^3\int_3\beta_j-(\sigma_2-\sigma_2|_{\partial_3=0})$$

et

$$\begin{aligned}\Lambda_1+\Lambda_2+\Lambda_3 &= \sum_{j=1}^{s}\lambda_j^1\int_1\beta_j|_{\partial_2=0,\partial_3=0}\\ &\quad+\sum_{j=1}^{s}\lambda_j^2\int_2\beta_j|_{\partial_3=0}+\sum_{j=1}^{s}\lambda_j^3\int_3\beta_j.\end{aligned}$$

Par récurrence, on obtient la formule (4) et pour tout $k,l\in\{1,\ldots,n\}$, les relations

$$\sigma_k=\Lambda_1+\cdots+\Lambda_k=\sum_{j=1}^{s}\lambda_j^1\int_1\beta_j|_{\partial_2=0,\ldots,\partial_k=0}$$
$$+\sum_{j=1}^{s}\lambda_j^2\int_2\beta_j|_{\partial_3=0,\ldots,\partial_k=0}+\cdots+\sum_{j=1}^{s}\lambda_j^k\int_k\beta_j \qquad (5)$$

et

$$\Lambda_l=\sum_{j=1}^{s}\lambda_j^l\int_l\beta_j-(\sigma_{l-1}-\sigma_{l-1}|_{\partial_l=0}). \qquad (6)$$

Le point *2* est une conséquence directe de $\Lambda\in I^\perp$. Montrons maintenant que *1* est vérifié. Nous utilisons, $d_{\partial_k}\Lambda_l=0$ pour $k<l$. D'après (6), $d_{\partial_k}\Lambda_l=0$ entraîne

$$\sum_{j=1}^{s}\lambda_j^l\int_l d_{\partial_k}\beta_j=d_{\partial_k}(\sigma_{l-1}-\sigma_{l-1}|_{\partial_l=0}).$$

En dérivant l'égalité précédente par rapport à ∂_l, et en utilisant $d_{\partial_k}(\sigma_{l-1})=d_{\partial_k}(\sigma_k)$ (pour $k<l$), $d_{\partial_k}(\sigma_k)=\sum_{j=1}^{s}\lambda_j^k\,\beta_j$ (d'après (5)), on obtient

$$\sum_{j=1}^{s}\lambda_j^l d_{\partial_k}\beta_j-\sum_{j=1}^{s}\lambda_j^k d_{\partial_l}\beta_j=0.$$

Réciproquement, supposons que Λ soit de la forme (4), que les conditions *1, 2* soient satisfaites et montrons que $\Lambda\in D_d$. Cet élément se décompose en $\Lambda=\Lambda_1+\cdots+\Lambda_n$ avec $\Lambda_k=\sum_{j=1}^{s}\lambda_j^k\int_k\beta_j-(\sigma_{k-1}-\sigma_{k-1}|_{\partial_k=0})$ et $\sigma_k=\Lambda_1+\cdots+\Lambda_k, 1\le k\le n$ (avec $\sigma_0=0$). Nous avons la relation (5) par récurrence. Puisque Λ vérifie *1*, d'après ce qui précéde, $d_{\partial_k}(\Lambda_l)=0$ pour $k<l$ et $\Lambda_l\in\mathbb{K}[\partial_l,\ldots,\partial_n]$. Par construction, Λ_l n'a pas de terme constant et appartient donc à $\mathbb{K}[\partial_l,\ldots,\partial_n]\backslash\mathbb{K}[\partial_{l+1},\ldots,\partial_n]$.

La formule (5) implique

$$d_{\partial_k}\Lambda = \sum_{j=1}^{s} \lambda_j^k \beta_j \in D_{d-1},\ 1 \le k \le n. \tag{7}$$

Comme D_{d-1} est stable par dérivation, toutes les dérivées de Λ sont dans D_{d-1}. La dérivation correspond à la multiplication sur les polynômes, donc si $\Lambda(p_i) = 0, 1 \le i \le n$, alors $\Lambda(p_i q) = 0$, pour tout $q \in R$, et $\Lambda \in I^\perp$. □

La condition *1* traduit seulement le fait que les *dérivations* $d_{\partial_i}, 1 \le i \le n$, *commutent ou de manière équivalente que la multiplication dans* B *est commutative.*

2.5.2 Exemple

On considère le point isolé $0 \in \mathbb{K}^2$ du système

$$p_1 = 2\,x_1\,x_2^2 + 5\,x_1^4,\ p_2 = 2\,{x_1}^2\,x_2 + 5\,x_2^4.$$

Pour tout $i, j \in \mathbb{N}$, on note $\mathbf{d}_i^j = \frac{1}{j!}\partial_i^j$. On vérifie facilement que $I^\perp$ contient $1, \mathbf{d}_1, \mathbf{d}_2$, $\mathbf{d}_1^2, \mathbf{d}_1\mathbf{d}_2, \mathbf{d}_2^2, \mathbf{d}_1^3, \mathbf{d}_2^3$. Pour trouver les autres éléments de D, on intègre ceux-ci suivant la formule (4) en ne gardant que les éléments qui apportent de nouveaux termes

$$\Lambda = \lambda_1\,\mathbf{d}_1^4 + \lambda_2\,\mathbf{d}_1^2\mathbf{d}_2 + \lambda_3\,\mathbf{d}_1\mathbf{d}_2^2 + \lambda_4\,\mathbf{d}_2^4 + \lambda_5\,\mathbf{d}_1^3\mathbf{d}_2 + \lambda_6\,\mathbf{d}_1\mathbf{d}_2^3,\ \lambda_i \in \mathbb{K}.$$

Les conditions $\Lambda(p_1) = \Lambda(p_2) = 0$, entraînent que

$$\Lambda = \lambda_1(2\,\mathbf{d}_1^4 - 5\,\mathbf{d}_1\mathbf{d}_2^2) + \lambda_2(2\,\mathbf{d}_2^4 - 5\,\mathbf{d}_1^2\mathbf{d}_2)$$

Un nouvel élément de $I^\perp$ sera (d'après le théorème précédent) de la forme $\Lambda = \lambda_1\mathbf{d}_1^5 + \lambda_2(2\,\mathbf{d}_1^4\mathbf{d}_2 - 5\,\mathbf{d}_1\mathbf{d}_2^3) + \lambda_3(2\,\mathbf{d}_2^5 - 5\,\mathbf{d}_1^2\mathbf{d}_2^2)$ et ses dérivées doivent être dans l'espace vectoriel engendré par les éléments précédents, ce qui impose que

$$\Lambda = \lambda\,(5\,\mathbf{d}_1^2\mathbf{d}_2^2 - 2\,\mathbf{d}_1^5 - 2\,\mathbf{d}_2^5),\ \lambda \in \mathbb{K}.$$

Une nouvelle intégration ne fournit pas d'autre élément dans D qui est alors engendré par

$$1, \mathbf{d}_1, \mathbf{d}_2, \mathbf{d}_1^2, \mathbf{d}_1\mathbf{d}_2, \mathbf{d}_2^2, \mathbf{d}_1^3, \mathbf{d}_2^3,$$
$$2\,\mathbf{d}_1^4 - 5\,\mathbf{d}_1\mathbf{d}_2^2, 2\,\mathbf{d}_2^4 - 5\,\mathbf{d}_1^2\mathbf{d}_2, 5\,\mathbf{d}_1^2\mathbf{d}_2^2 - 2\,\mathbf{d}_1^5 - 2\,\mathbf{d}_2^5.$$

Le point 0 est de multiplicité 11.

2.5.3 Un peu d'algèbre linéaire

Ceci nous conduit naturellement à un algorithme qui construit étape par étape, les générateurs de D. Nous obtiendrons par la même occasion la structure du quotient, c'est-à-dire les matrices de multiplications par les variables x_l ou les matrices de dérivations par $d_{\partial_l}, 1 \leq l \leq n$.

Entrée : $(p_1, \ldots, p_m) \in R^m$ et $\zeta \in \mathbb{K}^n$ tels que $I = (p_1, \ldots, p_m)$ a une composante $\mathbf{m}_\zeta$-primaire isolée Q_ζ.
Sortie : Une base de $Q_\zeta^\perp$ dans $\mathbb{K}[\partial_\zeta]$ et les matrices de multiplication par $x_k - \zeta_k$ dans B.

▷ $D_0 := 1$; d := 0; s_0 := 1; test := vrai;
Pour k de 1 à n faire $U^k[1]$:= [0];
▷ Tant que teste faire
1) S := système d'équations 1,2 en λ_j^k;
2) résoudre le système S;
3) S'il n'y a pas de nouvelle solution alors teste := faux
sinon
soit $(\delta_1, \ldots, \delta_s)$ une base des nouvelles solutions
telle que $d_{\partial_k}(\delta_i) = \sum_{j=1}^{s_d} \lambda_{j,s_d+i}\, \beta_j$;
$s_{d+1} := s_d + s$;
$D_{d+1} := D_d, \delta_1, \ldots, \delta_s = \beta_1, \ldots, \beta_{s_{d+1}}$;
Pour k de 1 à n faire
Pour i de $s_d + 1$ à s_{d+1} faire
$U^k[i] := [\lambda_{1,i}, \ldots, \lambda_{s_d,i}]$;
$d := d + 1$;
▷ D_d et U^k pour $1 \leq k \leq n$;

Une étape importante de cet algorithme est le point (2) que nous allons détailler. Supposons que nous soyons au rang d et que nous avons calculé une base $\beta_1, \ldots, \beta_{s_d}$ de D_d. Posons $U_k = (u_{i,j}^k)_{1 \leq i,j \leq s_d}$ tel que

$$d_{\partial_k}(\beta_j) = \sum_{i=1}^{s_d} u_{i,j}^k\, \beta_i \quad , \quad 1 \leq j \leq s_d.$$

Soient $v_l = (\lambda_1^l, \ldots, \lambda_{s_d}^l), 1 \leq l \leq n$, des vecteurs tels que $V = [v_1, \ldots, v_n]$ soit une solution du système *1, 2* du théorème (2.5.2). Les équations *1* se réécrivent sous la

forme

$$U_k\, v_l - U_l\, v_k = 0,\ 1 \leq k < l \leq n.$$

Les équations *2* correspondent à

$$[A_1, \ldots, A_n].\, V = 0,$$

où les matrices $A_1, \ldots, A_n$ sont de taille $m \times s_d$ et font intervenir les coefficients des $p_1, \ldots, p_m$. Le système générale est donc de la forme

$$\begin{bmatrix} U_n & & & & -U_1 \\ & U_n & & & -U_2 \\ & & \ddots & & \vdots \\ & & & U_n & -U_{n-1} \\ U_{n-1} & & & -U_1 & \\ & \ddots & & \vdots & \\ & & U_{n-1} & -U_{n-2} & \\ \vdots & \vdots & \vdots & & \\ U_2 & -U_1 & & & \\ A_1 & \cdots & \cdots & \cdots & A_n \end{bmatrix} .\, V = 0\ ,$$

où les blancs désignent des 0. C'est un système linéaire de taille $(\frac{1}{2}\, n\, (n-1)\, s_d + m) \times n\, s_d$. Pour résoudre ce système, nous supposons de plus que l'espace vectoriel engendré par les lignes des U_i est inclus dans celui engendré par les lignes de U_n. On peut toujours s'y ramener en prenant pour U_n une combinaison linéaire *générique* des matrices $U_1, \ldots, U_n$ (i.e. on remplace x_n par une combinaison linéaire de $x_1, \ldots, x_n$).

Par élimination de Gauss entre les lignes où intervient U_n et les autres, on remplace les lignes $U_{n-1}\, v_1 - U_1\, v_{n-1} = 0$ par un système de la forme $W_{1,n-1}\, v_n = 0$, où $W_{1,n-1}$ est une matrice de taille $s_d \times s_d$. Le même type de calcul sur les autres $\frac{1}{2}\,(n-1)\,(n-2)+m$ blocs non-nuls permet de transformer le système en un système de taille $(\frac{1}{2}\, n\, (n-1)\, s_d + m) \times s_d$ de la forme $W\, .\, v_n = 0$.

Comme cette matrice est élargie de $s_d - s_{d-1}$ à chaque étape de l'algorithme, on peut supposer que la triangulation des matrices U_n et la réduction ci-dessus sont faites jusqu'au rang s_{d-1}. Le nombre d'étapes nécessaires pour les réductions supplémentaires est donc majoré par $k\,(\frac{1}{2}\, n\, (n-1)\ + m) \times s_d^2 \times (s_d - s_{d-1})$ (k est une constante). Pour obtenir les nouvelles solutions du système $W\, .\, v_n = 0$, il faut au plus $k'\,(\frac{1}{2}\, n\, (n-1)\, s_d + m) \times s_d\, (s_d - s_{d-1})$ opérations arithmétiques supplémentaires (k' est une constante).

Le nombre total d'opérations pour l'étape (2) est donc majoré par $\mathcal{O}(n^2\mu^3+m\,\mu^3)$ où $\mu-1=s_\nu-s_0=(s_1-s_0)+\cdots+(s_\nu-s_{\nu-1})$.

Voir aussi [23] pour une autre approche.

3 Anneaux de Gorenstein

On suppose dans cette section que B est une $\mathbb{K}$-algèbre de dimension finie.

3.1 Isomorphisme entre $Ann_{B\otimes B}(\mathcal{D})$ et $Hom_B(\hat{B},B)$

Il existe un isomorphisme canonique $\triangleright$ de $\mathbb{K}$-espace vectoriel entre $B\otimes_{\mathbb{K}}B$ et $Hom_{\mathbb{K}}(\hat{B},B)$,

$$\begin{array}{rcl}\triangleright : B\otimes_{\mathbb{K}}B & \rightarrow & Hom_{\mathbb{K}}(\hat{B},B)\\ x & \mapsto & x^{\triangleright}\end{array}$$

tel que si $x=a\otimes b$ et $l\in\hat{B}$ alors $(a\otimes b)^{\triangleright}(l)=(1\otimes l)(a\otimes b)=l(b)a$.

En effet, supposons que l'application $\triangleright$ n'est pas injective, et soit $x(\neq 0)\in\ker(\triangleright)$; x s'écrit sous la forme

$$x=\sum_i a_i\otimes b_i$$

où les familles (a_i) et (b_i) sont indépendantes sur $\mathbb{K}$. Il existe alors $\lambda\in\hat{B}$ tel que $\lambda(b_1)=1$ et $\lambda(b_i)=0$ si $i\neq 1$. On a $x^{\triangleright}(\lambda)=a_1=0$, d'où une contradiction. Ainsi, $\triangleright$ est injective, et donc bijective (car B est un $\mathbb{K}$-espace vectoriel de dimension finie).

Pour tout $x\in B\otimes_{\mathbb{K}}B$, $\lambda\in\hat{B}$, on notera aussi $x^{\triangleright}(\lambda)=x\triangleright\lambda$. On pourra considérer, de la même façon, l'action de la forme linéaire à gauche: $x^{\triangleleft}(\lambda)=x\triangleleft\lambda=(\lambda\otimes 1)(x)$. Si rien n'est précisé, $x(\lambda)=x\triangleright\lambda$.

Nous considérons maintenant les éléments de $Hom_{\mathbb{K}}(\hat{B},B)$ qui sont compatibles avec la multiplication dans B, c'est-à-dire les éléments de $Hom_B(\hat{B},B)$.

Théorème 3.1.1 — *L'application $\triangleright$ définit ci-dessus induit un isomorphisme de B-module entre $Ann_{B\otimes B}(\mathcal{D})$ et $Hom_B(\hat{B},B)$.*

Preuve. En effet,

$$x=\sum_k a_k\otimes b_k\in Ann_{B\otimes B}(\mathcal{D}) \quad\Leftrightarrow\quad \forall s\in B, x\,(s\otimes 1-1\otimes s)=0$$

$$\Leftrightarrow$$

$$\begin{array}{rcl} \forall s \in B, \sum_k s\, a_k \otimes b_k & = & \sum_k a_k \otimes s\, b_k \\ & \Leftrightarrow & \\ \forall s \in B, \forall \lambda \in \hat{B}, \sum_k \lambda(b_k) s\, a_k & = & \sum_k \lambda(s\, b_k) a_k \quad = \quad \sum_k (s \cdot \lambda(b_k))\ a_k \\ & \Leftrightarrow & \\ \forall s \in B, \forall \lambda \in \hat{B},\ s\,(x^{\triangleright}(\lambda)) & = & x^{\triangleright}(s \cdot \lambda) \quad \Leftrightarrow\ x^{\triangleright} \in Hom_B(\hat{B}, B). \end{array}$$

Ceci montre, d'une part, que tout élément de $Ann_{B\otimes B}(\mathcal{D})$ a pour image par $\triangleright$, un élément de $Hom_B(\hat{B}, B)$; et d'autre part, que pour tout élément X de $Hom_B(\hat{B}, B)$, il existe un unique $x \in Ann_{B\otimes B}(\mathcal{D})$ tel que $X = x^{\triangleright}$. □

3.2 Caractérisation des algèbres Gorenstein

Cette section regroupe des résultats que l'on peut trouver dans [19] et [29]. Nous en donnons ici des preuves simplifiées dans le cas où l'algèbre B est de **dimension finie d sur $\mathbb{K}$**.

Théorème 3.2.1 — *Les assertions suivantes sont équivalentes*

1. $Hom_B(\hat{B}, B)$ *est un B-module libre de rang 1.*
2. *Il existe un B-isomorphisme de $\hat{B}$ sur B.*
3. $\hat{B}$ *est un B-module libre de rang 1.*
4. *Il existe une forme linéaire τ sur B telle que la forme bilinéaire $(a, b) \mapsto \tau(a\, b)$ soit non-dégénérée.*
5. *Il existe un élément $\Delta \in Ann_{B\otimes B}(\mathcal{D})$ tel que $\Delta = \sum_{i=1}^{d} a_i \otimes b_i$, où les familles (a_i) et (b_i) sont des bases de B.*

Dans ce cas, on dit que B est une algèbre Gorenstein. La forme linéaire τ est appelée résidu de B.

(1) ⇒ (2): *Soit (Δ) une base du B-module $Hom_B(\hat{B}, B)$ libre de rang 1; montrons que Δ est un B-isomorphisme entre $\hat{B}$ et B.*

Preuve. L'algèbre B est engendrée par un nombre fini d'éléments $\theta_1, \ldots, \theta_d$. Comme Δ est B-linéaire, $L = Im(\Delta)$ est un idéal de B; donc L en tant que sous espace vectoriel de B est stable par multiplication par les θ_i. Il admet alors un supplémentaire

L', lui aussi stable par multiplication par les θ_i (ces opérateurs de multiplication commutent). Soit p un élément quelconque de L'; pour tout élément $l \in L$, on a $p\,l \in L \cap L' = \{0\}$. Ceci montre que $p\Delta = 0$, donc $p = 0$ (car (Δ) est libre). Ainsi $L' = \{0\}$ et $L = Im(\Delta) = B$. L'application B-linéaire Δ est surjective, et c'est aussi un élément de $Hom_{\mathbb{K}}(\hat{B}, B)$, donc elle est bijective. □

(2) ⇒ (3): *Soit Δ un B-isomorphisme entre $\hat{B}$ et B; montrons que $\hat{B}$ est un B-module libre de rang 1 et de base $\tau = \Delta^{-1}(1)$.*

Preuve. Soient τ l'élément de $\hat{B}$ tel que $\Delta(\tau) = 1$ et $\lambda \in \hat{B}$. Posons $b = \Delta(\lambda)$; puisque $\Delta(\lambda - b \cdot \tau) = 0$ et Δ est B-isomorphisme, $\lambda = b \cdot \tau$, donc τ engendre le B-module $\hat{B}$.

D'autre part, soit $b \in B$ tel que $b \cdot \tau = 0$. L'application Δ est B-linéaire, donc $b = \Delta(b \cdot \tau) = 0$; alors le B-module $\hat{B} = \tau\, B$ est libre. □

(3) ⇒ (4): *Soit (τ) une base du B-module $\hat{B}$; alors la forme bilinéaire définie par $\langle a, b\rangle = \tau(a\,b)$ est non-dégénérée.*

Preuve. Supposons qu'il existe $b \in B$ tel que $0 = \langle x, b\rangle = \tau(x\,b) = (b \cdot \tau)(x)$, pour tout $x \in B$; alors $b = 0$ car (τ) est libre. □

(4) ⇒ (5): *Soit $\tau \in \hat{B}$ tel que la forme bilinéaire qui lui est associée soit non-dégénérée. Construisons $\Delta = \sum_{i=1}^{d} a_i \otimes b_i \in Ann_{B\otimes B}(\mathcal{D})$, où (a_i) et (b_i) sont des bases de B.*

Preuve. Soit (a_i) une base de B et (b_i) sa base duale pour le produit scalaire non-dégénéré défini par τ. Alors $\langle a_i, b_j\rangle = \tau(a_i b_j) = \delta_{i,j}$, et $b = \sum_{i=1}^{d} \tau(a_i b) b_i = \sum_{i=1}^{d} \tau(b_i\, b)\, a_i, \forall b \in B$. Posons

$$\Delta = \sum_{i=1}^{d} a_i \otimes b_i.$$

Si $b \in B$, $b\,a_i = \sum_{j=1}^{d} \tau(b\,a_i\,b_j) a_j$,

$$(b \otimes 1)\,\Delta \quad = \quad \sum_{i=1}^{d} b\,a_i \otimes b_i = \sum_{i=1}^{d}\sum_{j=1}^{d} \tau(b\,a_i\,b_j)\,a_j \otimes b_i$$

$$= \sum_{j=1}^{d} a_j \otimes \sum_{i=1}^{d} \tau(b\, b_j\, a_i)\, b_i$$
$$= \sum_{j=1}^{d} a_j \otimes b\, b_j = \Delta\,(1 \otimes b),$$

alors $\Delta \in Ann_{B\otimes B}(\mathcal{D})$. □

(5) ⇒ (2): *On vérifie immédiatement que $\Delta^{\triangleright}$ définit un B-isomorphisme entre $\hat{B}$ et B.*

Preuve. D'après le théorème (3.1.1), $\Delta^{\triangleright} \in Hom_B(\hat{B}, B)$. Il est clair que l'image de $\Delta^{\triangleright}$ est engendrée par la famille (a_i). Par conséquent, l'application $\mathbb{K}$-linéaire $\Delta^{\triangleright}$ est surjective et donc bijective pour des raisons de dimension. □

(2) ⇒ (1): *Soit Δ un B-isomorphisme entre $\hat{B}$ et B. Alors (Δ) est une base du B-module $Hom_B(\hat{B}, B)$.*

Preuve. Soient $\tau \in \hat{B}$ tel que $\Delta(\tau) = 1$ et T un élément de $Hom_B(\hat{B}, B)$. Posons $t = T(\tau)$; comme $\hat{B} = B \cdot \tau$ (d'après **(2) ⇒ (3)**), $T = t\,\Delta$. Alors le B-isomorphisme Δ engendre $Hom_B(\hat{B}, B)$. Par ailleurs, s'il existe un élément $b \in B$ tel que $b\,\Delta = 0$, alors $\Delta(b \cdot \tau) = b\Delta(\tau) = b = 0$; ainsi (Δ) est libre. □

3.2.1 Exemple d'algèbre Gorenstein

Plaçons-nous dans $R = \mathbb{K}[x_1, x_2, x_3]$; notons $\partial^{\mathbf{0}}$ la forme linéaire sur R telle que $\partial^{\mathbf{0}}(p) = p(0)$ et $\partial_i, 1 \le i \le 3$, l'élément de $\hat{R}$ défini par $\partial_i(p) = d_{x_i}(p)(0)$, où d_{x_i} désigne la dérivée partielle par rapport à x_i. Soit

$$\tau = \partial_1^2 + \partial_2^2 + \partial_3^2 \in \hat{R}$$

On vérifie que

$$x_1 \cdot \tau = 2\partial_1 \quad , \quad x_2 \cdot \tau = 2\partial_2 \quad , \quad x_3 \cdot \tau = 2\partial_3 \quad , \quad x_1^2 \cdot \tau = x_2^2 \cdot \tau = x_3^2 \cdot \tau = 2\,\partial^{\mathbf{0}}.$$

Les polynômes orthogonaux à ces formes linéaires sont dans l'idéal I engendré par

$$x_1^2 - x_2^2,\ x_1^2 - x_3^2,\ x_1\,x_2, x_1\,x_3,\ x_2\,x_3.$$

L'algèbre $B = R/I$ est Gorenstein, car la forme bilinéaire associée à τ (vu comme élément de $\hat{B}$) est non-dégénérée. C'est un exemple d'algèbre Gorenstein non intersection complète. Nous verrons plus loin que toute algèbre intersection complète est Gorenstein. Cet exemple se trouve dans [22].

On peut construire autant d'exemples d'algèbres Gorenstein que l'on veut par cette méthode. Il suffit de partir d'un polynôme τ en $\partial_1, \ldots, \partial_n$, de calculer toutes ses dérivées et de construire l'idéal orthogonal à ces éléments. L'algèbre quotient ainsi obtenue est Gorenstein.

3.2.2 Exemple d'algèbre non Gorenstein

Soient I l'idéal de $\mathbb{K}[x_1, x_2]$ engendré par $x_1^2, x_1\,x_2, x_2^2$, et B la $\mathbb{K}$-algèbre quotient $\mathbb{K}[x_1, x_2]/I$. La famille $(1, x_1, x_2)$ forme une base de B et $(\partial^{\mathbf{0}}, \partial_1, \partial_2)$ (la base duale de $(1, x_1, x_2)$) une base de $\hat{B}$. Soit τ un élément quelconque de $\hat{B}$; le sous espace vectoriel $B{\cdot}\tau$ de $\hat{B}$ est engendré par la famille $(\tau, \partial^{\mathbf{0}})$ (car $x_1{\cdot}\tau = x_2{\cdot}\tau = \partial^{\mathbf{0}}$). Comme $B{\cdot}\tau \neq \hat{B}$, l'algèbre B n'est pas Gorenstein. Par contre, elle est Cohen-Macaulay.

3.3 Formule de représentation dans B

Le produit scalaire défini dans le théorème 3.2.1 par $\langle a|b\rangle = \tau(a\,b)$, vérifie

- $\langle a|b\rangle = (a.\tau)(b) = \left((\Delta^{\triangleright})^{-1}(a)\right)(b)$,
- $\langle a|b\,c\rangle = \langle a\,b|c\rangle$

Proposition 3.3.1 — *Soit $\sum_{i=1}^{d'} a_i \otimes b_i$ une décomposition de Δ dans $B \otimes B$, avec la famille (a_i) libre sur $\mathbb{K}$. Alors $d' = d$, (a_i) et (b_i) sont deux bases de B duales pour le produit scalaire défini par τ.*

Preuve. Soit $(b_i)_{1\leq i\leq d"}$ (après avoir réordonner les b_i) la plus grande famille libre que l'on peut extraire de $(b_i)_{1\leq i\leq d'}$. Il existe alors pour tout $i, d" < i \leq d'$, des scalaires non tous nuls $\alpha_{ij} \in \mathbb{K}$ tels que $b_i = \sum_{j=1}^{d"} \alpha_{ij} b_j$. On a

$$\Delta = \sum_{j=1}^{d"} (a_j + \sum_{i=d"+1}^{d'} \alpha_{ij} a_i) \otimes b_j = \sum_{j=1}^{d"} a'_j \otimes b_j.$$

La famille $(a'_j)_{1\leq j\leq d"}$ est libre. Il est clair qu'elle engendre l'espace vectoriel B, donc c'est une base. Par conséquent, $d" = d = d'$ et (b_j) est une base de B.

Notons $(\hat{b}_i)$ la base duale de (b_i) dans $\hat{B}$. On a donc $\Delta^\triangleright(\hat{b}_j) = \sum_i \hat{b}_j(b_i)a_i = a_j$. Par conséquent, $\langle b_i|a_j\rangle = ((\Delta^\triangleright)^{-1}(a_j))(b_i) = \hat{b}_j(b_i) = \delta_{i,j}$; ce qui montre que la base duale de (a_i) pour $\langle\,|\,\rangle$ est bien (b_i). □

Ceci conduit naturellement à des *formules d'interpolation* ou *formules de traces* ou encore

Formule de Cauchy:

$$\forall\, b \in B\,,\, b = \sum_{i=1}^{d} \langle b|b_i\rangle\, a_i = \sum_{i=1}^{d} \langle b|a_i\rangle\, b_i. \tag{8}$$

On en déduit immédiatement le résultat suivant, qui dit que la forme bilinéaire associée au résidu τ de B est non-dégénérée.

Formule de Dualité:

$$\forall\, b \in B\,,\, b = 0 \text{ dans } B \Leftrightarrow \forall a \in B, \tau(a\,b) = \langle b|a\rangle = 0. \tag{9}$$

Forme quadratique associée à τ :

De la représentation $b_j = \sum_{i=1}^{d} \langle b_j|b_i\rangle\, a_i$, on déduit

$$\Delta = \sum_{1\le i,j\le d} \langle b_i|b_j\rangle a_i \otimes a_j.$$

En choisissant la même base $\mathbf{e}$ pour chaque facteur de $B \otimes B$, on obtient une matrice symétrique conjuguée de $(\langle b_i|b_j\rangle)_{i,j}$ dont la signature est un invariant de B si le corps $\mathbb{K}$ est ordonné. Voir par exemple [2].

3.4 Annulateur et orthogonal

Proposition 3.4.1 — *Soit J un idéal de B. Alors l'orthogonal de J pour le produit scalaire $\langle\,|\,\rangle$ défini par τ est $Ann_B(J)$.*

Preuve. Soit a un élément de $Ann_B(J)$. Comme $\langle\,|\,\rangle$ est non-dégénéré, $\forall\, h \in J$, $a\,h = 0$, si et seulement si, $\forall\, h \in J$, $\forall\, b \in B$, $\langle a\,h|b\rangle = \langle a|h\,b\rangle = 0$. Ce qui est équivalent à $\forall\, h' \in J$, $\langle a|h'\rangle = 0$, c.à.d. a est orthogonal à J pour $\langle\,|\,\rangle$. □

3.5 Le théorème de Wiebe

Cette section s'inspire de l'article [29]. Il relie un idéal engendré par une suite quasi-régulière et son image par une matrice à l'annulateur du déterminant de celle-ci.

Soient $\mathcal{A}$ un anneau intègre, $f_1, \ldots, f_n$ et $g_1, \ldots, g_n$ des éléments de $\mathcal{A}$ tels que

$$\forall i = 1, \ldots, n, \quad g_i = \sum_{j=1}^{n} a_{i,j} f_j \ , \ a_{i,j} \in \mathcal{A}.$$

Supposons que $(f_1, \ldots, f_n)$ et $(g_1, \ldots, g_n)$ soient des suites quasi-régulières de $\mathcal{A}$. Notons $\Delta = \det(a_{i,j}), \mathcal{G}$ (resp. $\mathcal{F}$) l'idéal de $\mathcal{A}$ engendré par $g_1, \ldots, g_n$ (resp. $f_1, \ldots, f_n$) et $\mathcal{B} = \mathcal{A}/\mathcal{G}$.

Théorème 3.5.1 (Wiebe)

1. *La classe de Δ dans $\mathcal{B}$ est indépendante du choix des coefficients $a_{i,j}$.*
2. *$Ann_{\mathcal{B}}(\Delta\, \mathcal{B}) = \mathcal{F}\, \mathcal{B}$.*
3. *$Ann_{\mathcal{B}}(\mathcal{F}\, \mathcal{B}) = \Delta\, \mathcal{B}$.*

Preuve. On peut supposer que l'anneau $\mathcal{A}$ est local, sinon on localise $\mathcal{A}$ par un idéal maximal contenant $\mathcal{G}$.

1. Soit $g_i = \sum_j b_{i,j} f_j, 1 \leq i \leq n$, une autre décomposition. On va montrer que $\det(a_{i,j}) = \det(b_{i,j})$ dans $\mathcal{B}$. Pour cela, on va le montrer pour la décomposition intermédiaire

$$g_i = \sum_{j=1}^{n} a_{i,j} f_j \ , \ i \neq i_0 \ , \ g_{i_0} = \sum_{j=1}^{n} b_{i_0,j} f_j \ ,$$

où i_0 est un entier quelconque compris entre 1 et n. Le cas général suivra de proche en proche en changeant à chaque fois la forme d'un g_i. Comme

$$\sum_{j=1}^{n} a_{i,j} f_j = g_i \ , \quad i \neq i_0 \ , \quad \sum_{j=1}^{n} (a_{i_0,j} - b_{i_0,j}) f_j = 0 \ ,$$

la règle de Cramer fournit $f_j(\det(a_{i,j}) - \det(b_{i,j})) \in (g_1, \ldots, g_{i_0-1}, g_{i_0+1}, \ldots, g_n), 1 \leq j \leq n$ (Signalons que la matrice $(b_{i,j})$ a les mêmes lignes que $(a_{i,j})$ sauf la $i_0^{\text{ième}}$). En particulier $g_{i_0}(\det(a_{i,j}) - \det(b_{i,j})) \in (g_1, \ldots, g_{i_0-1}, g_{i_0+1}, \ldots, g_n)$. Puisque g_{i_0} est non-diviseur de zéro dans $\mathcal{A}/(g_1, \ldots, g_{i_0-1}, g_{i_0+1}, \ldots, g_n)$,

$$\det(a_{i,j}) - \det(b_{i,j}) \in (g_1, \ldots, g_{i_0-1}, g_{i_0+1}, \ldots, g_n).$$

Pour les points *2* et *3* la démonstration se fera par récurrence sur n. Pour $n = 1$, les deux propriétés sont immédiates. Soit n un entier ≥ 2.

Posons $\mathcal{A}' = \mathcal{A}/(f_1)$, $\mathcal{F}' = (f_2, \ldots, f_n)$, $\mathcal{G}' = (g_2, \ldots, g_n)$, $C = \mathcal{A}/\mathcal{G}'$ et $\mathcal{B}' = \mathcal{A}'/\mathcal{G}'\,\mathcal{A}' = C/f_1\,C = \mathcal{A}/(f_1, g_2, \ldots, g_n)$. On a donc $g_i \equiv \sum_{j\geq 2} a_{i,j} f_j$ dans $\mathcal{A}'$; posons $\Delta' = \det(a_{i,j})_{2\leq i,j\leq n}$. Par hypothèse, il existe un élément de la forme $f_1 + \sum_{i\geq 2} \lambda_i f_i$ qui est non-diviseur de zéro dans C. Sinon , tous les f_i sont des diviseurs de zéro dans C et g_1 aussi. Ce qui contredit l'hypothèse. Quitte à remplacer f_1 par $f_1 + \sum_{i\geq 2} \lambda_i f_i$, on peut supposer que f_1 est non-diviseur de zéro dans $\mathcal{A}/(g_2, \ldots, g_n)$. Comme l'ordre n'a pas d'importance dans un anneau local, $(f_1, g_2, \ldots, g_n)$ est une suite régulière de $\mathcal{A}$.

D'après la règle de Cramer,

$$\Delta\, f_1 = \Delta_{1,1} g_1 + \cdots + \Delta_{n,1}\, g_n$$

où $\Delta_{i,1}$ est le cofacteur de $a_{i,1}$. Alors

$$\Delta\, f_1 = \Delta'\, g_1 \quad , \text{ dans } C \ ,$$

avec $\Delta' = \Delta_{1,1}$, et par conséquent, le diagramme suivant est commutatif,

$$\begin{array}{ccccc}
 & ? & & 0 & \\
 & \downarrow & & \downarrow & \supset Ann_{C/(f_1)}(\mathcal{F}) \\
0 \rightarrow & \mathcal{A}/\mathcal{F} & \xrightarrow{\mu_{\Delta'}} & \mathcal{A}/(f_1, g_2, \ldots, g_n) & \\
 & \downarrow{\scriptstyle \mu_\Delta} & & \downarrow{\scriptstyle \mu_{g_1}} & \\
0 \rightarrow & \mathcal{A}/\mathcal{G} & \xrightarrow{\mu_{f_1}} & \mathcal{A}/(f_1 g_1, g_2, \ldots, g_n) & \\
 & \supset Ann_{C/(g_1)}(\mathcal{F}) & & &
\end{array}$$

μ_a désigne la multiplication par a.

2. L'inclusion $\mathcal{F}\mathcal{B} \subset Ann_{\mathcal{B}}(\Delta\mathcal{B})$ est évidente et provient de $f_i\Delta \subset \mathcal{G}, 1 \leq i \leq n$. Montrons l'inclusion inverse.

D'après l'hypothèse de récurrence, $Ann_{\mathcal{B}'}(\Delta'\mathcal{B}') = \mathcal{F}'\,\mathcal{B}'$; donc l'application $\mu_{\Delta'}$ est injective. Les morphismes μ_{f_1} et μ_{g_1} sont injectifs car f_1 et g_1 sont non-diviseurs de zéro dans C. S'il existe un élément m de $\mathcal{A}/\mathcal{F}$ tel que $\mu_\Delta(m) = 0$, alors $m = 0$ (chasse au diagramme). Ce qui montre que μ_Δ est injective. Soit $f \in \mathcal{A}$, tel que $\Delta f = 0$ dans $\mathcal{B}$; d'après ce qui précéde $f \in \mathcal{F}$ et $Ann_{\mathcal{B}}(\Delta\mathcal{B}) \subset \mathcal{F}\mathcal{B}$.

3. L'inclusion $\Delta\mathcal{B} \subset Ann_{\mathcal{B}}(\mathcal{F}\mathcal{B})$ provient aussi de $f_i\Delta \subset \mathcal{G}, 1 \leq i \leq n$. D'après l'hypothèse de récurrence l'image de $\mu_{\Delta'}$ est $Ann_{C/(f_1)}(\mathcal{F})$. Montrons que

$$\mu_{f_1}(Ann_{C/(g_1)}(\mathcal{F})) = \mu_{g_1}(Ann_{C/(f_1)}(\mathcal{F})).$$

Soit $m \in Ann_{C/(g_1)}(\mathcal{F})$; pour tout f dans $\mathcal{F}$, il existe m' dans C tel que $m\,f = g_1 m'$. En particulier, $m\,f_1 = g_1 m''$, avec $m'' \in C$. Donc

$$g_1 f_1 m' = m\,f_1\,f = g_1 m'' f.$$

Comme g_1 est non-diviseur de zéro dans C, $m''f = f_1 m'$, et m'' est dans $Ann_{C/(f_1)}(\mathcal{F})$, alors $m\,f_1$ est dans $\mu_{g_1}(Ann_{C/(f_1)}(\mathcal{F}))$. Réciproquement, soit $m \in Ann_{C/(f_1)}(\mathcal{F})$. Pour tout f dans $\mathcal{F}$, il existe m' dans C tel que $m\,f = f_1 m'$. En particulier, $m\,g_1 = f_1 m'', m'' \in C$. De la même façon, comme f_1 n'est pas un diviseur de zéro dans C, m'' est dans $Ann_{C/(g_1)}(\mathcal{F})$ et $m\,g_1$ est dans $\mu_{f_1}(\,Ann_{C/(g_1)}(\mathcal{F}))$.

D'après l'hypothèse de récurrence, $Im(\mu_{\Delta'}) = Ann_{C/(f_1)}(\mathcal{F})$, donc l'image de μ_Δ (qui n'est autre que $\Delta\mathcal{B}$) est bien $Ann_{C/(g_1)}(\mathcal{F}) = Ann_{\mathcal{B}}(\mathcal{F})$. □

4 Intersection complète de dimension 0

4.1 Notations

Nous notons $(\mathbf{P})$ l'idéal de R engendré par les n polynômes $P_1, \ldots, P_n, d_i = \deg P_i, 1 \leq i \leq n, \mathbf{d}$ le n-uplet $(d_1, \ldots, d_n)$, B l'algèbre quotient $R/(\mathbf{P})$, $R \otimes R = \mathbb{K}[\mathbf{x}, \mathbf{y}]$ et $B \otimes B = R \otimes R/(\mathbf{P}(\mathbf{x}), \mathbf{P}(\mathbf{y}))$.

A chaque forme linéaire sur B correspond de façon naturelle une seule forme linéaire sur R s'annulant sur $(\mathbf{P})$, donc $\hat{B}$ s'injecte dans $\hat{R}$.

Etant donnés $\mathbf{x} = (x_1, \ldots, x_n)$ et $\mathbf{y} = (y_1, \ldots, y_n)$, on note

$$X_{(0)} = (x_1, \ldots, x_n), X_{(1)} = (y_1, x_2, \ldots, x_n), \ldots, X_{(n)} = (y_1, \ldots, y_n).$$

Pour tout polynôme $f \in R$,

$$\theta_j(f) = \frac{f(X_{(j)}) - f(X_{(j-1)})}{y_j - x_j} \quad , \quad 1 \leq j \leq n \quad , \qquad df = f(\mathbf{y}) - f(\mathbf{x}).$$

On désigne par Δ (ou encore) $\Delta_{\mathbf{P}}$ l'élément de $R \otimes R$ défini par,

$$\Delta_{\mathbf{P}} = \det(\theta_j(P_i))_{1 \leq i,j \leq n}.$$

On remarque que $\Delta_{\mathbf{P}}(\mathbf{x}, \mathbf{x}) = J_{\mathbf{P}}(\mathbf{x})$, où $J_{\mathbf{P}}(\mathbf{x})$ désigne le jacobien de l'application $\mathbf{P}$. On notera également $dx_i = y_i - x_i, 1 \leq i \leq n$, $\mathbf{dx} = (dx_1, \ldots, dx_n)$ et $\mathbf{dP} = (dP_1, \ldots, dP_n)$.

4.2 Les Bézoutiens

4.2.1 Une construction des Bézoutiens

Considérons l'application polynomiale

$$\begin{aligned} \mathbf{P} : \mathbb{K}^n &\to \mathbb{K}^n \\ \mathbf{x} &\mapsto \mathbf{P}(\mathbf{x}) = (P_1(\mathbf{x}), \ldots, P_n(\mathbf{x})) \ , \end{aligned}$$

et soient $X_{(0)}, \ldots, X_{(n)}$, $n+1$ points de $\mathbb{K}^n$ (par exemple ceux définis dans 4.1 à partir de $\mathbf{x}$ et $\mathbf{y}$). Nous allons construire un nouveau point χ de la façon suivante: on exprime le point origine O de $\mathbb{K}^n$ comme barycentre des points $\mathbf{P}(X_{(0)}), \ldots \mathbf{P}(X_{(n)})$,

$$\left\{ \begin{array}{l} t_0 P_1(X_{(0)}) + \cdots + t_n P_1(X_{(n)}) = 0 \\ \vdots \\ t_0 P_n(X_{(0)}) + \cdots + t_n P_n(X_{(n)}) = 0 \\ t_0 + \cdots + t_n = 1 \end{array} \right. \tag{10}$$

En utilisant la règle de Cramer, on voit que

$$\left\{ \begin{array}{lll} t_0 = & & \frac{|\mathbf{P}(X_{(1)}), \mathbf{P}(X_{(2)}), \ldots, \mathbf{P}(X_{(n)})|}{D} \\ t_1 = & - & \frac{|\mathbf{P}(X_{(0)}), \mathbf{P}(X_{(2)}), \ldots, \mathbf{P}(X_{(n)})|}{D} \\ \vdots & & \\ t_n = & (-1)^n & \frac{|\mathbf{P}(X_{(0)}), \mathbf{P}(X_{(1)}) \ldots, \mathbf{P}(X_{(n-1)})|}{D} \end{array} \right.$$

où,

$$D = \Delta \left(\prod_{i=1}^{n} (y_i - x_i) \right).$$

Le nouveau point est

$$\chi = t_0 \, X_{(0)} + \cdots + t_n \, X_{(n)}.$$

En itérant cette construction (i.e. associer à $\mathbf{x}$ et χ un autre point de la même façon, et ainsi de suite), on obtient une méthode des sécantes à plusieurs variables (voir [31] ou [25][p. 189, 193, 200]). Ce procédé converge quand les points $\mathbf{x}$ et $\mathbf{y}$ sont suffisamment proches d'une racine.

Nous pouvons étendre cette construction. En effet, au lieu de reporter le barycentre sur les points $X_{(0)}, \ldots, X_{(n)}$, nous allons le faire sur les valeurs d'un polynôme

$Q(X)$, ce qui conduit à des fractions rationnelles en $2n$ variables de la forme

$$t_0\,Q(X_{(0)}) + \cdots + t_n\,Q(X_{(n)}) = \frac{\begin{vmatrix} Q(X_{(0)}) & \cdots & Q(X_{(n)}) \\ P_1(X_{(0)}) & \cdots & P_1(X_{(n)}) \\ & \vdots & \\ P_n(X_{(0)}) & \cdots & P_n(X_{(n)}) \end{vmatrix}}{D}.$$

Cette égalité s'obtient en développant le déterminant par rapport à la première ligne.

Définition 4.2.1 — *Le Bézoutien de $n+1$ polynômes $Q, P_1, \ldots, P_n$ de R est le polynôme $\Phi(Q, P_1, \ldots, P_n)$ de $R \otimes R$ défini par,*

$$\Phi(Q, P_1, \ldots, P_n) = \frac{\begin{vmatrix} Q(X_{(0)}) & \cdots & Q(X_{(n)}) \\ P_1(X_{(0)}) & \cdots & P_1(X_{(n)}) \\ & \vdots & \\ P_n(X_{(0)}) & \cdots & P_n(X_{(n)}) \end{vmatrix}}{\prod_{i=1}^{n}(y_i - x_i)}.$$

On voit facilement que le Bézoutien est un polynôme de $\mathbb{K}[\mathbf{x}, \mathbf{y}]$ (car si $x_i = y_i, X_{(i-1)} = X_{(i)}, 1 \leq i \leq n$, et le déterminant est nul). Si les polynômes $P_1, \ldots, P_n$ sont donnés implicitement, nous noterons $\Phi(Q, P_1, \ldots, P_n)$ par $\Phi(Q)$. Remarquons que $\Delta = \Phi(1)$.

La méthode des sécantes consiste donc à prendre comme nouveau point le barycentre des points $X_{(0)}, \ldots, X_{(n)}$ affectés des coefficients $t_0, \ldots, t_n$, c'est-à-dire le point

$$\chi = \left(\frac{\Phi(x_1)}{\Phi(1)}, \ldots, \frac{\Phi(x_n)}{\Phi(1)}\right) ,$$

ou de manière projective $(\Phi(1) : \Phi(x_1) : \cdots : \Phi(x_n))$.

4.2.2 Une autre formulation des Bézoutiens

On vérifie facilement que pour tout polynôme f,

$$f(X_{(i)}) = f(X_{(0)}) + \theta_1(f)\,dx_1 + \cdots + \theta_i(f)\,dx_i \ , \ 1 \leq i \leq n.$$

Il en résulte que,

$$\begin{aligned} &\Phi(P_0, \ldots, P_n) && (11)\\ &= \frac{|\tilde{\mathbf{P}}(X_{(0)}), \tilde{\mathbf{P}}(X_{(0)}) + \theta_1(\tilde{\mathbf{P}})\,dx_1, \ldots, \tilde{\mathbf{P}}(X_{(0)}) + \theta_1(\tilde{\mathbf{P}})\,dx_1 + \cdots + \theta_n(\tilde{\mathbf{P}})\,dx_n|}{\prod_{i=1}^{n} dx_i} \\ &= |\tilde{\mathbf{P}}(X_{(0)}), \theta_1(\tilde{\mathbf{P}}), \ldots, \theta_n(\tilde{\mathbf{P}})| && (12) \end{aligned}$$

où $\tilde{\mathbf{P}}(X_{(0)}) = (P_0(X_{(0)}), \ldots, P_n(X_{(0)})$, et $\theta_i(\tilde{\mathbf{P}})\, dx_i = (\theta_i(P_0)dx_i, \ldots, \theta_i(P_n)dx_i), 1 \leq i \leq n$. En utilisant cette fois-ci la formule,

$$f(X_{(i)}) = \theta_{i+1}(f)(-dx_{i+1}) + \ldots + \theta_n(f)(-dx_n) + f(X_{(n)}) \ , \ 0 \leq i \leq n-1 \ ,$$

on obtient

$$\Phi(P_0, \ldots, P_n) = |\tilde{\mathbf{P}}(X_{(n)}), \theta_1(\tilde{\mathbf{P}}), \ldots, \theta_n(\tilde{\mathbf{P}})|. \tag{13}$$

4.2.3 Quelques propriétés de Φ

$*$ Calcul de Φ par linéarité

L'application Φ étant linéaire sur $\mathbb{K}$, il suffit de la définir sur les monômes.

Proposition 4.2.2 — *Soit* $\mathbf{x^u} = x_1^{u_1} \cdots x_n^{u_n}$ *un monôme de* $\mathbb{K}[\mathbf{x}]$, *alors*

$$\Phi(\mathbf{x^u}) = \frac{\left|x_1^{u_1}\mathbf{P}(X_{(1)}) - y_1^{u_1}\mathbf{P}(X_{(0)}), \cdots, x_n^{u_n}\mathbf{P}(X_{(n)}) - y_n^{u_n}\mathbf{P}(X_{(n-1)})\right|}{\prod_{i=1}^n (y_i - x_i)}.$$

Preuve. Notons $m(X_{(i)}) = y_1^{u_1} \cdots y_i^{u_i} x_{i+1}^{u_{i+1}} \cdots x_n^{u_n}, 0 \leq i \leq n$. Nous avons

$$\begin{vmatrix} m(X_{(0)}) & \cdots & m(X_{(n)}) \\ \mathbf{P}(X_{(0)}) & \cdots & \mathbf{P}(X_{(n)}) \end{vmatrix} = \prod_{i=0}^{n} m(X_{(i)}) \begin{vmatrix} 1 & \cdots & 1 \\ \mathbf{P}(X_{(0)})/m(X_{(0)}) & \cdots & \mathbf{P}(X_{(n)})/m(X_{(n)}) \end{vmatrix}.$$

En soustrayant la i$^{\text{ième}}$ colonne de la (i+1)$^{\text{ième}}$, $0 \leq i \leq n-1$, on obtient

$$\overbrace{x_1^{u_1} \cdots x_n^{u_n}}^{m(X_{(0)})} \overbrace{y_1^{u_1}\, x_2^{u_2} \cdots x_n^{u_n}}^{m(X_{(1)})} \cdots \overbrace{y_1^{u_1} \cdots y_n^{u_n}}^{m(X_{(n)})}$$
$$\left|\mathbf{P}(X_{(1)})/m(X_{(1)}) - \mathbf{P}(X_{(0)})/m(X_{(0)}), \ldots, \mathbf{P}(X_{(n)})/m(X_{(n)}) - \mathbf{P}(X_{(n-1)})/m(X_{(n-1)})\right|.$$

En réduisant au même dénominateur la première colonne, on trouve

$$x_2^{u_2} \cdots x_n^{u_n} \cdots y_1^{u_1} \cdots y_n^{u_n}$$
$$\left| \ x_1^{u_1}\mathbf{P}(X_{(1)}) - y_1^{u_1}\mathbf{P}(X_{(0)}), \ldots, \mathbf{P}(X_{(n)})/m(X_{(n)}) - \mathbf{P}(X_{(n-1)})/m(X_{(n-1)}) \ \right|,$$

et en itérant,

$$\left|x_1^{u_1}\mathbf{P}(X_{(1)}) - y_1^{u_1}\mathbf{P}(X_{(0)}), \cdots, x_n^{u_n}\mathbf{P}(X_{(n)}) - y_n^{u_n}\mathbf{P}(X_{(n-1)})\right|.$$

□

$*$ Calcul de Φ modulo l'idéal $(\mathbf{P})$

Proposition 4.2.3 — *Pour toute application polynomiale* $\tilde{\mathbf{P}} = (P_0, \ldots, P_n)$,

$$\Phi(P_0, \ldots, P_n) = P_0\Phi(1, P_1, \ldots, P_n) + P_1\Phi(P_0, 1, P_2, \ldots, P_n) + \cdots + P_n\Phi(P_0, \ldots, P_{n-1}, 1).$$

Preuve. En développant le déterminant (11) par rapport à la première colonne, on obtient

$$\Phi(P_0, \ldots, P_n) = P_0(\mathbf{x})M_0(\theta_1(\tilde{\mathbf{P}}), \ldots, \theta_n(\tilde{\mathbf{P}})) - \cdots + (-1)^n P_n(\mathbf{x})M_n(\theta_1(\tilde{\mathbf{P}}), \ldots, \theta_n(\tilde{\mathbf{P}}))$$

où $\theta_i(\tilde{\mathbf{P}}) = (\theta_i(P_0), \ldots, \theta_i(P_n))$ et M_i est le mineur de la matrice $(\theta_1(\tilde{\mathbf{P}}), \ldots, \theta_n(\tilde{\mathbf{P}}))$ sans la $(i+1)^{\text{ième}}$ ligne. Ce mineur s'obtient en prenant $P_i = 1$ dans la formule précédente. Par suite,

$$\Phi(P_0, \ldots, P_n) = P_0\Phi(1, P_1, \ldots, P_n) + P_1\Phi(P_0, 1, P_2, \ldots, P_n) + \cdots + P_n\Phi(P_0, \ldots, P_{n-1}, 1).$$

□

On en déduit immédiatement le résultat suivant

Corollaire 4.2.4 — *Pour tout* $Q \in \mathbb{K}[\mathbf{x}]$, $\Phi(Q) \equiv Q(\mathbf{x})\,\Phi(1)$ *dans* $\mathbb{K}[\mathbf{x}, \mathbf{y}]/(\mathbf{P}(\mathbf{x}))$.

Ceci était prévisible; en effet, en faisant des calculs modulo l'idéal $(\mathbf{P}(\mathbf{x}))$, on voit que la solution $(t_0, \ldots, t_n)$ du système (10) est $(1, 0, \ldots, 0)$, et donc $\Phi(Q) \equiv Q(\mathbf{x})\Phi(1)$. Ceci revient encore à dire que si le point $\mathbf{x}$ est une solution du système $P_i(\mathbf{x}) = 0, 1 \leq i \leq n$, alors le point χ calculé par la méthode des sécantes est le point de départ $\mathbf{x}$.

Corollaire 4.2.5 — *Pour tout* $Q \in \mathbb{K}[\mathbf{x}], \Phi(Q) \equiv Q(\mathbf{y})\Phi(1)$ *dans* $\mathbb{K}[\mathbf{x}, \mathbf{y}]/\ (\mathbf{P}(\mathbf{y}))$.

Preuve. On calcule $\Phi(Q)$ modulo $(\mathbf{P}(\mathbf{y}))$, après le développement du déterminant (13) par rapport à la dernière colonne. □

4.3 Caractérisation du résidu

Nous supposons que $B = R/(\mathbf{P})$ est un $\mathbb{K}$-espace vectoriel de dimension finie, donc que $\mathbf{P} = (P_1, \ldots, P_n)$ est une suite quasi-régulière.

Posons $\mathcal{A} = R \otimes B$, $f_i = x_i - y_i$, $\mathcal{F}$ l'idéal de $R \otimes R$ engendré par $x_i - y_i, 1 \leq i \leq n$, $g_i = P_i(\mathbf{x}) - P_i(\mathbf{y}) = \sum_j \theta_j(P_i)f_j$ dans $R \otimes R$, et $\Delta = \det(\theta_j(P_i))$. On vérifie facilement que les images des suites $(f_1, \ldots, f_n)$ et $(g_1, \ldots, g_n)$ dans $\mathcal{A} = R \otimes B$ sont quasi-régulières, et que l'idéal $\mathcal{G}$ de $\mathcal{A}$ engendré par $(g_1, \ldots, g_n)$ est égal à $(\mathbf{P}(\mathbf{x}))$; donc $\mathcal{B} = \mathcal{A}/\mathcal{G} = B \otimes B$. En appliquant le théorème de Wiebe (3.5.1), on obtient,

– $Ann_{\mathcal{B}}(\mathcal{F}\mathcal{B}) = \Delta\mathcal{B}$.

– $Ann_{\mathcal{B}}(\Delta\mathcal{B}) = \mathcal{F}\mathcal{B}$.

Ces deux résultats se traduisent de la façon suivante

Corollaire 4.3.1 — *Soit* $T \in R \otimes R = \mathbb{K}[\mathbf{x}, \mathbf{y}]$,

– *Si pour tout élément* $Q(\mathbf{x}) \in R$, $Q(\mathbf{x})T(\mathbf{x}, \mathbf{y}) \equiv Q(\mathbf{y})T(\mathbf{x}, \mathbf{y})$ *dans* $\mathcal{B}$, *alors il existe* $S \in R \otimes R$ *tel que* $T(\mathbf{x}, \mathbf{y}) \equiv \Delta\, S(\mathbf{x}, \mathbf{y})$ *dans* $\mathcal{B}$.

– *Si* $T\Delta \equiv 0$ *dans* $\mathcal{B}$, *alors* $T(\mathbf{x}, \mathbf{x}) \equiv 0$ *dans* B.

Preuve. Le premier point provient de, $Ann_{\mathcal{B}}(\mathcal{F}\,\mathcal{B}) = \{T(\mathbf{x}, \mathbf{y}) \in \mathcal{B} : T\,Q(\mathbf{x}, \mathbf{y}) = 0, \forall Q \in \mathcal{F}\mathcal{B}\} = \Delta\mathcal{B}$, et $\mathcal{F}\mathcal{B}$ est engendré par les polynômes de la forme $Q(\mathbf{x}) - Q(\mathbf{y})$, où $Q \in B$. Le deuxième point découle de $Ann_{\mathcal{B}}(\Delta\mathcal{B}) = \mathcal{F}\mathcal{B}$ ou encore, si $\Delta\, T \equiv 0$ dans B, alors $T \in \mathcal{F}\mathcal{B}$. □

Voir aussi [7] pour une autre approche.

En utilisant les résultats de la section 3.2, on voit que si $(\mathbf{P})$ est une suite quasi-régulière, alors B est Gorenstein, et on a la caractérisation suivante

Théorème et définition 4.3.1 — *Soit* Θ *une matrice vérifiant* $\mathbf{dP} = \Theta\ \mathbf{dx}$ *et* $\Delta_{\mathbf{P}}$ *son déterminant. Le résidu de l'application polynomiale* $\mathbf{P}$ *est l'unique forme linéaire* $\tau_{\mathbf{P}} \in \hat{R}$ *telle que*

– $\tau_{\mathbf{P}} = 0$ sur $(\mathbf{P})$

– $\Delta_{\mathbf{P}} \triangleright \tau_{\mathbf{P}} - 1 \in (\mathbf{P})$.

Le résidu $\tau_{\mathbf{P}}$ est un générateur de $\hat{B}$ en tant que B-module libre de rang 1. L'existence et l'unicité de $\tau_{\mathbf{P}}$ découlent du fait que $\Delta_{\mathbf{P}}^{\triangleright}$ est un B-isomorphisme entre $\hat{B}$ et B.

Nous avons le théorème de dualité qui complète le premier point de la définition précédente.

Théorème 4.3.1 (Théorème de dualité) — *Soit* $\mathbf{P} = (P_1, ..., P_n)$ *une application définissant une suite quasi-régulière et* f *un élément de* $\mathbb{K}[\mathbf{x}]$. *Si* $f \cdot \tau_{\mathbf{P}} = 0$, *alors* f *est dans l'idéal de* $\mathbb{K}[\mathbf{x}]$ *engendré par* $P_1, ..., P_n$.

Preuve. Ce théorème découle de la formule de dualité (9). □

4.3.1 Le résidu dans le cas $n = 1$

Soit $P = a_0x^d + a_1x^{d-1} + ... + a_d$ un polynôme d'une variable à coefficients dans $\mathbb{K}$. Son Bézoutien

$$\Delta = \frac{P(x) - P(y)}{x - y} = \sum_{i=1}^{d} x^{i-1} H_{d-i}(y),$$

où $H_j(y) = a_0y^j + a_1y^{j-1} + ... + a_j, 0 \leq j \leq d-1$, sont les polynômes de Hörner. La famille $(H_{d-1}, \ldots, H_0)$ forme une base du quotient $B = \mathbb{K}[x]/(P)$, duale de la base de monômes $(1, x, ..., x^{d-1})$ pour le produit scalaire défini par τ_P (proposition 3.3.1). D'après la caractérisation du résidu τ_P, pour tout $f \in R, \tau_P(f) = \tau_P(r)$, où r est le reste de la division euclidienne de f par P, et le polynôme

$$\Delta \triangleright \tau_P - 1 = \sum_{i=1}^{d} x^{i-1} \tau_P(H_{d-i}) - 1 = 0 \ ,$$

car $\deg(\Delta \triangleright \tau_P - 1) \leq d-1$ et $\Delta \triangleright \tau_P - 1 \in (P)$. Donc

$$\tau_P(H_{d-1}) = 1 \quad , \quad \tau_P(H_i) = 0 \quad , \quad 0 \leq i \leq d-2 \ .$$

Par conséquent, $\tau_P(f) = \tau_P(r) = \alpha_{d-1}$, avec $r = \alpha_{d-1}H_{d-1} + \ldots + \alpha_0 H_0, \alpha_i \in \mathbb{K}, 0 \leq i \leq d-1$. Il en résulte que

$$\tau_P(f) = \frac{1}{a_0} \text{ coefficient de } x^{d-1} \text{ dans le reste de la division euclidienne de } f \text{ par } P. \tag{14}$$

4.3.2 Le résidu dans le cas où $P_i = x_i^{d_i}, 1 \leq i \leq n$

Dans ce cas, une base $\mathbf{e}$ du quotient B est formée des monômes

$$\prod_{i=1}^{n} x_i^{\alpha_i}; \ 0 \leq \alpha_i < d_i.$$

Donc B est un espace vectoriel sur $\mathbb{K}$ de dimension $\prod_{i=1}^{n} d_i$. Le Bézoutien de $\mathbf{P}$ est

$$\Phi(1) = \prod_{i=1}^{n} \left(x_i^{d_i-1} + x_i^{d_i-2} y_i + \cdots + y_i^{d_i-1} \right) = \sum_{i=1}^{n} \sum_{j_i=1}^{d_i} x_1^{d_1-j_1} ... \ x_n^{d_n-j_n} \ y_1^{j_1-1} ... \ y_n^{j_n-1}.$$

La matrice associée à $\Phi(1)$ est

$$\begin{array}{c} \\ 1 \\ x_1 \\ \vdots \\ \mathbf{x^{d-1}} \end{array} \begin{array}{c} \begin{array}{cccc} 1 & \cdots & \cdots & \mathbf{y^{d-1}} \end{array} \\ \begin{bmatrix} 0 & \dots & 0 & 1 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix} \end{array}.$$

C'est la matrice de $\Phi(1)^\triangleright : \hat{B} \to B$ dans les bases $\mathbf{e}$ de B et $\hat{\mathbf{e}}$ (la base duale de $\mathbf{e}$) de $\hat{B}$. Donc $\tau_{\mathbf{x^d}} = \widehat{x^{d-1}}$ et par suite le résidu, associé à $\mathbf{P} = (x_1^{d_1}, \dots, x_n^{d_n})$, d'un polynôme f est

$$\tau_{\mathbf{x^d}}(f) = \text{coefficient de } \mathbf{x^{d-1}} \text{dans } f \ . \tag{15}$$

C'est la formule habituelle de Cauchy que l'on rencontre en analyse complexe (voir [15]).

4.3.3 Le résidu dans le cas où $P_i = a_{i,0}x_i^{d_i} + a_{i,1}x_i^{d_i-1} + \ldots + a_{i,d_i}, 1 \leq i \leq n$

Dans ce cas, le Bézoutien $\Delta = \Delta_1 \ldots \Delta_n$, où $\Delta_i = \sum_{j=1}^{d_i} x_i^{j-1} H_{i,d_i-j}(y_i), 1 \leq i \leq n$, avec $H_{i,d_i-j}, 0 \leq j \leq d_i - 1$, sont les polynômes de Hörner correspondant au polynôme $P_i \in \mathbb{K}[x_i]$. On vérifie facilement que pour tout monôme $f = \mathbf{x}^\alpha$ de $\mathbb{K}[\mathbf{x}]$,

$$\tau_{\mathbf{P}}(f) = \prod_{i=1}^{n} \tau_{\mathbf{P}_i}(x_i^{\alpha_i}). \tag{16}$$

4.3.4 Le résidu dans le cas où tous les zéros de P sont simples

Nous nous plaçons dans le cas où toutes les racines (l'ensemble de ces racines est noté $V(\mathbf{P})$) du système $\{\mathbf{P} = 0\}$ sont simples (i.e. $J_{\mathbf{P}}(\alpha) \neq 0$, si $\alpha \in V(\mathbf{P})$). Pour tout point $\zeta \in \mathbb{K}^n$, on note ∂_ζ la forme linéaire sur R, consistant à évaluer un polynôme au point ζ.

Proposition 4.3.1 — *Dans le cas où tous les zéros de* $\mathbf{P}$ *sont simples, le résidu de* $\mathbf{P}$ *est*

$$\tau_{\mathbf{P}} = \sum_{\zeta \in V(\mathbf{P})} \frac{\partial_\zeta}{J_{\mathbf{P}}(\zeta)}.$$

Preuve. Soient α et β deux éléments distincts de $V(\mathbf{P})$. Par construction, $\mathbf{P}(\mathbf{x}) - \mathbf{P}(\mathbf{y}) = \mathbf{A}(\mathbf{x},\mathbf{y})\mathbf{dx}$, avec $\det(\mathbf{A}) = \Delta_{\mathbf{P}}$. Par conséquent, $\mathbf{A}(\alpha,\beta)\mathbf{d}\alpha = 0$, avec $\mathbf{d}\alpha = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n) \neq 0$. Donc, $\det(\mathbf{A}(\alpha,\beta)) = \Delta_{\mathbf{P}}(\alpha,\beta) = 0$. D'autre part, si $\alpha \in V(\mathbf{P}), \Delta_{\mathbf{P}}(\alpha,\alpha) = J_{\mathbf{P}}(\alpha) \neq 0$.

La famille $(\partial_\beta)_{\beta\in V(\mathbf{P})}$ forme une base de $\hat{B}$, il existe alors des scalaires $(a_\beta)_{\beta\in V(\mathbf{P})}$ tels que

$$\tau_{\mathbf{P}} = \sum_{\beta\in V(\mathbf{P})} a_\beta \partial_\beta.$$

D'après la caractérisation (4.3.1) du résidu, on sait que le polynôme en $\mathbf{x}$

$$\Delta_{\mathbf{P}} \triangleright \tau_{\mathbf{P}} - 1 = \sum_{\beta\in V(\mathbf{P})} a_\beta \Delta(\mathbf{x},\beta) - 1 \in (\mathbf{P}).$$

Si $\alpha \in V(\mathbf{P}), (\Delta_{\mathbf{P}} \triangleright \tau_{\mathbf{P}} - 1)(\alpha) = a_\alpha J_{\mathbf{P}}(\alpha) - 1 = 0$, donc $a_\alpha = \frac{1}{J_{\mathbf{P}}(\alpha)}$. □

On remarque en particulier que les polynômes $(\frac{\Delta(\mathbf{x},\alpha)}{J_{\mathbf{P}}(\alpha)})_{\alpha\in V(\mathbf{P})}$ sont des polynômes d'interpolation aux points α. Pour construire, un polynôme de petit degré qui vaut a_α au point α, il suffit par exemple de prendre

$$\sum_{\alpha\in V(\mathbf{P})} a_\alpha \frac{\Delta(\mathbf{x},\alpha)}{J_{\mathbf{P}}(\alpha)}.$$

Cette formule généralise la formule d'interpolation de Lagrange, à plusieurs variables.

Exercice 1:

Etant donné N points $\alpha_1, \ldots, \alpha_N \in \mathbb{K}^n$, peut-on (et comment) trouver $P_1, \ldots, P_n \in R$ tels que les points α_i soient les zéros simples des polynômes P_j ?

Corollaire 4.3.1 – *Si les polynômes P_i sont des formes affines $P_i = a_{i,1}x_1 + \ldots + a_{i,n}x_n + a_{i,n+1}, 1 \leq i \leq n$, alors*

$$\tau_{\mathbf{P}} = \frac{1}{\det a_{i,j}} \partial_\zeta \ ,$$

où ζ est la racine commune à $P_1, \ldots, P_n$.

4.4 Action du groupe affine sur le résidu

Considérons une transformation affine A de $\mathbb{K}^n$,

$$\mathbf{x} \mapsto A(\mathbf{x}) = U \cdot \mathbf{x} + T$$

où U est une matrice du groupe linéaire $\mathrm{GL}(n, \mathbb{K})$ et T un vecteur translation de $\mathbb{K}^n$. Nous voulons décrire la variation du résidu de $\mathbf{P} = (P_1, \ldots, P_n)$ par ce changement de variables. Pour cela, nous notons pour tout $f \in \mathbb{K}[\mathbf{x}]$, $f^A(\mathbf{x}) = f(U \cdot \mathbf{x} + T)$ et pour tout polynôme $D(\mathbf{x}, \mathbf{y}) \in \mathbb{K}[\mathbf{x}, \mathbf{y}]$, $D^A(\mathbf{x}, \mathbf{y}) = D(U \cdot \mathbf{x} + T, U \cdot \mathbf{y} + T)$. Comme

$$\mathbf{dP} = \mathbf{P}(\mathbf{x}) - \mathbf{P}(\mathbf{y}) = \Theta(\mathbf{P})\, \mathbf{dx} \ ,$$

on a

$$\mathbf{dP}^A = \mathbf{P}^A(\mathbf{x}) - \mathbf{P}^A(\mathbf{y}) = \Theta(\mathbf{P})^A\, U\, \mathbf{dx}.$$

Donc on peut prendre

$$\Delta_{\mathbf{P}^A} = (\Delta_{\mathbf{P}})^A \det(U).$$

Définissons $\tau \in \hat{R}$ par

$$\tau(Q) = \frac{1}{\det(U)} \tau_{\mathbf{P}}(Q^{A^{-1}}) \ , \ \text{pour} \ \ Q \in R \ .$$

- Pour tout $Q \in (\mathbf{P}^A)$, $Q^{A^{-1}} \in (\mathbf{P})$ et $\tau(Q) = 0$.
- Montrons que $(\Delta_{\mathbf{P}^A} \triangleright \tau - 1) \in (\mathbf{P}^A)$. Pour cela, on remarque que

$$\Delta_{\mathbf{P}^A} \triangleright \tau - 1 = \det(U)\, (\Delta_{\mathbf{P}})^A \triangleright \tau - 1 = (\Delta_{\mathbf{P}} \triangleright \tau_{\mathbf{P}} - 1)^A \in (\mathbf{P})^A = (\mathbf{P}^A).$$

Ces deux propriétés caractérisent le résidu $\tau_{\mathbf{P}^A}$ de $\mathbf{P}^A$ et donc $\tau = \tau_{\mathbf{P}^A}$.

Théorème 4.4.1 — *Soit* $\mathbf{x} \mapsto A(\mathbf{x}) = U \cdot \mathbf{x} + T$ *une transformation affine inversible; alors pour tout* $Q \in R$

$$\tau_{\mathbf{P}^A}(Q^A) = \frac{1}{\det(U)} \tau_{\mathbf{P}}(Q).$$

Exercice 2:

Généraliser cette formule au cas d'une transformation polynomiale quelconque.

4.5 Trace et résidu

A tout élément $b \in B = \mathbb{K}[\mathbf{x}]/(\mathbf{P})$ correspond un opérateur de multiplication μ_b; la trace de cet opérateur $\mathbb{K}$-linéaire est notée $Tr(b)$. L'application

$$\begin{aligned} Tr : B &\rightarrow \mathbb{K} \\ b &\mapsto Tr(b) \end{aligned}$$

est un élément de $\hat{B}$. Comme B est Gorenstein, il existe un unique $b \in B$ tel que $Tr = b.\tau$. Nous allons déterminer b. Pour cela désignons par $J_{\mathbf{P}}$ le jacobien de l'application $\mathbf{P}$.

Théorème 4.5.1 — $Tr = J_{\mathbf{P}} \cdot \tau$

Preuve. Soit $\Delta = \sum_{i=1}^{d} a_i \otimes b_i$, où (a_i) et (b_i) sont deux bases duales pour le produit scalaire défini par τ (proposition 3.3.1). Dans B, $J_{\mathbf{P}} = \sum a_i b_i$ (car $\Delta(\mathbf{x}, \mathbf{x}) = J_{\mathbf{P}}(\mathbf{x})$). Soit $b \in B$; d'après la formule (8), on a $b\, b_j = \sum_i \langle a_i | b\, b_j \rangle b_i = \sum_i \langle b | a_i b_j \rangle b_i$. Donc la trace de μ_b (calculée dans la base (b_i)) est

$$Tr(b) = \sum_i \langle b | a_i b_i \rangle = \tau(b \sum_i a_i b_i) = \tau(b\, J_{\mathbf{P}}) = (J_{\mathbf{P}}.\tau)(b).$$

□

Nous en déduisons, lorsque la caractéristique du corps de base $\mathbb{K}$ est nulle ou supérieure à la dimension de l'espace vectoriel B, le corollaire suivant.

Corollaire 4.5.2 — *La dimension de l'espace vectoriel B sur $\mathbb{K}$ est égale à $\tau_{\mathbf{P}}(J_{\mathbf{P}})$.*

Preuve. Il suffit de remarquer que $\dim_{\mathbb{K}} B = Tr(1) = (J_{\mathbf{P}} \cdot \tau_{\mathbf{P}})(1) = \tau_{\mathbf{P}}(J_{\mathbf{P}})$. □

4.6 Loi de transformation

La loi de transformation décrit la variation du résidu lorsque l'on passe d'une application polynomiale à l'autre (voir [19]). Pour une preuve analytique (voir [15], [4]).

Soient $\mathbf{P} = (P_1, \ldots, P_n)$ et $\mathbf{Q} = (Q_1, \ldots, Q_n)$ deux applications polynomiales définissant des suites quasi-régulières de R telles que

$$Q_i = \sum_{j=1}^{n} A_{i,j} P_j \ , \quad A_{i,j} \in R \ , \quad 1 \leq i, j \leq n.$$

Notons $\mathbf{A}$ la matrice $(A_{i,j})_{i,j}$, A son déterminant et $\tau_{\mathbf{P}}$ (resp. $\tau_{\mathbf{Q}}$) le résidu associé à $\mathbf{P}$ (resp. $\mathbf{Q}$).

Théorème 4.6.1 (Loi de transformation) — $\tau_{\mathbf{P}} = A \cdot \tau_{\mathbf{Q}}$

Preuve. Il suffit de vérifier, d'après la caractérisation (4.3.1), que $A \cdot \tau_{\mathbf{Q}} = 0$ sur $(\mathbf{P})$ et $\Delta_{\mathbf{P}} \triangleright (A \cdot \tau_{\mathbf{Q}}) - 1 \in (\mathbf{P})$.

Soit $h \in (\mathbf{P})$; d'après l'identité de Cramer, $AP_i \in (\mathbf{Q}), 1 \leq i \leq n$, donc $A\,h \in (\mathbf{Q})$, et $(A \cdot \tau_{\mathbf{Q}})(h) = \tau_{\mathbf{Q}}(A\,h) = 0$.

Vérifions que $\Delta_{\mathbf{P}} \triangleright (A \cdot \tau_{\mathbf{Q}}) - 1 \in (\mathbf{P})$ ou encore $(\Delta_{\mathbf{P}}(\mathbf{x}, \mathbf{y})\, A(\mathbf{y})) \triangleright \tau_{\mathbf{Q}} - 1 \in (\mathbf{P})$. Par construction

$$P_i(\mathbf{x}) - P_i(\mathbf{y}) = \sum_{j=1}^{n} \theta_j(P_i)(\mathbf{x}, \mathbf{y})\, dx_j \quad , \quad 1 \leq i \leq n \quad ,$$

ou encore

$$\mathbf{P}(\mathbf{x}) - \mathbf{P}(\mathbf{y}) = (\theta_j(P_i))\,\mathbf{dx} = \Theta(\mathbf{P})\,\mathbf{dx} \quad ,$$

avec $\det(\Theta(\mathbf{P})) = \det(\theta_j(P_i)) = \Delta_{\mathbf{P}}$. Il en résulte que

$$\begin{aligned} \mathbf{Q}(\mathbf{x}) - \mathbf{Q}(\mathbf{y}) &= \mathbf{A}(\mathbf{x})\,\mathbf{P}(\mathbf{x}) - \mathbf{A}(\mathbf{y})\,\mathbf{P}(\mathbf{y}) \\ &= \mathbf{A}(\mathbf{y})\,(\mathbf{P}(\mathbf{x}) - \mathbf{P}(\mathbf{y})) + (\mathbf{A}(\mathbf{x}) - \mathbf{A}(\mathbf{y}))\,\mathbf{P}(\mathbf{x}) \\ &= (\mathbf{A}(\mathbf{y})\,\Theta(\mathbf{P}) + \mathbf{R})\mathbf{dx} \\ &= \tilde{\Theta}(\mathbf{Q})\mathbf{dx} \quad , \end{aligned}$$

avec $\mathbf{R} = (R_{i,j}), R_{i,j} \in (\mathbf{P}(\mathbf{x}))\mathbb{K}[\mathbf{x}, \mathbf{y}]$ et $\tilde{\Theta}(\mathbf{Q}) = \mathbf{A}(\mathbf{y})\,\Theta(\mathbf{P}) + \mathbf{R}$. D'après (3.5.1),

$$\tilde{\Delta}_{\mathbf{Q}} - \Delta_{\mathbf{Q}} \in (\mathbf{Q}(\mathbf{x}) - \mathbf{Q}(\mathbf{y})) \quad , \quad \tilde{\Delta} = \det \Theta(\mathbf{Q}).$$

Par suite, $\tilde{\Delta}_{\mathbf{Q}} \triangleright \tau_{\mathbf{Q}} - \Delta_{\mathbf{Q}} \triangleright \tau_{\mathbf{Q}} \in (\mathbf{Q}(\mathbf{x}))$. Comme $\Delta_{\mathbf{Q}} \triangleright \tau_{\mathbf{Q}} - 1 \in (\mathbf{Q}), \tilde{\Delta}_{\mathbf{Q}} \triangleright \tau_{\mathbf{Q}} - 1 \in (\mathbf{Q})$. Or

$$H(\mathbf{x}, \mathbf{y}) = \tilde{\Delta}_{\mathbf{Q}} - \det(\mathbf{A}(\mathbf{y})\,\Theta(\mathbf{P})) \in (\mathbf{P}(\mathbf{x})).$$

Ainsi

$$\begin{aligned} \Delta_{\mathbf{P}} \triangleright (A \cdot \tau_{\mathbf{Q}}) - 1 &= (A(\mathbf{y})\Delta_{\mathbf{P}}(\mathbf{x}, \mathbf{y})) \triangleright \tau_{\mathbf{Q}} - 1 \\ &= \tilde{\Delta}_{\mathbf{Q}} \triangleright \tau_{\mathbf{Q}} - 1 - H(\mathbf{x}, \mathbf{y}) \triangleright \tau_{\mathbf{Q}} \in (\mathbf{P}). \end{aligned}$$

□

Les corollaires suivants sont des conséquences immédiates de la loi de transformation

Corollaire 4.6.2 — *L'application* $\mathbf{P} \mapsto \tau_{\mathbf{P}}$ *est alternée.*

Preuve. Pour toute permutation σ de $\{1,\ldots,n\}$, on applique la loi de transformation, avec la matrice associée à σ dans une base canonique, son déterminant étant la signature de σ. □

Corollaire 4.6.3 — *Soient* $\mathbf{P}=(P_1,\ldots,P_n)$ *et* $\mathbf{Q}=(Q_1,\ldots,Q_n)$ *deux applications polynomiales. Supposons que* $\mathbf{P}$ *et* $\mathbf{P}\star\mathbf{Q}=(P_1\,Q_1,\ldots,P_nQ_n)$ *définissent des suites quasi-régulières. Alors*

$$\tau_{\mathbf{P}}=Q_1\cdots Q_n\cdot\tau_{\mathbf{P}\star\mathbf{Q}}.$$

On peut voir cette formule comme une simplification dans une fraction rationnelle de dénominateur $\prod_{i=1}^n P_i\,Q_i$ et de numérateur $\prod_{i=1}^n Q_i$.

4.7 Transformation polynomiale

Supposons que $P_1,\ldots,P_{n-1}\in\tilde{R}=\mathbb{K}[x_1,\ldots,x_{n-1}]$ et $P_n=x_n-Q$, avec $Q\in\tilde{R}$. Supposons que $\mathbf{P}=(P_1,\ldots,P_n)$ forme une suite quasi-régulière de R. Notons $\tilde{\mathbf{P}}=(P_1,\ldots,P_{n-1})$ l'application polynomiale de $\tilde{R}$, et pour tout $f\in R$, $\tilde{f}=f(x_1,\ldots,x_{n-1},Q(x_1,\ldots,x_{n-1}))\in\tilde{R}$.

Théorème 4.7.1 — *Pour tout* $f\in R,\tau_{\mathbf{P}}(f)=\tau_{\tilde{\mathbf{P}}}(\tilde{f})$.

Preuve. Vérifions que $\tau_{\mathbf{P}}$ restreint à $\tilde{R}$ (noté $\tau_{\mathbf{P}}|_{\tilde{R}}$) coïncide avec $\tau_{\tilde{\mathbf{P}}}$. Remarquons d'abord que $\Delta_{\mathbf{P}}=\Delta_{\tilde{\mathbf{P}}}$. Alors

$$\Delta_{\tilde{\mathbf{P}}}\triangleright\tau_{\mathbf{P}}-1\in(\mathbf{P})\cap\tilde{R}=(\tilde{\mathbf{P}}).$$

De plus, $\tau_{\mathbf{P}}|_{\tilde{R}}$ s'annule sur $(\mathbf{P})\cap\tilde{R}=(\tilde{\mathbf{P}})$. Donc d'après la caractérisation du résidu (4.3.1), $\tau_{\mathbf{P}}|_{\tilde{R}}=\tau_{\tilde{\mathbf{P}}}$.

Par ailleurs $\forall f\in R$, $f-\tilde{f}\in(\mathbf{P})$; il en résulte que

$$\tau_{\mathbf{P}}(f)=\tau_{\mathbf{P}}(\tilde{f})=\tau_{\tilde{\mathbf{P}}}(\tilde{f}).$$

□

Plaçons nous maintenant dans le cas où $P_1,\ldots,P_{n-1}\in R$ et $P_n=x_n-Q$, avec $Q\in\tilde{R}$. Supposons que $\mathbf{P}=(P_1,\ldots,P_n)$ forme une suite quasi-régulière de R. Notons pour tout polynôme f de R, $f^Q=f(x_1,\ldots,x_{n-1},Q(x_1,\ldots,x_{n-1}))$, et $\mathbf{P}^Q=(P_1^Q,\ldots,P_{n-1}^Q)$.

Corollaire 4.7.1 — *Pour tout* $f\in R,\tau_{\mathbf{P}}(f)=\tau_{\mathbf{P}^Q}(f^Q)$.

Preuve. On peut écrire P_i^Q sous la forme $P_i^Q = P_i + A_i\,(x_n - Q) = P_i + A_i\,P_n, 1 \leq i \leq n-1$, avec $A_i \in R$. En appliquant la loi de transformation

$$\tau_{\mathbf{P}} = \tau_{(P_1^Q,\ldots,P_{n-1}^Q,x_n-Q)}\ ,$$

et le corollaire provient du théorème précédent. □

Exercice 3:

Retrouver le même type de résultats avec $P_n = x_n^d - Q(x_1,\ldots,x_n)$ et $\deg_{x_n}(Q) < d$.

4.8 Résidu et produit

Etant donnés $n+1$ polynômes $P_1, ..., P_{n-1}, F, G$ de $\mathbb{K}[\mathbf{x}]$ tels que $(P_1,\ldots,P_{n-1},F)$ et $(P_1,\ldots,P_{n-1},G)$ soient quasi-regulières, et posons $P_n = FG$. L'application $\mathbf{P} = (P_1, ..., P_n)$ définit aussi une suite quasi-regulière. Supposons que $P_1,\ldots,P_{n-1},F,G$ n'ont pas de racine commune; d'après le théorème des zéros de Hilbert, il existe deux polynômes $U, V \in R$ tels que $V\,F + U\,G - 1 \in (P_1,\ldots,P_{n-1})$.

Proposition 4.8.1 — $\tau_{\mathbf{P}} = U \cdot \tau_{(P_1,\ldots,P_{n-1},F)} + V \cdot \tau_{(P_1,\ldots,P_{n-1},G)}$.

Preuve. Pour tout $f \in R$, $f - (V\,F\,f + U\,G\,f) \in (P_1,\ldots,P_{n-1})$, donc en appliquant le corollaire (4.6.3),

$$\begin{aligned}\tau_{\mathbf{P}}(f) &= \tau_{\mathbf{P}}(F\,V\,f) + \tau_{\mathbf{P}}(G\,U\,f)\\ &= \tau_{(P_1,\ldots,P_{n-1},G)}(V\,f) + \tau_{(P_1,\ldots,P_{n-1},F)}(U\,f)\\ &= U\cdot\tau_{(P_1,\ldots,P_{n-1},F)}(f) + V\cdot\tau_{(P_1,\ldots,P_{n-1},G)}(f).\end{aligned}$$

□

4.9 Formule de Weil

La formule de Weil est une généralisation de la formule de Cauchy (15). Le corps de base $\mathbf{K}$ est le corps des fractions $\mathbb{K}(z_1,\ldots,z_n)$. Nous considérons l'idéal de $\mathbf{K}[\mathbf{x}]$ engendré par l'application $\mathrm{d}\mathbf{P} = (P_1(\mathbf{x}) - P_1(\mathbf{z}),\ldots,P_n(\mathbf{x}) - P_n(\mathbf{z}))$.

Théorème 4.9.1 — *Soit $\tau_{\mathrm{d}\mathbf{P}}$ le résidu associé à $\mathrm{d}\mathbf{P}$ dans $\mathbf{K}[x_1,\ldots,x_n]$. Alors pour tout $f \in \mathbf{K}[x_1,\ldots,x_n]$*

$$f(\mathbf{z}) = \tau_{\mathrm{d}\mathbf{P}} \triangleright f(\mathbf{x})\Delta(\mathbf{x},\mathbf{z}).$$

Preuve. Par construction

$$\mathrm{d}\mathbf{P} = (\theta_i(P_j(\mathbf{x},\mathbf{z}))\,\mathrm{d}\mathbf{x}\ ,$$

avec $\mathrm{d}\mathbf{x} = (x_1 - z_1, \ldots, x_n - z_n)$. D'après la loi de transformation (4.3.1),

$$\tau_{\mathrm{d}\mathbf{x}} = \Delta(\mathbf{x},\mathbf{z}) \cdot \tau_{\mathrm{d}\mathbf{P}}\ .$$

D'après la formule de Cauchy (15),

$$\tau_{\mathrm{d}\mathbf{x}}(f(\mathbf{x})) = f(\mathbf{z}).$$

Par conséquent

$$f(\mathbf{z}) = \tau_{\mathrm{d}\mathbf{x}}(f(\mathbf{x})) = \tau_{\mathrm{d}\mathbf{P}}(\Delta(\mathbf{x},\mathbf{z}) \cdot f(\mathbf{x}))\ .$$

□

4.10 Une base du quotient B

D'après le théorème (3.2.1), une partie génératrice de B est formée des éléments qui apparaissent dans une décomposition de Δ. Notons $\nu = \sum_{i=1}^{n} d_i - n$ où $d_i = deg(P_i)$; c'est une borne pour les degrés des polynômes qui apparaissent dans Δ. Ainsi, les monômes de degré au plus ν forment une partie génératrice de l'espace vectoriel B.

Théorème 4.10.1 — *Il existe une base de B formée de monômes de degré au plus ν.*

Pour l'exemple pathologique classique

$$P_1 = x_1^d - x_2, P_2 = x_2^d - x_3, \ldots, P_{n-1} = x_{n-1}^d - x_n, P_n = x_n^d,$$

une base de $R/(\mathbf{P})$ est formée des monômes de la forme $\prod_{i=1}^{n} x_i^{a_i}$, avec $a_i < d$. Le degré total de ces monômes est au plus $n\,d - n$. On remarque que $(P_1, \ldots, P_n)$ est une base de Gröbner de l'idéal $(\mathbf{P})$. On rajoute souvent à ce système $P_0 = 1 - x_0^{d-1} x_1$ pour qu'il n'y ait aucun point dans la partie affine.

Le théorème précédent entraîne le résultat suivant

Théorème 4.10.2 — *Il existe une base standard de $(\mathbf{P})$ dont le degré de ses éléments est au plus $\sum_i \deg P_i - n + 1$.*

Preuve. D'après le théorème (4.10.1), on choisit une base $\mathbf{e} = (m_1, \ldots, m_d)$ de $B = R/(\mathbf{P})$ formée de monômes de degré $\leq \nu$. On les prend le plus proche de l'origine, suivannt un ordre monomial. On peut supposer qu'elle est stable par dérivation (i.e. elle est au dessous d'un escalier). Soit $\mathcal{B}$ le sous espace vectoriel de R engendré par $m_1, \ldots, m_d$. Pour tout $x_l, 1 \leq l \leq n$, il existe des polynômes uniques $\sigma_i^l \in (\mathbf{P})$ et $\rho_i^l \in \mathcal{B}$ tels que

$$x_l\, m_i = \sigma_i^l + \rho_i^l \quad , \quad 1 \leq i \leq n \ .$$

Si $x_l\, m_i \in \mathcal{B}, \sigma_i^l = 0$. Donc, l'élément σ_i^l non nul provient de la multiplication de x_l par le monôme m_i, qui se trouve au bord de la base $\mathbf{e}$; le degré d'un tel $x_l m_i$ est au plus $\nu + 1$. En utilisant les relations $x_l\, m_i = \rho_i^l$, dans B, on peut réécrire tout élément du sous espace vectoriel $\mathcal{B}_1 = \sum_i x_i\, \mathcal{B}$ dans $\mathcal{B}$. On définit $\mathcal{B}_k = \sum_i x_i\, \mathcal{B}_{k-1}$, pour tout $k \in \mathbb{N}^*$.

Pour tout $h \in R$, il existe $k \in \mathbb{N}^*$ tel que $h \in \mathcal{B}_1 + \ldots + \mathcal{B}_k$. Par récurrence, h se réécrit dans $\mathcal{B}$ modulo $\sigma = (\sigma_i^l)_{l,i}$. Ceci montre que $\mathbf{e}$ est une partie génératrice de $R/(\sigma)$. Comme $(\sigma) \subset (\mathbf{P})$ et $\mathcal{B} \oplus (\mathbf{P}) = R, (\sigma) = (\mathbf{P})$, et la réécriture ci-dessus est canonique. Les polynômes $\sigma_i^l, 1 \leq i, l \leq n$, de degré $\leq \nu + 1$, forment donc une base standard de $(\mathbf{P})$. □

4.11 Résidu et application polynomiale

On s'intéresse à l'application polynomiale

$$\begin{array}{rcl} \mathbb{K}^n & \to & \mathbb{K}^n \\ (x_1, \ldots, x_n) & \mapsto & (P_1(\mathbf{x}), \ldots, P_n(\mathbf{x})). \end{array}$$

Pour cela nous considérons son graphe et nous le définissons en rajoutant de nouvelles variables $\mathbf{u} = (u_1, \ldots, u_n)$ par les équations de $\mathbb{K}[\mathbf{x}, \mathbf{u}]$:

$$P_1(\mathbf{x}) - u_1 = \cdots = P_n(\mathbf{x}) - u_n = 0$$

Notons $\mathbf{P_u}$ la liste de ces polynômes. Nous allons en fait considérer les u_i comme des paramètres et prendre comme nouveau corps de coefficients $\mathbf{K} = \mathbb{K}(u_1, \ldots, u_n)$.

Definition 4.11.1 — *Une application polynomiale $\mathbf{P} = (P_1, ..., P_n)$ est dite propre, si l'anneau $\mathbb{K}[x_1, ..., x_n]$ est entier sur le sous anneau $\mathbb{K}[\mathbf{P}]$ (i.e. les coordonnées $x_1, \ldots, x_n$ vérifient des relations de dépendance intégrale à coefficients dans $\mathbb{K}[\mathbf{P}]$).*

Remarquons qu'une application polynomiale propre définit une suite quasi-régulière: en effet, si α est une racine du système $\{\mathbf{P}=0\}$, les coordonnées $\alpha_1,\ldots,\alpha_n$ de α sont solutions de polynômes d'une variable, donc leur nombre est fini.

Théorème 4.11.2 — *L'application polynomiale* $\mathbf{P}$ *est propre, si et seulement si, pour tout* $f\in\mathbb{K}[\mathbf{x}]$, $\tau_{\mathbf{P_u}}(f)\in\mathbb{K}[\mathbf{u}]$.

Preuve. Supposons que pour tout $f\in R$, $\tau_{\mathbf{P_u}}(f)\in\mathbb{K}[\mathbf{u}]$, et soit $\mathbf{b}=(b_1,\ldots,b_d)$ une base du $\mathbb{K}(\mathbf{P})$-espace vectoriel $\mathbb{K}(\mathbf{x})$. La famille $\mathbf{b}$ est aussi une base de $B_{\mathbf{u}}=\mathbf{K}[\mathbf{x}]/(\mathbf{P_u})$. La formule de représentation (8) appliquée dans l'algèbre $B_{\mathbf{u}}$ fournit,

$$x_l\,b_j=\sum_{i=1}^{d}\tau_{\mathbf{P_u}}(x_l\,b_j\,a_i)\,b_i=\sum_{i=1}^{d}m_{i,j}^{l}(\mathbf{u})\,b_i.$$

Par conséquent la matrice $M_l=(m_{i,j}^{l})_{i,j}$ est la matrice de la multiplication par x_l dans $B_{\mathbf{u}}$ dans la base (b_i).

Par hypothèse, $m_{i,j}^{l}(\mathbf{u})=\tau_{\mathbf{P_u}}(x_l\,b_j\,a_i)\in\mathbb{K}[\mathbf{u}]$. En considérant le polynôme caractéristique A de la matrice M_l, on obtient en utilisant le théorème de Cayley-Hamilton

$$A(x_l)=x_l^{d}+c_1(\mathbf{u})\,x_l^{d-1}+\cdots+c_d(\mathbf{u})\in(P_1-u_1,\ldots,P_n-u_n)\ ,\ c_i\in\mathbb{K}[\mathbf{u}]. \quad (17)$$

En substituant, dans A, $\mathbf{u}$ par $\mathbf{P}$, on trouve une relation de dépendance intégrale de x_l à coefficients dans $\mathbb{K}[\mathbf{P}]$. Donc l'application polynomiale $\mathbf{P}$ est propre.

Supposons $\mathbf{P}$ propre, et soit $f\in R$. Comme pour tout $i=1,...,n$, il existe des entiers positifs d_i et des polynômes $a_{i,j}\in\mathbb{K}[\mathbf{x}]$ tels que

$$x_i^{d_i}+a_{i,1}(\mathbf{P})\,x_i^{d_i-1}+\cdots+a_{i,d_i}(\mathbf{P})=0,$$

on a

$$x_i^{d_i}+a_{i,1}(\mathbf{u})\,x_i^{d_i-1}+\cdots+a_{i,d_i}(\mathbf{u})=\sum_{i=1}^{n}A_{i,j}\,(P_i-u_i),$$

avec $A_{i,j}\in\mathbb{K}[\mathbf{x},\mathbf{u}]$. Posons $Q_i(x)=x_i^{d_i}+a_{i,1}(\mathbf{u})\,x_i^{d_i-1}+\cdots+a_{i,d_i}(\mathbf{u})$ et $\mathbf{Q}=(Q_1,\ldots,Q_n)$. En appliquant la loi de transformation, (16) et (14), on a

$$\tau_{\mathbf{P_u}}(f)=\tau_{\mathbf{Q}}(\det(A_{i,j})\,f)=\sum_{\alpha}a_\alpha(\mathbf{u})\tau_{\mathbf{Q}}(\mathbf{x}^\alpha)=\sum_{\alpha}a_\alpha(\mathbf{u})\prod_{i=1}^{n}\tau_{Q_i}(x_i^{\alpha_i})\in\mathbb{K}[\mathbf{u}].$$

□

Théorème 4.11.1 — *Soit* $\overline{\Delta}(\mathbf{u})$ *l'application de* $Hom_{\mathbf{K}}(\mathbf{K}[\mathbf{x}]/(\mathbf{P_u}),\mathbf{K})$ *dans* $\mathbf{K}[\mathbf{x}]/(\mathbf{P_u})$ *associée à* Δ. *Si* $\mathbf{P}$ *est propre alors le déterminant de* $\overline{\Delta_{\mathbf{u}}}$ *est dans* $\mathbb{K}-\{0\}$.

Preuve. Comme $\mathbf{P}$ est propre, $R = \mathbb{K}[\mathbf{x}]$ est un $\mathbb{K}[\mathbf{P}]$-module libre de base, toute base $m_1, \ldots, m_d$ de B (voir [24], [20]). On a donc une décomposition de R de la forme

$$R = \oplus_{i=1}^{d} m_i \, \mathbb{K}[P_1, \ldots, P_n]. \tag{18}$$

Notons $R_{\mathbf{K}} = R \otimes \mathbf{K} = \mathbf{K}[\mathbf{x}]$. De même $R_{\mathbf{K}}$ se décompose sous la forme

$$R_{\mathbf{K}} = \oplus_{i=1}^{d} m_i \, \mathbf{K}[P_1, \ldots, P_n] \tag{19}$$

par extension des scalaires et (m_i) est aussi une base de $R_{\mathbf{K}}/(\mathbf{P_u})$. Comme les fibres de l'application $\mathbf{P}$ sont de même cardinal, on en déduit également que pour toutes valeurs de $\mathbf{u}$ dans $\mathbb{K}^n$, (m_i) est une base du $\mathbb{K}[\mathbf{P} - \mathbf{u}]$-module libre R.

Considérons une décomposition de $\Delta_{\mathbf{P}} = \Delta_{\mathbf{P_u}}$ de la forme

$$\Delta_{\mathbf{P}} = \sum_{i=1}^{s} a_i \otimes b_i$$

où $(a_1, \ldots, a_d)$ (resp. $(b_1, \ldots, b_d)$) est une base de B et $a_{d+1}, \ldots, a_s$ (resp. $b_{d+1}, \ldots, b_s$) dans $(\mathbf{P})$. En utilisant la décomposition (18) avec la base $(a_i)_{1 \le i \le d}$ et les relations $P_i = (P_i - u_i) + u_i$ on obtient pour $j > d$,

$$\begin{array}{l} a_j - \sum_{i=1}^{d} h_{i,j}(\mathbf{u})\, a_i \in (\mathbf{P_u}) \\ b_j - \sum_{i=1}^{d} l_{i,j}(\mathbf{u})\, b_i \in (\mathbf{P_u}) \end{array}$$

avec $l_{i,j}, h_{i,j} \in \mathbb{K}[u_1, \ldots, u_n]$. On déduit de ces décompositions que

$$\Delta - \sum_{1 \le i,j \le d} \delta_{i,j}(\mathbf{u})\, a_i \otimes b_j \in (\mathbf{P_u}(\mathbf{x}), \mathbf{P_u}(\mathbf{y}))$$

avec $\delta_{i,j} \in \mathbb{K}[\mathbf{u}]$. Notons $\overline{\Delta}(\mathbf{u})$ la matrice $(\delta_{i,j}(\mathbf{u}))$ des coefficients ci-dessus. C'est la matrice de l'application de $Hom_{\mathbf{K}}(\mathbf{K}[\mathbf{x}]/(\mathbf{P_u}), \mathbf{K})$ dans $\mathbf{K}[\mathbf{x}]/(\mathbf{P_u})$ associée à Δ ou encore la matrice de l'application de $Hom_{\mathbb{K}}(\mathbb{K}[\mathbf{x}]/(\mathbf{P_u}), \mathbb{K})$ dans $\mathbb{K}[\mathbf{x}]/(\mathbf{P_u})$ quand on spécifie les valeurs de $u_1, \ldots, u_n$ dans $\mathbb{K}$.

Pour toute valeur de $\mathbf{u}$, le système $\mathbf{P_u}$ est une intersection complète, car on a des relations de dépendance intégrale modulo $(\mathbf{P_u})$ du type (17). On en déduit que $\overline{\Delta}(\mathbf{u})$ est un isomorphisme donc son déterminant est non nul, pour toute valeur de $\mathbf{u}$. Par conséquent, c'est une constante non-nulle. □

Pour construire le résidu de $\tau_{\mathbf{P_u}}$ ($\mathbf{P}$ étant quasi-régulière), on peut procéder de la façon suivante. La décomposition (18) montre que

$$1 - \sum_{i=1}^{d} t_i(\mathbf{u})\, a_i \in (\mathbf{P_u}), t_i \in \mathbb{K}[\mathbf{u}]$$

avec en particulier $1 - \sum_{i=1}^{d} t_i(0)\, a_i \in (\mathbf{P})$.

Soit $s = [s_1, \ldots, s_d] \in \mathbf{K}^d$ tel que $\overline{\Delta}^{-1}[t_1, \ldots, t_d]^t = [s_1, \ldots, s_d]$ ($\overline{\Delta}$ est inversible car $\overline{\Delta}(0) = Id$). Les s_i sont donc des fractions rationnelles en $\mathbf{u}$ dont le dénominateur est le déterminant de $\overline{\Delta}$. En particulier $s_i(0) = t_i(0)$. Définissons maintenant $\tau_{\mathbf{u}}$ par

1. $\tau_{\mathbf{u}} = 0$ sur $(\mathbf{P_u})$,
2. $\tau_{\mathbf{u}}(b_i) = s_i(\mathbf{u})$

On vérifie que

$$\Delta \triangleright \tau_{\mathbf{u}} = \sum_{i,j=1}^{d} \delta_{i,j}(\mathbf{u})\, \tau_{\mathbf{u}}(b_j)\, a_i + f = \sum_{i=1}^{d} (\sum_{j=1}^{d} \delta_{i,j}(\mathbf{u})\, s_j(\mathbf{u}))\, a_i + f = \sum_{i=1}^{d} t_i\, a_i + f = 1 + g$$

avec $f, g \in (\mathbf{P_u})$. Donc d'après (4.3.1), $\tau_{\mathbf{u}}$ est le résidu associé à $\mathbf{P_u}$. Remarquons que le résidu $\tau_{\mathbf{P}}$ est tel que $\tau_{\mathbf{P}}(b_i) = t_i(0) = s_i(0)$.

Pour tout élément $h \in R$, il existe $h_1, \ldots, h_d \in \mathbb{K}[\mathbf{u}]$ tels que

$$h = \sum_{i=1}^{d} h_i(\mathbf{u})\, b_i + (\mathbf{P_u}).$$

Il en résulte que

$$\tau_{\mathbf{u}}(h) = \sum_{i=1}^{d} h_i(\mathbf{u})\, s_i(\mathbf{u}) = \frac{n(\mathbf{u})}{\det(\overline{\Delta})}$$

avec $n(\mathbf{u}) \in \mathbb{K}[\mathbf{u}]$.

4.11.1 Exemples d'applications polynomiales propres

– Exemple d'application propre ayant des points à l'infini. Nous allons voir dans la section suivante qu'une application sans zéro à l'infini est propre.

$$\begin{cases} p_1 := x^2 - y \\ p_2 := x\, y - 1 \end{cases}$$

La variable x vérifie la relation

$$x^3 - p_1 x - p_2 - 1 = 0.$$

La variable y vérifie la relation

$$y^3 + y^2 p_1 - 1 - 2\,p_2 - {p_2}^2 = 0.$$

C'est un exemple où l'intersection est « propre » en projectif.

– Si on remplace p_1 par $x^2 - x$, l'application n'est plus propre car en remplaçant x par 0, on voit qu'il n'existe pas de relation de dépendance intégrale en y.

– Exemple d'application polynomiale propre où la partie à l'infini est une courbe

$$\begin{cases} p_1 := x^2 + y^2 + z^2 - x \\ p_2 := x^2 + y^2 + z^2 - y \\ p_3 := x^2 + y^2 + z^2 - z \end{cases}$$

La variable x vérifie la relation

$$3\,x^2 + (4\,p_1 - 2\,p_2 - 2\,p_3 - 1)\,x + 2\,{p_1}^2 - 2\,p_1 p_3 + {p_2}^2 + {p_3}^2 - 2\,p_1 p_2 - p_1 = 0.$$

Par symétrie les variables y, z vérifient des relations de dépendance intégrale du même type.

4.12 Le résidu dans le cas où P n'a pas de zéro à l'infini

4.12.1 Cas de polynômes homogènes

Nous nous plaçons maintenant, dans le cas où les polynômes $P_1, \ldots, P_n$ sont homogènes et ayant l'origine comme seul zéro commun dans $\mathbb{K}^n$.

Théorème 4.12.1 (Macaulay) — *Tout monôme de degré au moins* $\nu+1 = \sum_{i=1}^n d_i - n + 1$ *est dans l'idéal de* $\mathbb{K}[\mathbf{x}]$ *engendré par* $P_1, \ldots, P_n$.

Preuve. D'après (4.10.1), tout monôme m de degré au moins $\nu + 1$ est égal, modulo $(\mathbf{P})$, à une combinaison linéaire de monômes de B, de degrés au plus ν. Comme l'idéal $(\mathbf{P})$ est homogène, on déduit que m est dans $(\mathbf{P})$. □

Ceci implique que la fonction de Hilbert du quotient est nulle à partir du degré ν. C'est le plus petit degré, à partir duquel la fonction de Hilbert est constante et qui coïncide ici avec la *régularité de Castelnuovo*.

D'après (4.12.1), on peut trouver des polynômes homogènes $A_{i,j}, 1 \leq i,j \leq n$, de degré $\nu + 1 - d_j$ tels que

$$x_i^{\nu+1} = \sum_{j=1}^{n} A_{i,j}\, P_j \ , \quad 1 \leq i \leq n. \tag{20}$$

L'identité précédente s'écrit sous la forme d'un système linéaire dans lequel les inconnues sont les coefficients des polynômes $A_{i,j}, 1 \leq i,j \leq n$. En utilisant la loi de transformation (4.6.1) et la formule (15), on a pour tout polynôme f

$$\tau_{\mathbf{P}}(f) = \tau_{\mathbf{x}^{\nu+1}}\left(\det(A_{i,j})\, f\right) = \text{coefficient de } x_1^{\nu} \dots x_n^{\nu} \text{ dans } \det(A_{i,j}) f.$$

Donc le calcul du résidu associé à une application homogène $\mathbf{P}$, d'un polynôme f, se ramène à la résolution du système linéaire (20).

Proposition 4.12.2 — *Pour tout monôme f de degré $\neq \nu, \tau_{\mathbf{P}}(f) = 0$.*

Preuve. Le degré du polynôme homogène $\det(A_{i,j})f$ est différent de $n\nu$, donc

$$\tau_{\mathbf{P}}(f) = \tau_{\mathbf{x}^{\nu+1}}\left(\det(A_{i,j})\, f\right) = \text{coefficient de } x_1^{\nu} \dots x_n^{\nu} \text{ dans } \det(A_{i,j}) f = 0.$$

□

Corollaire 4.12.3 — *Soit $\mathbb{K}$ un corps de caractéristique zéro et $\mathbf{P} = (P_1, \dots, P_n)$ une application polynomiale homogène définissant une suite quasi-régulière de $\mathbb{K}[\mathbf{x}]$. Alors, le résidu de $\mathbf{P}$ est un opérateur differentiel de degré ν à coefficients constants $(c_\alpha)_\alpha$:*

$$\tau_{\mathbf{P}} = \sum_{|\alpha|=\nu} c_\alpha \partial_0^\alpha \ ,$$

avec $\partial_0^\alpha(f) = d_{x_1}^{\alpha_1} \dots d_{x_n}^{\alpha_n}(f)(0)$, pour tout $f \in \mathbb{K}[\mathbf{x}]$, où d_{x_i} désigne la dérivée partielle par rapport à x_i.

Preuve. Soient $\alpha = (\alpha_1, \dots, \alpha_n)$ et $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$, on note $\alpha \leq \beta$ si pour tout $i \in \{1, \dots, n\}, \alpha_i \leq \beta_i$. D'après ce qui précède, (15) et la formule de Leibniz,

$$\begin{aligned}
\tau_{\mathbf{P}}(f) &= \tau_{\mathbf{x}^{\nu+1}}\left(\det(A_{i,j})\, f\right) \\
&= \frac{1}{(\nu!)^n} \partial_0^{(\nu,\dots,\nu)}\left(\det(A_{i,j})\, f\right) \\
&= \frac{1}{(\nu!)^n} \sum_{\alpha \leq \nu} C_\alpha^\nu \partial_0^{\nu-\alpha}\left(\det(A_{i,j})\right) \partial_0^\alpha(f) \\
&= \sum_{\alpha \leq \nu} c_\alpha \partial_0^\alpha(f).
\end{aligned}$$

En utilisant (4.12.2) avec $f = \mathbf{x}^\alpha, |\alpha| \leq \nu$ et $\alpha \neq \nu$, on voit que $c_\alpha = 0$ si $|\alpha| \neq \nu$. □

Dans le cas homogène, la situation est particulièrement simple pour la construction du résidu.

Proposition 4.12.4 — *Si les polynômes $P_1, \ldots, P_n$ sont homogènes, alors*

$$\Delta_{\mathbf{P}} \triangleright \tau_{\mathbf{P}} = 1, \quad \text{dans} \quad R\ .$$

Preuve. Comme $\Delta_{\mathbf{P}}(\mathbf{x}, \mathbf{y})$ est un polynôme homogène de degré ν,

$$\Delta_{\mathbf{P}}(\mathbf{x}, \mathbf{y}) = \sum_{|\alpha| \leq \nu} A_\alpha(\mathbf{x}) \mathbf{y}^\alpha\ ,\ A_\alpha \in \mathbb{K}[\mathbf{x}].$$

D'après la proposition (4.12.2) et la caractérisation (4.3.1) du résidu $\tau_{\mathbf{P}}$,

$$\Delta_{\mathbf{P}} \triangleright \tau_{\mathbf{P}} - 1 = \sum_{|\alpha| = \nu} A_\alpha \tau_{\mathbf{P}}(\mathbf{y}^\alpha) - 1 \in (\mathbf{P}),$$

alors $\Delta_{\mathbf{P}} \triangleright \tau_{\mathbf{P}} - 1 = 0$. □

Ceci permet de calculer le résidu en résolvant un système linéaire associé à Δ.

4.12.2 Déformation du cas $P_i = x_i^{d_i}, 1 \leq i \leq n$.

Plaçons-nous maintenant dans le cas où

$$P_i = x_i^{d_i} - Q_i\ ,\quad \deg Q_i < d_i\ ,\quad 1 \leq i \leq n. \tag{21}$$

Une base du $\mathbb{K}$-espace vectoriel quotient $B = R/(\mathbf{P})$ est formée des monômes de la forme

$$\prod_{i=1}^{n} x_i^{\alpha_i}\ ,\quad 0 \leq \alpha_i < d_i\ ,\quad 1 \leq i \leq n.$$

On note $\mathcal{B}_{\mathbf{d}}$ le sous espace vectoriel de R engendré par ces monômes. On remarque que l'on a la même base pour l'algèbre quotient que dans le cas $P_i = x_i^{d_i}, 1 \leq i \leq n$. En homogénéisant P_i, on obtient

$$P_i^t = x_i^{d_i} - t\, Q_i^t\ \ ,\ 1 \leq i \leq n.$$

Pour $t = 0, P_i^0 = x_i^{d_i}$ et pour $t = 1$, $P_i^1 = P_i$. On vérifie facilement que

$$\Phi(1, P_1^t, \ldots, P_n^t) = \Phi(1, x_1^{d_1}, \ldots, x_n^{d_n}) + tR_1 + \cdots + t^s R_s\ ,$$

où les polynômes $R_i \in \mathbb{K}[\mathbf{x},\mathbf{y}]$ sont de degrés au plus $\sum_{i=1}^{n}(d_i-1)-1 = \nu-1$. D'après (15), $R_i \triangleleft \tau_{\mathbf{x^d}} = 0, 1 \leq i \leq s$.

Proposition 4.12.5 — *Le résidu $\tau_{\mathbf{P}}$ de l'application (21) est défini par*

- $\tau_{\mathbf{P}} = 0$ sur $(\mathbf{P})$,
- $\tau_{\mathbf{P}} = \tau_{\mathbf{x^d}}$ sur $\mathcal{B}_{\mathbf{d}}$.

Preuve. Cette définition définit $\tau_{\mathbf{P}}$ sur R, car $\mathcal{B}_{\mathbf{d}} \oplus (\mathbf{P}) = R$. En utilisant (4.3.1), il suffit de vérifier que $\Phi(1, P_1, \ldots, P_n) \triangleright \tau_{\mathbf{P}} - 1 \in (\mathbf{P})$. En effet,

$$\Phi(1, P_1, \ldots, P_n) \triangleright \tau_{\mathbf{P}} = \Phi(1, x_1^{d_1}, \ldots, x_n^{d_n}) \triangleright \tau_{\mathbf{P}} + \sum_{i=1}^{s} R_i \triangleright \tau_{\mathbf{P}}.$$

En écrivant R_i sous la forme $R_i = f_i + g_i, 1 \leq i \leq n$, où $f_i = \sum_\alpha a_{i,\alpha}(\mathbf{x}) b_{i,\alpha}(\mathbf{y})$, avec $b_{i,\alpha}(\mathbf{y}) \in (\mathbf{P}(\mathbf{y}))$ et $g_i = \sum_\beta c_{i,\beta}(\mathbf{x}) d_{i,\beta}(\mathbf{y}), d_{i,\beta}(\mathbf{y}) \in \mathcal{B}_{\mathbf{d}}$; il découle de (15) et de la proposition (4.12.4) que

$$\Phi(1, P_1, \ldots, P_n) \triangleright \tau_{\mathbf{P}} = \Phi(1, x_1^{d_1}, \ldots, x_n^{d_n}) \triangleright \tau_{\mathbf{x^d}} + \sum_{i=1}^{s} g_i \triangleright \tau_{\mathbf{x^d}} = 1.$$

□

4.12.3 Le cas général

Nous considérons maintenant le cas général de la configuration où $\mathbf{P} = (P_1, \ldots, P_n)$ n'a pas de zéro à l'infini. Ce cas est important car on peut s'y ramener par l'élimination et la loi de transformation.

Théorème 4.12.6 (Euler-Jacobi) — *Soit $\mathbf{P} = (P_1, \ldots, P_n)$ une application polynomiale sans zéro à l'infini. Alors, pour tout polynôme f de degré au plus $\nu - 1$*

$$\tau_{\mathbf{P}}(f) = 0.$$

Preuve. Comme les polynômes $P_1, \ldots, P_n$ n'ont pas de zéro à l'infini, il existe alors des polynômes $R_i, S_i, 1 \leq i \leq n$, vérifiant

$$P_i = R_i - S_i \quad , \quad \deg R_i = d_i \quad , \quad \deg S_i < d_i, \quad 1 \leq i \leq n.$$

Par hypothèse, les polynômes homogènes $R_1, \ldots, R_n$ définissent l'origine; donc d'après le théorème (4.12.1), il existe des polynômes homogènes $A_{i,j}$ de degré $\nu + 1 - d_j$ tels que

$$x_i^{\nu+1} = \sum_{j=1}^{n} A_{i,j} R_j \quad , \quad 1 \leq i \leq n.$$

Posons

$$Q_i = \sum_{j=1}^{n} A_{i,j} P_j = x_i^{\nu+1} - \sum_{j=1}^{n} A_{i,j} S_j \quad , \quad 1 \leq i \leq n.$$

Les polynômes Q_i sont de la forme (21). La loi de transformation et la décomposition $R = (\mathbf{Q}) \oplus \mathcal{B}_{\nu+\mathbf{1}}$ de la section précédente (la notation $\nu + \mathbf{1}$ désigne le n-uplet $(\nu + 1, ..., \nu + 1)$) impliquent que

$$\tau_{\mathbf{P}}(f) = \tau_{\mathbf{Q}}(f \det(A_{i,j})) = \tau_{\mathbf{Q}}(f_1) + \tau_{\mathbf{Q}}(f_2) \ ,$$

où $f \det(A_{i,j}) = f_1 + f_2$, avec f_1 (resp. f_2) appartient au sous espace vectoriel $(\mathbf{Q})$ (resp. $\mathcal{B}_{\nu+\mathbf{1}}$) de R. Par suite

$$\tau_{\mathbf{P}}(f) = \tau_{\mathbf{x}^{\nu+1}}(f_2) = 0,$$

car $\deg f_2 \leq n\nu - 1$. □

Nous allons maintenant voir le lien entre les résidus de $\mathbf{P}$ et $\mathbf{R}$. Dans un premier temps, nous montrons que les $\mathbb{K}$-espaces vectoriels $R/(\mathbf{P})$et $R/(\mathbf{R})$ ont une même base.

Pour tout polynôme $h \in R$, notons $\mathrm{In}(h)$ la composante homogène de plus haut degré de h, et pour tout idéal I de R, $\mathrm{In}(I)$ l'idéal engendré par $\mathrm{In}(h)$ pour tout $h \in I$.

Lemme 4.12.7 — *Si les polynômes $P_1, \ldots, P_n$ n'ont pas de zéro à l'infini, alors l'idéal* $\mathrm{In}((\mathbf{P})) = (\mathrm{In}(P_1), \ldots, \mathrm{In}(P_n))$.

Preuve. Les polynômes $R_i, 1 \leq i \leq n$, définissent comme seul point l'origine; ils forment donc une suite quasi-régulière. Supposons qu'il existe un polynôme $h \in (\mathbf{P})$ tel que $\mathrm{In}(h) \notin (R_1, \ldots, R_n)$. Nous avons une écriture de la forme

$$h = \sum_{i=1}^{n} H_i P_i = \sum_{i=1}^{n} H_i R_i - \sum_{i=1}^{n} H_i S_i \quad , \quad H_i \in \mathbb{K}[\mathbf{x}].$$

Notons p le plus petit indice tel que $H_p P_p$ soit de degré maximum. Supposons que parmi tous les $h \in (\mathbf{P})$ tels que $\mathrm{In}(h) \notin (R_1, \ldots, R_n)$, ce degré soit minimal; et une fois ce degré fixé, p soit maximal.

Comme $\mathrm{In}(h) \notin (R_1, \ldots, R_n)$, $\sum_{i=p}^{n} \tilde{H}_i R_i = 0$, avec $\tilde{H}_i = In(H_i)$, si $\deg H_i P_i = \deg H_p P_p$, et $\tilde{H}_i = 0$ si $\deg H_i P_i \neq \deg H_p P_p$. Puisque $(R_1, \ldots, R_n)$ est une suite quasi-régulière $\tilde{H}_p \in (R_{p+1}, \ldots, R_n)$. Donc, il existe des polynômes homogènes $K_i, p+1 \leq i \leq n$, vérifiant $\tilde{H}_p = \sum_{i=p+1}^{n} K_i R_i$. Par suite,

$$\begin{aligned} h &= \sum_{i=1}^{n} H_i P_i - \sum_{i=p+1}^{n} P_p K_i P_i + \sum_{i=p+1}^{n} P_p K_i P_i \\ &= \sum_{i=1}^{p-1} H_i P_i + (H_p - \sum_{i=p+1}^{n} K_i P_i) P_p + \sum_{i=p+1}^{n} (H_i + K_i P_p) P_i. \end{aligned}$$

Nous avons $h = \sum_{i=1}^{n} H_i' P_i$, avec soit $\max_i \deg(H_i' P_i)$ plus petit, soit le premier indice où ce maximum est atteint plus grand. Ceci contredit les hypothèses faites sur h; donc pour tout $h \in R$, $\mathrm{In}(h) \in (R_1, \ldots, R_n)$. □

Comme $R/(\mathbf{P})$ et $R/(\mathrm{In}(\mathbf{P}))$ sont isomorphes comme $\mathbb{K}$-espaces vectoriels, ils ont les mêmes bases. Notons $\mathcal{B}$ le sous espace vectoriel de R engendré par les éléments d'une base commune à $R/(\mathbf{P})$ et $R/(\mathrm{In}(\mathbf{P}))$. On a la décomposition $R = \mathcal{B} \oplus (\mathbf{P})$. Nous pouvons donc réduire tout polynôme de R par les relations $R_i \to S_i$ en une forme normale $\in \mathcal{B}$. Voir [10] pour plus d'information.

De la même façon que précédemment (cette fois-ci la base n'est pas forcément monomiale, mais la propriété sur les degrés est conservée), on montre

Théorème 4.12.8 — *Le résidu $\tau_{\mathbf{P}}$ de l'application polynomiale $\mathbf{P}$ sans zéro à l'infini est défini par*

- $\tau_{\mathbf{P}} = 0$ sur $(\mathbf{P})$,
- $\tau_{\mathbf{P}} = \tau_{\mathbf{R}}$ sur $\mathcal{B}$.

Le résultat suivant décrit le résidu de l'application $\mathbf{P}$ en fonction des résidus itérés de $\mathbf{R}$. Cette formule a un équivalent analytique qui consiste à faire un développement en séries sous l'intégrale et à échanger les signes «somme» (voir [4]). Des connexions ont été établies dans [8], entre ce développement en séries et la mise sous forme normale d'un polynôme par une base de Gröbner. Nous explicitons ici ces connections en montrant (simplement et sans utiliser d'analyse) comment ce développement en

série, n'est qu'une réécriture d'un procédé de réduction par rapport aux polynômes initiaux.

Théorème 4.12.9 — *Le résidu $\tau_{\mathbf{P}}$ est aussi donné par la formule*

$$\tau_{\mathbf{P}} = \sum_{\beta\in\mathbb{N}^n} \mathbf{S}^\beta \cdot \tau_{\mathbf{R}^{\beta+1}} \tag{22}$$

où $\mathbf{1} = (1,\ldots,1)$ et pour tout multi-indice $\beta = (\beta_1,\ldots,\beta_n), \mathbf{S}^\beta = S_1^{\beta_1}\cdots S_n^{\beta_n}$.

Remarquons que si $f \in R$, d'après (4.12.6)

$$\tau_{\mathbf{P}}(f) = \sum_{\beta\in\mathbb{N}^n : \sum_i \beta_i(\deg P_i - \deg S_i)\le \deg f-\nu} \tau_{\mathbf{R}^{\beta+1}}(f\mathbf{S}^\beta).$$

Preuve. Soit $p \in R$ de la forme $p = \tilde{p}\,\mathbf{R}^\alpha$, on a d'après le corollaire (4.6.3) et avec $\tau_{\mathbf{R}^{\beta-\alpha+1}} = 0$ si $\beta-\alpha$ n'est pas dans $\mathbb{N}^n$,

$$\begin{aligned}\mathbf{S}^\beta \cdot \tau_{\mathbf{R}^{\beta+1}}(p) &= \mathbf{S}^\beta \cdot \tau_{\mathbf{R}^{\beta-\alpha+1}}(\tilde{p}) \\ &= \tau_{\mathbf{R}^{\beta-\alpha+1}}(\mathbf{S}^\beta\,\tilde{p}) \\ &= \mathbf{S}^{\beta-\alpha}\cdot\tau_{\mathbf{R}^{\beta-\alpha+1}}(\tilde{p}\,\mathbf{S}^\alpha)\ ,\end{aligned}$$

où $r = \tilde{p}\mathbf{S}^\alpha$ est la réduction de p par rapport aux polynômes $P_1,\ldots,P_n$. Ceci montre que

$$\sum_{\beta\in\mathbb{N}^n} \mathbf{S}^\beta\cdot\tau_{\mathbf{R}^{\beta+1}}(p) = \sum_{\beta-\alpha\in\mathbb{N}^n} \mathbf{S}^{\beta-\alpha}\cdot\tau_{\mathbf{R}^{\beta-\alpha+1}}(r) = \sum_{\beta\in\mathbb{N}} \mathbf{S}^\beta\cdot\tau_{\mathbf{R}^{\beta+1}}(r).$$

En particulier $\sum_{\beta\in\mathbb{N}^n}\mathbf{S}^\beta\cdot\tau_{\mathbf{R}^{\beta+1}} = 0$ sur $(\mathbf{P})$. En utilisant la décomposition $R = \mathcal{B}\oplus(\mathbf{P})$, nous avons pour tout polynôme p

$$\sum_{\beta\in\mathbb{N}^n}\mathbf{S}^\beta\cdot\tau_{\mathbf{R}^{\beta+1}}(p) = \sum_{\beta\in\mathbb{N}^n}\mathbf{S}^\beta\cdot\tau_{\mathbf{R}^{\beta+1}}(p_{\mathrm{red}}) = \tau_{\mathbf{R}}(p_{\mathrm{red}}) + \sum_{\beta\in(\mathbb{N}^*)^n}\tau_{\mathbf{R}^{\beta+1}}(\mathbf{S}^\beta p_{\mathrm{red}})\ ,$$

où $p = p_{\mathrm{red}} + q$, avec $p_{\mathrm{red}} \in \mathcal{B}$ et $q \in (\mathbf{P})$. Nous savons, d'après (4.12.8), que $\tau_{\mathbf{P}}(p) = \tau_{\mathbf{R}}(p_{\mathrm{red}})$.

D'après le théorème (4.12.1), tout monôme m de degré plus grand que $\nu+1$ est dans l'idéal homogène engendré par $R_1,\ldots,R_n$; m peut donc être réduit par les polynômes $P_1,\ldots,P_n$. Par conséquent, le degré de p_{red} est au plus ν. Par suite, pour $\beta\in(\mathbb{N}^*)^n$, le degré de $\mathbf{S}^\beta p_{\mathrm{red}}$ est inférieur ou égal à $\sum_{i=1}^n d_i\,\beta_i + \nu - \mathbf{1}$. Comme le résidu $\tau_{\mathbf{R}^\beta}$ est nul sur tout polynôme de degré $\le \sum_{i=1}^n d_i\,\beta_i + \nu - \mathbf{1}$, nous en déduisons

$$\sum_{\beta\in\mathbb{N}^n}\mathbf{S}^\beta\cdot\tau_{\mathbf{R}^{\beta+1}}(p) = \tau_{\mathbf{R}}(p_{\mathrm{red}}).$$

Or, d'après le théorème (4.12.8)

$$\sum_{\beta\in\mathbb{N}^n} \mathbf{S}^\beta \cdot \tau_{\mathbf{R}^{\beta+\mathbf{1}}}(p) = \tau_{\mathbf{R}}(p_{\mathrm{red}}) = \tau_{\mathbf{P}}(p_{\mathrm{red}}) = \tau_{\mathbf{P}}(p).$$

□

Dans le cas $R_i = x_i^{d_i}, 1 \leq i \leq n$, la formule (22) montre que le résidu d'un polynôme p est un coefficient de la forme normale de p après réduction par les polynômes $P_1, \ldots, P_n$. Pour plus de détail sur ce point, voir [8]. Dans ce cas $\tau_{\mathbf{R}^{\beta+\mathbf{1}}}(f)$ est le coefficient de $\mathbf{x}^{\mathbf{d}\,(\beta+\mathbf{1})-\mathbf{1}}$ dans f. C'est aussi le coefficient de $\mathbf{x}^{\mathbf{d}-\mathbf{1}}$ dans $\frac{f}{\mathbf{x}^{\mathbf{d}\,\beta}}$ et la formule précédente se simplifie ($\mathbf{d}\,\beta = (d_1\,\beta_1, \ldots, d_n\,\beta_n)$).

Corollaire 4.12.10 — *Dans le cas où $R_i = x_i^{d_i}, 1 \leq i \leq n$, le résidu de $f \in R$ est le coefficient de $x_1^{d_1-1} \cdots x_n^{d_n-1}$ dans*

$$\sum_{\beta\in\mathbb{N}^n} f\,\left(\frac{\mathbf{S}}{\mathbf{x}^{\mathbf{d}}}\right)^\beta.$$

Ceci revient à faire le développement en séries de la fraction rationnelle

$$\frac{x_1 \cdots x_n\, f}{\prod_{i=1}^n x_i^{d_i}\,(1-\frac{S_i}{x_i^{d_i}})},$$

et à prendre le coefficient constant comme résidu de f. Nous en déduisons le corollaire suivant.

Corollaire 4.12.11 — *La fraction*

$$\frac{x_1 \cdots x_n}{\prod_{i=1}^n x_i^{d_i}\,(1-\frac{S_i}{x_i^{d_i}})}$$

admet un développement en série de la forme

$$\sum_{\mathbf{a}\in\mathbb{N}^n} \frac{\tau(\mathbf{x}^{\mathbf{a}})}{\mathbf{x}^{\mathbf{a}}} + \rho$$

avec $\rho \notin \mathbb{K}[x_1^{-1}, \ldots, x_n^{-1}]$.

4.12.4 Passage du cas sans zéro à l'infini au cas homogène

Nous allons montrer que le résidu d'une application polynomiale sans zéro à l'infini se ramène, quitte à ajouter une variable, au calcul du résidu d'une application polynomiale homogène, qui peut être calculer, comme nous l'avons vu dans la sous section (4.12.1), en résolvant un système linéaire de taille raisonnable.

Théorème 4.12.12 — *Soient $P_1, \ldots, P_n$ des polynômes de $\mathbb{K}[\mathbf{x}]$ sans zéro à l'infini; alors pour tout multi-indice $\alpha \in \mathbb{N}^n$ tel que $|\alpha| \geq \nu$,*

$$\tau_{\mathbf{P}}(\mathbf{x}^\alpha) = \tau_{({}^hP_1,\ldots,{}^hP_n,x_0^{|\alpha|-\nu+1})}(\mathbf{x}^\alpha) \ ,$$

où ${}^hP_i$ désigne l'homogénéisé de $P_i, 1 \leq i \leq n$.

Preuve. En utilisant la même idée que dans la preuve du corollaire (4.7.1), on peut écrire tout polynôme f de $\mathbb{K}[\mathbf{x}]$ sous la forme ${}^hf = f + (x_0 - 1)g$, avec $g \in \mathbb{K}[x_1, \ldots, x_n, x_0]$. Donc

$$\begin{pmatrix} {}^hP_1 \\ \vdots \\ {}^hP_n \\ x_0 - 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & g_1 \\ \vdots & \ddots & \cdots & \vdots \\ 0 & \cdots & 1 & g_n \\ 0 & \cdots & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} P_1 \\ \vdots \\ P_n \\ x_0 - 1 \end{pmatrix}$$

D'après la preuve du théorème (4.7.1), la loi de transformation et la formule (22),

$$\begin{aligned} \tau_{\mathbf{P}}(\mathbf{x}^\alpha) &= \tau_{(\mathbf{P},x_0-1)}(\mathbf{x}^\alpha) \\ &= \tau_{({}^hP_1,\ldots,{}^hP_n,x_0-1)}(\mathbf{x}^\alpha) \\ &= \sum_{\gamma\in\mathbb{N}} \tau_{({}^hP_1,\ldots,{}^hP_n,x_0^{\gamma+1})}(\mathbf{x}^\alpha) \\ &= \tau_{({}^hP_1,\ldots,{}^hP_n,x_0^{|\alpha|-\nu+1})}(\mathbf{x}^\alpha). \end{aligned}$$

□

Voir aussi [27], pour une autre démonstration, consistant à homogénéiser, puis à faire tendre le paramètre vers 0, et ([32]) pour une preuve analytique.

4.12.5 Théorème de Bézout

Le lemme (4.12.3) nous permet de déduire le théorème de Bézout (pour $car(\mathbb{K}) = 0$ ou $car(\mathbb{K}) > \dim_{\mathbb{K}}(R/(\mathbf{P}))$.

Théorème 4.12.13 — *Soient $P_1, \ldots, P_n$ des polynômes sans zéro à l'infini; alors*

$$\dim_{\mathbb{K}}(R/(\mathbf{P})) = \prod_{i=1}^{n} d_i.$$

Preuve. D'après le lemme (4.12.3), $\mathrm{In}(\mathbf{P}) = (R_1, \ldots, R_n)$, où $R_i = In(P_i), 1 \leq i \leq n$, on a donc $\dim_{\mathbb{K}}(R/(\mathbf{P})) = \dim_{\mathbb{K}}(R/\mathrm{In}(\mathbf{P})) = \dim_{\mathbb{K}}(R/(\mathbf{R}))$. D'après l'identité d'Euler

$$\begin{cases} d_1 R_1 = d_{x_1}(R_1)\, x_1 + \cdots + d_{x_n}(R_1)\, x_n \\ \vdots \\ d_n R_n = d_{x_1}(R_n)\, x_1 + \cdots + d_{x_n}(R_n)\, x_n \end{cases}$$

D'après la loi de transformation

$$\tau_{\mathbf{x}} = \frac{1}{\prod_{i=1}^{n} d_i} J_{\mathbf{R}} \cdot \tau_{\mathbf{R}} \ ,$$

où $J_{\mathbf{R}}$ désigne le jacobien de $\mathbf{R}$. En utilisant (4.5.2)

$$\prod_{i=1}^{n} d_i = \left(\prod_{i=1}^{n} d_i \right) \tau_{\mathbf{x}}(1) = \tau_{\mathbf{R}}(J_{\mathbf{R}}) = \dim_{\mathbb{K}}(R/(\mathbf{R})) = \dim_{\mathbb{K}}(R/(\mathbf{P})).$$

□

Corollaire 4.12.14 — *Soient $P_1, \ldots, P_n$ des polynômes homogènes définissant une variété discrète de $\mathbb{P}^n(\mathbb{K})$; alors le nombre de racines communes (en comptant les multiplicités) à $P_1, \ldots, P_n$ est* $\deg P_1 \cdots \deg P_n$.

Preuve. On peut choisir les coordonnées homogènes $(x_0, \ldots, x_n)$ de $\mathbb{P}^n(\mathbb{K})$ pour que l'hyperplan à l'infini ne contienne pas de zéro de $\mathbf{P}$. Posons

$$\tilde{P}_i(\mathbf{x}) = P_i(1, x_1, \ldots, x_n) \quad , \quad 1 \leq i \leq n.$$

Les polynômes $\tilde{P}_1, \ldots, \tilde{P}_n$ n'ont pas de zéro à l'infini, et sont de degrés $\deg P_1, \ldots, \deg P_n$. D'après le théorème (4.12.13)

$$\begin{aligned} &\mathrm{card}\{[x_0, \ldots, x_n] \in \mathbb{P}^n(\mathbb{K}) : P_i(x_0, \ldots, x_n) = 0, 1 \leq i \leq n\} \\ &= \quad \dim_{\mathbb{K}} R/(\tilde{\mathbf{P}}) = \deg P_1 \ldots \deg P_n. \end{aligned}$$

□

Corollaire 4.12.15 — *Soient $P_1, \ldots, P_n$ des polynômes de $\mathbb{K}[\mathbf{x}]$ définissant une variété V discrète; alors le cardinal de V (en comptant les multiplicités) est au plus* $\deg P_1 \ldots \deg P_n$.

Preuve. (Voir [4]). Posons $P_{c,i} = cx_i^{ed_i+1} + P_i^e, 1 \leq i \leq n$, où $c \in \mathbb{K}$ et e un entier. D'après le théorème (4.12.13), le nombre de zéros de $P_c = (P_{c,1}, \ldots, P_{c,n})$ est $(ed_1 + 1) \ldots (ed_n + 1)$. Lorsque c tend vers zéro, certaines racines de P_c tendent vers les racines de $(P_1^e, \ldots, P_n^e)$, et les autres partent à l'infini, donc

$$e^n \operatorname{card}\{z \in \mathbb{K}^n : P_i(z) = 0, 1 \leq i \leq n\} \leq (ed_1 + 1) \ldots (ed_n + 1).$$

En choisissant l'entier e suffisament grand, il s'ensuit

$$\operatorname{card} V \leq \deg P_1 \ldots \deg P_n.$$

□

5 Le cas local

Nous nous plaçons dans le cas d'un système de polynômes $P_1, \ldots, P_n$ définissant un point isolé ζ. On suppose que ζ est l'origine de $\mathbb{K}^n$ (i.e. dans l'anneau local

$$R_0 = \{\frac{f}{g},\ f, g \in R,\ g(0) \neq 0\},$$

la suite $P_1, \ldots, P_n$ est régulière). Notons $(\mathbf{P})$ l'idéal engendré par $P_1, \ldots, P_n$ dans R, Q_0 la composante primaire de $(\mathbf{P})$ associée à l'idéal maximal $\mathbf{m}$ définissant l'origine, $B_0 = R/Q_0$ et $\mathcal{B}_0 = R_0/(\mathbf{P})R_0 = R_0/Q_0R_0$.

5.1 Caractérisation du résidu local

En appliquant les résultats des sections 3.2, 3.5 et 4.3 au cas où $P_1, \ldots, P_n$ est une suite régulière dans l'anneau R_0, nous obtenons le résultat suivant.

Théorème 5.1.1 — *Sous les hypothèses précédentes, l'application $\Delta = \Phi(1, P_1, \ldots, P_n)$ définit un isomorphisme entre $\hat{\mathcal{B}}_0$ et $\mathcal{B}_0$.*

Définition 5.1.1 — *On appelle résidu local de l'application polynomiale $\mathbf{P}$ au point 0 l'unique forme linéaire $\tau_{\mathbf{P}}$ définie sur $\mathcal{B}_0$ telle que $\Delta(\tau_{\mathbf{P}}) \equiv 1$.*

Dans le cas où $\mathbb{K} = \mathbb{C}$, en utilisant la formule de Weil, on voit que ce résidu local coïncide avec le résidu local analytique défini par l'intégrale d'une n-forme méromorphe sur un cycle autour de 0 (voir [15], [4]).

Le système inverse de Q_0 est donc engendré par le résidu local et ses dérivations

$$Q_0^{\perp} = \langle\langle \tau_{\mathbf{P}} \rangle\rangle.$$

5.2 Construction du résidu local

Connaissant le système inverse donné par la méthode proposée dans la section 2.5.3, il est facile de construire le résidu local.

Entrée : $\mathbf{P} = (P_1, \ldots, P_n) \in R^n$ définissant une suite quasi-régulière et ζ tel que $(\mathbf{P}) \subset \mathbf{m}_\zeta$.
Sortie : Le résidu $\tau_{\mathbf{P}}$ de $\mathbf{P}$ en ζ.

- ▷ Construire une base $\beta_1, \ldots, \beta_\mu$ de $(\mathbf{P})^{\perp} \cap \mathbb{K}[\partial_\zeta]$ avec l'algorithme (2.5.3).
- ▷ Résoudre le système
  $$\beta_j(\textstyle\sum_{l=1}^{\mu} \lambda_l \, \Delta(\beta_l) - 1) = 0, \ 1 \leq j \leq \mu.$$
- ▷ Le résidu $\tau_{\mathbf{P}}$ est $\sum_{l=1}^{\mu} \lambda_l \, \beta_l$ ou $(\lambda_l)_l$ est solution du système précédent.

Comme nous l'avons vu en (2.3.3), il existe N tel que $\mathbf{m}^{N+1} \subset Q_\zeta$ et $\mathbf{m}^N \not\subset Q_\zeta$. Cet entier N est aussi le maximum des degrés des éléments de $D_\zeta = (P)^{\perp} \cap \mathbb{K}[\partial_\zeta]$. Comme D_ζ est engendré par un polynôme (le résidu local en ζ) et ses dérivées, N est le degré du résidu.

Il est facile de construire une base monomiale du quotient, à partir du résidu. Il suffit de le dériver et puis d'en extraire une base ($\beta_i = m_i \cdot \tau$) où les m_i sont des monômes. On vérifie alors que (m_i) est une base monomiale de B_0.

5.3 Exemple de construction d'une base du quotient

On considère les polynômes de l'exemple (2.5.2). Le polynôme $\Delta \in \mathbb{K}[\mathbf{x}, \mathbf{y}]$ est

$$\begin{aligned}
&10\,{x_2}^5 + 25\,{x_1}^3\,{x_2}^3 + \left(10\,{x_2}^3 + 25\,{x_1}^3\,x_2\right)\,{y_2}^2 \\
&\quad + \left(10\,{x_2}^4 + 25\,{x_1}^3\,{x_2}^2\right)\,y_2 + \left(25\,{x_1}^2\,{x_2}^3 - 4\,x_1\,{x_2}^2\right)\,y_1 \\
&\quad + \left(-4\,x_2 + 25\,x_1\,{x_2}^2\right)\,{y_1}^2\,y_2 + \left(25\,{x_1}^2\,{x_2}^2 - 4\,x_1\,x_2\right)\,y_1\,y_2 \\
&\quad + \left(10\,{x_1}^3 + 25\,x_1\,{x_2}^3\right)\,{y_1}^2 + \left(10\,{x_2}^2 + 25\,{x_1}^3\right)\,{y_2}^3 \\
&\quad + \left(25\,{x_2}^3 + 10\,{x_1}^2\right)\,{y_1}^3 + 25\,{x_1}^2\,y_1\,{y_2}^3 + 25\,x_1\,{y_1}^2\,{y_2}^3
\end{aligned}$$

$$+ 25\,{x_1}^2\,x_2\,y_1\,{y_2}^2 + 25\,x_2{}^2\,{y_1}^3\,y_2 + 25\,{y_2}^2\,x_2\,{y_1}^3$$
$$+ 25\,x_1\,x_2\,{y_2}^2\,{y_1}^2 + 10\,x_1\,{y_1}^4 + 25\,{y_1}^3\,{y_2}^3 + 10\,{y_1}^5.$$

Le résidu local $\tau_{\mathbf{P}}$ est de la forme

$$u_1 + u_2\,\mathbf{d}_1 + u_3\,\mathbf{d}_2 + u_4\,{\mathbf{d}_1}^2 + u_5\,{\mathbf{d}_2}^2 + u_6\,\mathbf{d}_1\,\mathbf{d}_2 + u_7\,{\mathbf{d}_2}^3 + u_8\,{\mathbf{d}_1}^3$$
$$+ u_9\,\left(5\,\mathbf{d}_1\,{\mathbf{d}_2}^2 - 2\,{\mathbf{d}_1}^4\right) + u_{10}\,\left(5\,{\mathbf{d}_1}^2\,\mathbf{d}_2 - 2\,{\mathbf{d}_2}^4\right)$$
$$+ u_{11}\,\left(5\,{\mathbf{d}_1}^2\,{\mathbf{d}_2}^2 - 2\,{\mathbf{d}_1}^5 - 2\,{\mathbf{d}_2}^5\right),$$

et satisfait

$$\begin{aligned} -20\,u_{11} - 1 = -20\,u_9 = -20\,u_{10} = 10\,u_8 = 10\,u_7 \\ = \quad 125\,u_{11} - 4\,u_6 = 10\,u_5 + 25\,u_8 = 10\,u_4 + 25\,u_7 \\ = \quad -20\,u_2 + 625\,u_{10} = 625\,u_9 - 20\,u_3 = -20\,u_1 + 125\,u_6 = 0, \end{aligned}$$

ce qui donne

$$\tau_{\mathbf{P}} = -\frac{625}{64} - \frac{25}{16}\,\mathbf{d}_1\,\mathbf{d}_2 - \frac{1}{4}\,{\mathbf{d}_1}^2\,{\mathbf{d}_2}^2 + \frac{1}{10}\,{\mathbf{d}_1}^5 + \frac{1}{10}\,{\mathbf{d}_2}^5.$$

En calculant la valeur de $\tau_{\mathbf{P}}$ en le Jacobien de p_1, p_2, qui est égal à: $-12\,{x_1}^2\,{x_2}^2 + 40\,{x_2}^5 + 40\,{x_1}^5 + 400\,{x_1}^3\,{x_2}^3$, on obtient $(-12) \times (-\frac{1}{4}) + 40 \times \frac{1}{10} + 40 \times \frac{1}{10} = 11$. Donc la multiplicité de 0 (ou la dimension de $B_0 = R/Q_0$) est bien 11, comme nous l'avons vu dans l'exemple 2.5.2.

Une base du quotient est donc d'après ci-dessus,

$$x_1^5, x_1^4, x_1^3, x_1^2, x_1, 1, x_2, x_1\,x_2, x_2^2, x_2^3, x_2^4$$

5.4 Socle et résidu

Définition 5.4.1 — *On appelle* socle *de B_0 l'idéal*

$$Ann_{B_0}(\mathbf{m}) = \{f \in B_0;\ \forall i = 1 \ldots n,\ x_i f \equiv 0\}.$$

Le socle de B_0 est aussi $(Q_0 : \mathbf{m})/Q_0$. Si $Q_0^\perp$ est engendré par le résidu τ, c'est aussi d'après la section 3.4

$$\{f \in B_0;\ \forall p \in \mathbf{m},\ \tau(f\,p) = 0\}.$$

D'après la proposition (2.2.7),

$$(Q_0 : \mathbf{m})^\perp = \langle\langle x_1 \cdot \tau, \ldots, x_n \cdot \tau \rangle\rangle$$

est un espace vectoriel de dimension $\mu-1$, avec $\mu = \dim_{\mathbb{K}}(Q_0^{\perp})$. Par suite, $R/(Q_0 : \mathbf{m})$ est un $\mathbb{K}$-espace vectoriel de dimension $\mu - 1$. De la suite exacte

$$0 \to (Q_0 : \mathbf{m})/Q_0 \to R/Q_0 \to R/(Q_0 : \mathbf{m}) \to 0,$$

on déduit que $Ann_{B_0}(\mathbf{m}) = (Q_0 : \mathbf{m})/Q_0$ est un espace vectoriel de dimension 1.

Proposition 5.4.1 — *Soit $\mathbb{K}$ un corps de caractéristique nulle ou supérieure à la dimension de B_0; alors le socle de B_0 est engendré par le jacobien J de $\mathbf{P}$.*
Preuve. Il suffit de vérifier que le jacobien est un élément non nul de $Ann_{B_0}(\mathbf{m})$. D'après le théorème (4.5.1), pour tout $p \in R$

$$\tau(J\,p) = J \cdot \tau(p) = Tr(p).$$

Si le polynôme p est de la forme $x_i q$, les valeurs propres de l'opérateur de multiplication par p dans B_0 sont nulles et sa trace aussi. Donc

$$\forall q \in R,\ \forall i = 1 \ldots n,\ \tau(x_i J\,q) = 0.$$

Comme la forme bilinéaire définie par τ est non dégénérée, $x_i J \equiv 0$ dans B_0, et $J \in Ann_{B_0}(\mathbf{m})$. D'après le corollaire (4.5.2), $\tau(J) = \dim_{\mathbb{K}}(B_0) \neq 0$, et $J \not\equiv 0$ dans B_0. □

Il est assez facile de construire d'autres générateurs de $Ann_{B_0}(\mathbf{m})$ de la façon suivante: notons N le degré du résidu en ∂ et prenons un monôme M de τ de degré N. Notons m le monôme de $\mathbb{K}[\mathbf{x}]$ obtenu en remplaçant ∂ par $\mathbf{x}$ dans M.

On voit que $\tau(m) \neq 0$, donc $m \not\equiv 0$ dans B_0. De plus, pour tout élément p non-nul de $\mathbf{m}$, le polynôme $m\,p$ est de valuation strictement plus grande que N, donc $\tau(m\,p) = 0$ et $m \in Ann_{B_0}(\mathbf{m})$. Nous avons la proposition suivante vraie en caractéristique quelconque.

Proposition 5.4.2 — *Le socle de B_0 est engendré par tout monôme de degré maximal, qui apparaît dans le polynôme obtenu en substituant ∂ par $\mathbf{x}$ dans l'expression du résidu local τ.*

Dans l'exemple 5.3, le socle est donc engendré par x_1^5 ou x_2^5 ou même $x_1^5 + \lambda\,x_2^5$, avec $\lambda \neq -1$.

Remerciements

Nous tenons à remercier J-P. Cardinal, Y. Pitteloud, M-F. Roy et C. Walter pour les discussions et remarques durant la rédaction de ce rapport.

Références

[1] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

[2] E. Becker, J.P. Cardinal, M.F. Roy, and Z. Szafraniec. Multivariate Bezoutians, Kronecker symbol and some applications to Real Geometry. In *Effective Methods in Algebraic Geometry (MEGA)*, Progress in Math. Birkhäuser, 1994. to appear.

[3] C. A. Berenstein and A. Yger. Bezout identities in $\mathbb{Q}[z_1, \ldots, z_n]$. *Acta. Math.*, 166:69–120, 1991.

[4] C.A. Berenstein, R. Gay, A. Vidras, and A. Yger. *Residue Currents and Bezout Identities*, volume 114 of *Prog. in Math.* Birkhäuser, 1993.

[5] E. Bézout. *Théorie générale des Equations Algébriques.* Paris, 1779.

[6] J. Canny and I. Emiris. An efficient algorithm for the sparse mixed resultant. In G. Cohen, T. Mora, and O. Moreno, editors, *Proc. Intern. Symp. Applied Algebra, Algebraic Algor. and Error-Corr. Codes, LNCS 263*, pages 89–104, Puerto Rico, 1993. Springer Verlag.

[7] J.P. Cardinal. *Dualité et algorithmes itératifs pour la résolution de systèmes polynomiaux.* PhD thesis, Univ. de Rennes, 1993.

[8] E. Cattani, A. Dickenstein, and B. Sturmfels. Computing multidimensional residues. In *Effective Methods in Algebraic Geometry (MEGA)*, Progress in Math, Santander (Spain), 1994. Birkhäuser.

[9] A.L. Dixon. The eliminant of three quantics in two independent variables. *Proc. of Lond. Math. Society*, 6:49–69,473–492, 1908.

[10] D. Eisenbud. *Commutative Algebra with a view toward Algebraic Geometry*, volume 150 of *Graduate Texts in Math.* Springer-Verlag, 1994.

[11] M. Elkadi. Bornes pour les Degrés et les Hauteurs dans le Problème de Division. *Michigan Math. J.*, 40:609–618, 1993.

[12] M. Elkadi. Résidu de Grothendieck et forme de Chow. *Publ. math.*, 38:381–393, 1994.

[13] J. Emsalem. Géométrie des points épais. *Bull. Soc. Math. France*, 106:399–416, 1978.

[14] N. Fitchas, M. Giusti, and M. Smietanski. Sur la complexité du théorème des zéros. In J. Gudatt, editor, *Proc. of the second. Int. Conf. on Approximation and Optimization*, Peter Lang Verlag, La Habana, 1993. (to appear).

[15] Ph. Griffiths and J. Harris. *Principles of Algebraic Geometry.* Wiley Interscience Pub., 1978.

[16] W. Gröbner. *Algebrische Geometrie II*, volume 737 of *Bib. Inst. Mannheim.* Hochschultaschenbücher, 1970.

[17] A.S. Householder. Bezoutians, elimination and localization. *SIAM Review*, 12(1):73–78, 1970.

[18] J.P. Jouanolou. Le formalisme du résultant. *Adv. in Math.*, 90(2):117–263, 1991.

[19] E. Kunz. *Kähkler differentials.* Advanced lectures in Mathematics. Friedr. Vieweg and Sohn, 1986.

[20] S. Lang. *Algebra.* Addison-Wesley, 1980.

[21] F.S. Macaulay. Some formulae in elimination. *Proc. London Math. Soc.*, 1(33):3–27, 1902.

[22] F.S. Macaulay. *The Algebraic Theory of Modular Systems*, volume 19 of *Cambridge tracts in Math. and Math. Physics.* Stechert-Hafner Service Agency, 1964.

[23] M.G Marinari, T. Mora, and H.M. Möller. Grobner duality and multiplicities in polynomial system solving. In A.H.M. Levelt, editor, *ISSAC'95*, pages 167–179. ACM Press, 1995.

[24] H. Matsumura. *Commutative Algebra.* Mathematics Lecture Notes Series. The Benjamin/Cummings Publishing Company, 1980.

[25] J.M. Ortega and W.G. Rheinboldt. *Iterative solution of nonlinear equations in several variables.* Computer Science and Applied Mathematics. Academic Press, 1970.

[26] P. S. Perdersen. A Basis for Polynomial Solutions to Systems of Linear Constant Coefficient PDE's. *Adv. In Math.*, 117:157–163, 1996.

[27] M.F. Roy and A. Szpirglas. Bezoutiens et résidus. Prépublication de l'Univ. Paris XIII, 1996.

[28] J. Sabia and P. Solerno. Bounds for traces in complete intersections and degree in the nullstellenstaz. *AAECC*, 1995. (to appear).

[29] G. Scheja and U. Storch. Über Spurfunktionen bei vollständigen Durschnitten. *Journal Reine Angew Mathematik*, 278:174–190, 1975.

[30] B.L. Van der Waerden. *Modern algebra Vol II.* Frederick Ungar Publishing Co, 1948.

[31] W. Wolfe. The secant method for simultaneous nonlinear equations. *Comm. ACM*, 2, 1959.

[32] H. Zhang. Some computations of residues. (preprint), 1996.

Unité de recherche INRIA Lorraine, Technopôle de Nancy-Brabois, Campus scientifique,
615 rue du Jardin Botanique, BP 101, 54600 VILLERS LÈS NANCY
Unité de recherche INRIA Rennes, Irisa, Campus universitaire de Beaulieu, 35042 RENNES Cedex
Unité de recherche INRIA Rhône-Alpes, 46 avenue Félix Viallet, 38031 GRENOBLE Cedex 1
Unité de recherche INRIA Rocquencourt, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex
Unité de recherche INRIA Sophia-Antipolis, 2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS Cedex

Éditeur
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
ISSN 0249-6399