Résolution des systèmes zéro-dimensionnels

Fabrice Rouillier[1]

IRMAR, Université de Rennes I
Campus de Beaulieu
Avenue des Buttes de Coesme
35042 Rennes cedex
rouillie@posso.univ-rennes1.fr

[1]avec le soutien du projet européen ESPRIT BRA contract 6846 POSSO.

Contents

1 Préliminaires

Nous introduisons dans cette partie les résultats élémentaires qui seront à la base de nos algorithmes.

Soient K un corps ordonné de clôture algébrique C, $S \subset K[X_1, \ldots, X_n]$ un système polynômial engendrant un idéal que nous noterons $\mathcal{I}$. Rappelons que l'ensemble des zéros $V(\mathcal{I}) \subset C^n$ de $\mathcal{I}$ est fini si et seulement si le K-espace vectoriel $K[X_1, \ldots, X_n]/\mathcal{I}$ est de dimension finie. Dans ce cas, $C[X_1, \ldots, X_n]/\mathcal{I} = \prod_{\alpha \in V(\mathcal{I})} A_\alpha$ où A_α est le localisé de $C[X_1, \ldots, X_n]/\mathcal{I}$ en α. Le localisé A_α est alors un C-espace vectoriel dont la dimension est égale, par définition, à la multiplicité de α que nous noterons $\mu(\alpha)$. Le système initial étant dans $K[X_1, \ldots, X_n]$, on peut montrer aisément que $dim_K(K[X_1, \ldots, X_n]/\mathcal{I}) = dim_C(C[X_1, \ldots, X_n]/\mathcal{I})$, en utilisant, par exemple, le fait que les calculs effectués dans l'algorithme de

Buchberger (calcul d'une base de Groebner de $\mathcal{I}$) sont tous dans $K[X_1, \ldots, X_n]$. Quelques unes de ces propriétés peuvent être résumées par la proposition suivante :

Proposition 1.1 *Soit $\mathcal{I}$ un idéal de $K[X_1, \ldots, X_n]$ admettant un nombre fini de zéros. Alors :*

$$dim_K(K[X_1, \ldots, X_n]/\mathcal{I}) = dim_C(C[X_1, \ldots, X_n]/\mathcal{I}) = \sum_{\alpha \in V(\mathcal{I})} \mu(\alpha).$$

L'idéal $\mathcal{I}$ (resp. $\mathcal{S}$) est dans ce cas un idéal zéro-dimensionnel *(resp.* système zéro-dimensionnel*).*

2 Le théorème de Stickelberger

Nous étudions, dans ce paragraphe, les propriétés d'une application linéaire simple : la multiplication par un polynôme dans $K[X_1, \ldots, X_n]/\mathcal{I}$.

Notation 2.1 *Pour tout polynôme $h \in K[X_1, \ldots, X_n]/\mathcal{I}$ nous noterons m_h l'endomorphisme de $K[X_1, \ldots, X_n]/\mathcal{I}$:*

$$\begin{array}{ccc} K[X_1, \ldots, X_n]/\mathcal{I} & \longrightarrow & K[X_1, \ldots, X_n]/\mathcal{I} \\ f & \longmapsto & h \cdot f \end{array}$$

Lemme 2.1 *Les sous-espaces A_α , $\alpha \in V(\mathcal{I})$ sont invariants sous l'action de m_h.*

Preuve : Par définition, A_α peut être identifié au quotient

$$C[X_1, \ldots, X_n]_\alpha / \mathcal{I} C[X_1, \ldots, X_n]_\alpha \, ,$$

$C[X_1, \ldots, X_n]_\alpha$ désignant le localisé de $C[X_1, \ldots, X_n]$ au point α. Aussi, si p/q est un élément de A_α, $h(p/q)$ et (hp/q) représentent le même élément. □

Corollaire 2.1 *Pour tout $\alpha \in V(\mathcal{I})$, la multiplication par*

$$h_\alpha(X_1, \ldots, X_n) = h(X_1, \ldots, X_n) - h(\alpha)$$

dans A_α est un opérateur nilpotent.

Preuve : On remarque que $h_\alpha(\alpha) = 0$. Par conséquent, le théorème des zéros de Hilbert nous assure de l'existence d'un entier strictement positif k tel que $h_\alpha^k \in \mathcal{M}_\alpha$, $\mathcal{M}_\alpha$ désignant l'unique idéal maximal de l'anneau local $C[X_1, \ldots, X_n]_\alpha$. Par passage au quotient, nous pouvons donc conclure que m_{h_α} est un opérateur nilpotant de A_α. □

D'après le lemme précédent, il existe un entier k tel que le polynôme minimal de l'opérateur m_{h_α} divise T^k. Comme C est algébriquement clos, on en déduit que, pour tout $\alpha \in V(\mathcal{I})$, il existe une base de A_α dans laquelle m_{h_α} a pour matrice :

$$\begin{pmatrix} 0 & \star & \cdots & \star \\ 0 & 0 & \cdots & \star \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

et par conséquent dans laquelle m_h a pour matrice :

$$\begin{pmatrix} h(\alpha) & \star & \cdots & \star \\ 0 & h(\alpha) & \cdots & \star \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & h(\alpha) \end{pmatrix}$$

On peut alors voir que $h(\alpha)$ est une valeur propre de m_h de multiplicité $\mu(\alpha) = dim_C(A_\alpha)$.
Le corollaire suivant récapitule quelques propriétés de m_h. Il énonce des résultats courament utilisées pour l'étude des systèmes zéro-dimensionels (voir par exemple [BW92],[Ped91],[Yoko92],[PRS93]):

Corollaire 2.2 *(Stickelberger) Soient $\mathcal{I}$ un idéal de $K[X_1, \ldots, X_n]$ admettant un nombre fini de zéros, et pour tout $h \in K[X_1, \ldots, X_n]$, m_h l'opérataur* multiplication par *h dans $K[X_1, \ldots, X_n]/\mathcal{I}$. Les valeurs propres de m_h sont exactement les zéros de $\mathcal{I}$ avec même multiplicités.*
Cette propriété a beaucoup de conséquences, en particulier :

- $Det(m_h) = \prod_{\alpha \in V(\mathcal{I})} h(\alpha)^{\mu(\alpha)}$,
- $Trace(m_h) = \sum_{\alpha \in V(\mathcal{I})} \mu(\alpha) h(\alpha) \cdot$,
- *Le polynôme caractéristique de m_h est :* $\prod_{\alpha \in V(\mathcal{I})} (T - h(\alpha))^{\mu(\alpha)}$.

3 La forme quadratique de Hermite généralisée

Lorsque $\mathcal{I} \subset K[X_1, \ldots, X_n]$ est zéro-dimensionel, nous avons pu voir que $A = K[X_1, \ldots, X_n]/\mathcal{I}$ est un K-espace vectoriel de dimension finie. Il est donc possible de prendre les traces d'éléments de $End_K(A)$ pour définir une forme bilinéaire symétrique $B : A \otimes A \longrightarrow K$

$$B(f, g) = Trace(fg)$$

En particulier, à tout polynôme $h \subset K[X_1, \ldots, X_n]$, on associe une forme quadratique comme suit :

Definition 3.1 *Soit $h \in K[X_1, \ldots, X_n]$ on définit une forme bilinéaire B_h : $A \otimes A \longrightarrow K$ en posant :*

$$B_h(f, g) = B(hf, g) = Trace(fgh)$$

Nous noterons Q_h, la forme quadratique associée à B_h et définie par :

$$Q_h(f) = B_h(f, f)$$

Théorème 3.1 *Soient un corps ordonné K, un idéal zéro-dimensionel $\mathcal{I} = (f_1, \ldots, f_s)$ de $K[X_1, \ldots, X_n]$, R un corps réel contenant K, C la clôture algébrique de R et un polynôme $h \in K[X_1, \ldots, X_n]$. Si $V_R(\mathcal{I}) = V(\mathcal{I}) \bigcap R^n$, alors:*

A. $\sigma(Q_h) = \sharp\{\alpha \in V_R(I) | h(\alpha) > 0\} - \sharp\{\alpha \in V_R(I) | h(\alpha) < 0\}$

B. $\rho(Q_h) = \sharp\{\alpha \in V(I) | h(\alpha) \neq 0\}$

où $\sigma(Q_h)$ (resp. $\rho(Q_h)$) désigne la signature (resp. le rang) de Q_h.

Ce théorème n'est pas nouveau (voir [BW92],[Ped91],[PRS93]). Nous proposons ici une variante de sa démonstration nous permettant d'introduire une notion de polynôme séparant, utilisée par divers auteurs sous des formes variées (voir par exemple [Ca88], [BW93], [Laz92], [GH91b], [GHMP95], [GVT95], [Re92], [ABRW94]) :

Definition 3.2 *Un polynôme $t \in K[X_1, \ldots, X_n]$ sépare $V(\mathcal{I})$ si*

$$\forall \alpha, \beta \in V(\mathcal{I}) \, , \alpha \neq \beta \Rightarrow t(\alpha) \neq t(\beta).$$

L'existence de tels éléments est montrée par le lemme suivant :

Lemme 3.1 *Soit $\mathcal{X}$ un ensemble de points de C^n tel que $\sharp\mathcal{X} = d$. La famille de formes linéaires $\{X_1 + iX_2 + \ldots + i^{n-1}X_n$ pour $0 \leq i \leq (n-1)d(d-1)/2\}$ contient au moins un élément séparant $\mathcal{X}$.*

Preuve : Notons $u_i(X) = X_1 + iX_2 + \ldots + i^{n-1}X_n$ et supposons que $(x, y) = ((x_1, \ldots, x_n), (y_1, \ldots, y_n))$ soit un couple de points distincts de $\mathcal{X}$ tels que $u_i(x) = u_i(y)$. Comme le polynôme $\sum_{i=1}^{n}(x_i - y_i)X^{i-1}$ admet au plus $n-1$ solutions distinctes (il n'est pas indentiquement nul car $x \neq y$), la famille $\{u_0, \ldots, u_{n-1}\}$ contient donc au moins un élément u_k tel que $u_k(x) \neq u_k(y)$. Comme de plus le nombre total de couples de points distincts de $\mathcal{X}$ n'exède pas $d(d-1)/2$, la famille de polynômes $\{X_1 + iX_2 + \ldots + i^{n-1}X_n \ , \ 0 \leq i \leq (n-1)d(d-1)/2\}$ contient au moins un élément séparant $\mathcal{X}$. □

Ces familles d'éléments séparants ont beaucoup de propriétés utiles pour l'étude des algèbres $K[X_1,\ldots,X_n]/\mathcal{I}$. En particulier :

Lemme 3.2 *Soient $\mathcal{I} \subset K[X_1,\ldots X_n]$ un idéal zéro-dimensionel et t un polynôme séparant $V(\mathcal{I})$. Si nous notons $d = \sharp V(\mathcal{I})$, $\{1,t,\ldots,t^{d-1}\}$ est une famille libre de $K[X_1,\ldots,X_n]/\mathcal{I}$.*

Preuve : Soient $a_0,\ldots,a_{d-1}$ des scalaires ($\in K$) tels que

$$g(t) = \sum_{i=0}^{d-1} a_i t^i = 0 \ mod\ \mathcal{I}$$

Pour tout, $\alpha \in V(\mathcal{I})$, $t(\alpha)$ est alors une racine de $g(T) = \sum_{i=0}^{d-1} a_i T^i$. Comme t sépare $V(\mathcal{I})$, le polynôme $g(T)$ admet par conséquent d racines (les $t(\alpha)$, $\alpha \in V(\mathcal{I})$) et est donc identiquement nul. La famille $\{1,t,\ldots,t^{d-1}\}$ est donc libre dans $K[X_1,\ldots,X_n]/\mathcal{I}$. □

Preuve du théorème: Soit t un élément séparant $V(\mathcal{I}) = \{\alpha_1,\ldots,\alpha_d\}$. Si $d = \sharp V(\mathcal{I})$, la famille $\{1,t,\ldots,t^{d-1}\}$ est libre dans $A = K[X_1,\ldots X_n]/\mathcal{I}$. Il est donc possible de trouver des polynômes $\omega_{d+1}\ \ldots,\omega_D$ tels que la famille $\mathcal{B}' = \{\omega_1 = 1,\omega_2 = t,\ldots,\omega_d = t^{d-1},\omega_{d+1}\ \ldots,\omega_D\}$ soit une base de A. Pour un polynôme $f \in K[X_1,\ldots,X_n]$ donné, notons $Y_1,\ldots,Y_D$ ses coordonnées dans la base $\mathcal{B}'$. Dans ce cas, $Q_h(f) = \sum_{i=1}^{d} \mu(\alpha_i)h(\alpha_i)\left(\sum_{j=1}^{D} \omega_j(\alpha_i)Y_j\right)^2$

Comme $\alpha_1,\ldots,\alpha_d$ sont des racines distinctes de f et comme t est un élément séparant $V(\mathcal{I})$, la matrice

$$\begin{pmatrix} 1 & t(\alpha_1) & \ldots & t(\alpha_1)^{d-1} \\ \vdots & & & \vdots \\ 1 & t(\alpha_d) & \ldots & t(\alpha_d)^{d-1} \end{pmatrix}$$

est une matrice de Vandermonde (donc inversible) sous-matrice de la matrice associée aux formes linéaires induites par le changement de variables :

$$Z_i = \sum_{j=1}^{D} \omega_j(\alpha_i)\cdot Y_j\ ,\ i = 1\ldots d$$

qui sont donc linéairement indépendantes. Par conséquent :

$$Q_h(f) = \sum_{i=1}^{d} \mu_i h(\alpha_i) Z_i^2$$

et donc :

$$\rho(Q_h) = \sharp\{\alpha \in V(I) | h(\alpha) \neq 0\}$$

Rappelons que C peut-être considéré comme un R-espace vectoriel:

$$C = \{a + ib\ ,\ i^2 = -1\ ,\ (a,b) \in R^2\}$$

ce qui nous permet d'utiliser pour la suite de la preuve la terminologie et les notations habituellement réservées aux nombres complexes. Nous noterons donc pour tout $c = a + ib \in C$:

- Partie Réelle : $Re(c) = a$
- Partie Imaginaire : $Im(c) = b$
- Conjugaison : $\overline{c} = a - ib$

Comme dans le cas complexe, l'opération de conjugaison est clairement un automorphisme de R-algèbres laissant R invariant, par conséquent $\overline{p(c)} = p(\overline{c})$ pour tout $p \in C[X_1, \ldots, X_n]$, ce qui montre en particulier que si $\alpha \in V(\mathcal{I})$, alors $\overline{\alpha} \in V(\mathcal{I})$.
Ainsi, il existe un entier positif ou nul s tel que $\sharp(V(\mathcal{I})\backslash V_R(\mathcal{I})) = 2s$. Quitte à permuter l'ordre des variables, on peut alors supposer que :

- $\alpha_i \in V(\mathcal{I})\backslash V_R(\mathcal{I})$ ssi $i \leq 2s$
- $\forall i = 1 \ldots s$, $\alpha_{i+s} = \overline{\alpha_i}$.

Nous avons alors :

$$Q_h = \sum_{i=1}^{s} \mu_i (h(\alpha_i) Z_i^2 + \overline{h(\alpha_i)} Z_{s+i}^2) + \sum_{i=2s+1}^{d} \mu_i h(\alpha_i) Z_i^2$$

Si nous posons :

$$U_i = (X_i + X_{i+s})/2\ ,\ V_i = (X_i + X_{i+s})/(2 \cdot i)\ ,\ i = 1 \ldots s$$

et :

$$Q_h^i = h(\alpha_i) Z_i^2 + \overline{h(\alpha_i)} Z_{s+i}^2$$

alors :

$$Q_h^i = h(\alpha_i)(U_i + iU_{i+s})^2 + \overline{h(\alpha_i)}(\overline{U_i + iU_{i+s}})^2 = 2Re(h(\alpha_i)(U_i + iU_{i+s})^2)$$

Si $h(\alpha_i) = a + ib$:

$$Q_h^i = 2aU_i^2 - 2aV_i^2 - 4bU_iV_i$$

d'où :

- $Q_h^i = \frac{2}{a}((aU_i - 2bU_{i+s})^2 - (a^2 + 4b^2)U_{i+s}^2)$ si $a \neq 0$

- $Q_h^i = -b((U_i + U_{i+s})^2 - (U_i - U_{i+s})^2)$ si $a = 0$.

Les signatures des formes quadratiques Q_h^i sont donc nulles et par conséquent (les formes linéaires associées aux changements de variables effectués étant clairement linéairement indépendantes) ,

$$\sigma(Q_h) = \sigma(\sum_{i=2s+1}^{d} \mu_i h(\alpha_i) Z_i^2) = \sharp\{\alpha \in V_R(f) \mid h(\alpha) > 0\} - \sharp\{\alpha \in V_R(f) \mid h(\alpha) < 0\}$$

□

Nous décrivons maintenant quelques conséquences du théorème 3.1, en particulier nous rapellerons un critère utile pour tester l'appartenance d'un polynôme au radical d'un idéal.

Le théorème 3.1 montre que un polyôme h s'annule sur $V(\mathcal{I})$ si et seulement si le rang de la forme quadratique de Hermite généralisée Q_h qui lui est associée est nul c'est à dire si et seulement si Q_h est nulle.

Notation 3.1 *Nous noterons $Trace(h)$ pour $Trace(m_h)$.*
Soit Q_h la forme quadratique de Hermite généralisée associée à un polynôme $h \in K[X_1, \ldots, X_n]$, de matrice q_h dans une base $\mathcal{B} = \{\omega_1, \ldots \omega_D\}$ de $A = K[X_1, \ldots, X_n]/\mathcal{I}$ avec $\omega_1 = 1$. Nous noterons $q_h[i, j]$ l'élément situé à l'intersection de la i^e colonne et de la j^e ligne de q_h, $q_h[i]$ la i^e ligne de q_h.

Pour tout polynôme $h \in K[X_1, \ldots, X_n]$, $\overrightarrow{h}$ sera l'expression de h modulo $\mathcal{I}$ dans la base $\mathcal{B}$.

Enfin, nous noterons Vtr le vecteur de K^n : $Vtr = [Trace(\omega_1), \ldots, Trace(\omega_D)]$ et pour tout polynôme $h \in K[X_1, \ldots, X_n]$, $Vtr(h) = [Trace(h\omega_1), \ldots, Trace(h\omega_D)]$.

Lemme 3.3 *Pour tout couple de polynômes (f, g) de $K[X_1, \ldots, X_n]$,*

$$Trace(m_{fg}) = \overrightarrow{f} \cdot Vtr(g)$$

Preuve : En exprimant fg dans la base $\mathcal{B}$ et en posant $\overrightarrow{f} = \sum_{i=1}^{D} a_i \omega_i$, il vient :

$$Trace(fg) = Trace(\sum_{i=1}^{D} a_i \omega_i g) = \sum_{i=1}^{D} a_i Trace(g\omega_i)$$

et par conséquent,

$$Trace(fg) = [a_1, \ldots, a_D] \cdot [Trace(h\omega_1), \ldots, Trace(h\omega_D)] = \overrightarrow{f} \cdot Vtr(g)$$

□

Ceci nous donne alors une propriété intéressante sur la forme quadratique de Hermite généralisée :

Proposition 3.1 *Q_h est nulle si et seulement si $q_h[1]$ est nulle.*

Preuve : Pour tout $i > 1$,

$$q_h[i] = [Trace(\omega_i\omega_1), \ldots, Trace(\omega_i\omega_D)].$$

Par conséquent, d'après le lemme 3.3

$$q_h[i,j] = \overrightarrow{\omega_i\omega_j} \cdot Vtr(1) = \overrightarrow{\omega_i\omega_j} \cdot q_h[1]$$

□

Nous retrouvons ainsi un critère d'appartenance d'un polynôme à $\sqrt{\mathcal{I}}$, ne nécessitant pas le calcul explicite de $\sqrt{\mathcal{I}}$ (voir [Ron90], [GMT88],[GV92]) , ce qui présentera plus tard un avantage algorithmique certain :

Proposition 3.2 *(Dickson) Soit $\mathcal{S} = \{f_1, \ldots, f_s\} \subset K[X_1, \ldots, X_n]$ un système zéro-dimensionel, $\mathcal{I}$ l'ideal engendré par $\mathcal{S}$ et $\{\omega_1, \ldots, \omega_D\}$ une base de l'espace vectoriel de dimension finie $K[X_1, \ldots, X_n]/\mathcal{I}$ (avec $\omega_1 = 1$). Un polynôme $h \in K[X_1, \ldots, X_n]$ appartient à $\sqrt{\mathcal{I}}$ si et seulement si*

$$Trace(h\omega_i) = 0 \ , \ \forall i = 1, \ldots, D.$$

4 μ-résolution, représentation univariée d'un système zéro-dimensionnel

Nous proposons de ramener l'étude d'un idéal zéro-dimensionnel de $K[X_1, \ldots, X_n]$ à celle d'une famille de fractions rationnelles de $K(T)$. Nous définissons, pour commencer, une équivalence entre idéaux faisant appel à des morphismes d'ensembles algébriques particuliers :

Definition 4.1 *Soit $\mathcal{E} \subset C^n$ un ensemble algébrique. Une application $\phi^\star : \mathcal{E} \subset C^n \longrightarrow C$ sera dite K-régulière si il existe $p \in K[X_1, \ldots, X_n]$ tel que $\forall \alpha \in \mathcal{E}$, $p(\alpha) = \phi^\star(\alpha)$*

De la même manière, si $\mathcal{E} \subset C^n$ et $\mathcal{F} \subset C^m$ sont deux ensembles algébriques, l'application $\phi^\star : \mathcal{E} \subset C^n \longrightarrow \mathcal{F} \subset C^m$ sera un K-morphisme d'ensembles algébriques si chacune de ses fonctions coordonnée est K-régulière.

L'application $\phi^\star : \mathcal{E} \subset C^n \longrightarrow \mathcal{F} \subset C^m$ sera un K-isomorphisme d'ensembles algébriques si il existe un K-morphisme d'ensembles algébriques $\psi^\star : \mathcal{F} \subset C^m \longrightarrow \mathcal{E} \subset C^n$ tel que $\psi^\star \circ \phi^\star = Id_{\mathcal{E}}$ et $\phi^\star \circ \psi^\star = Id_{\mathcal{F}}$.

A tout morphisme de K-algèbres $\phi : K[X_1, \ldots, X_n] \longrightarrow K[Y_1, \ldots, Y_m]$, on associe canoniquement un K-morphisme d'ensembles algébriques en posant :

$$\begin{array}{rccc} \phi^\star : & C^m & \longrightarrow & C^n \\ & \alpha & \longmapsto & (\phi(X_1)(\alpha), \ldots, \phi(X_n)(\alpha)) \end{array}$$

Nous insistons sur le fait que ces morphismes d'ensembles algébriques sont définis sur$K$ (et non sur C), ce qui a, comme nous le verrons plus tard, un grand intéret algorithmique.
Il résulte de ces définitions quelques propriétés simples qui nous seront utiles par la suite :

Proposition 4.1 *Soient $\phi : K[X_1, \ldots, X_n] \longrightarrow K[Y_1, \ldots, Y_m]$ un morphisme de K-algèbres , $\mathcal{E} \subset C^n$ et $\mathcal{F} \subset C^m$ deux ensembles algébriques tels que $\phi^\star$ induise un K-isomorphisme de $\mathcal{F}$ dans $\mathcal{E}$.*

Pour tout morphisme de K-algèbres $\psi : K[Y_1, \ldots, Y_m] \longrightarrow K[X_1, \ldots, X_n]$ tel que $\psi^\star = (\phi^\star)^{-1}$ sur $\mathcal{E}$,

- $\forall \alpha \in \mathcal{E}$, $\forall p \in K[X_1, \ldots, X_n]$, $p(\alpha) = \phi(p)(\psi^\star(\alpha))$
- $\forall \alpha \in \mathcal{E}$, $\forall p \in K[X_1, \ldots, X_n]$, $p(\alpha) = (\psi \circ \phi)(p)(\alpha)$

Preuve : Pour tout $\beta \in \mathcal{F}$,

$$p(\phi^\star(\beta)) = p(\phi(X_1)(\beta), \ldots, \phi(X_n)(\beta)).$$

Comme ϕ est un morphisme d'algèbres, ceci nous donne :

$$p(\phi^\star(\beta)) = \phi(p)(\beta).$$

Pour tout $\beta \in \mathcal{F}$, $\phi^\star$ étant un isomorphisme de $\mathcal{F}$ dans $\mathcal{E}$, il existe $\alpha \in \mathcal{E}$ tel que $\alpha = \phi^\star(\beta)$. Par définition de $\psi^\star$, nous avons alors $\beta = \psi^\star(\alpha)$ et par conséquent,

$$p(\alpha) = \phi(p)(\psi^\star(\alpha))$$

De plus, $\forall \alpha \in \mathcal{E}$, $\forall p \in K[X_1, \ldots, X_n]$,

$$(\psi \circ \phi)(p)(\alpha) = (\psi(\phi(p))(\phi^\star(\psi^\star(\alpha))) = \phi(p)(\psi^\star(\alpha)) = p(\alpha).$$

□

Introduisons maintenant une relation d'équivalence entre idéaux zéro-dimensionnels :

Definition 4.2 *Soient $\mathcal{I} \subset K[X_1, \ldots, X_n]$ et $\mathcal{J} \subset K[Y_1, \ldots, Y_m]$ deux idéaux zéro-dimensionnels. Nous dirons que $\mathcal{I}$ est μ-équivalent à $\mathcal{J}$ et nous noterons $\mathcal{I} \simeq_\mu \mathcal{J}$, si il existe un K-ismorphisme $\phi^\star : V(\mathcal{J}) \longrightarrow V(\mathcal{J})$ tel que :*

$$\forall \beta \in V(\mathcal{J}) \ , \ \mu(\phi^\star(\beta)) = \mu(\beta)$$

Nous avons pu voir que l'application *Trace* est à la base de résultats utiles pour l'étude des systèmes zéro-dimensionnels. Montrons que la μ-équivalence *préserve les traces* :

Proposition 4.2 *Soient $\mathcal{I} \subset K[X_1, \ldots, X_n]$ et $\mathcal{J} \subset K[Y_1, \ldots, Y_m]$ deux idéaux zéro-dimensionnels. Les idéaux $\mathcal{I}$ et $\mathcal{J}$ sont μ-équivalents si et seulement si il existe un morphisme de K algèbres $\phi : K[X_1, \ldots, X_n] \longrightarrow K[Y_1, \ldots, Y_m]$ tel que :*

- *$\phi^\star$ induise un K-isomorphisme d'ensembles algébriques de $V(\mathcal{J})$ dans $V(\mathcal{I})$*
- $\forall p \in C[X_1, \ldots, X_n] \ , \ \sum_{\alpha \in V(\mathcal{I})} \mu(\alpha) p(\alpha) = \sum_{\beta \in V(\mathcal{J})} \mu(\beta) \phi(p)(\beta)$

Preuve :

- Si $\mathcal{I}$ et $\mathcal{J}$ sont μ-équivalents , il existe un morphisme de K-algèbres $\phi : K[X_1, \ldots, X_n] \longrightarrow K[Y_1, \ldots, Y_m]$ tel que $\phi^\star$ vérifie les propriétés de la définition 4.2. Soit $p \in C[X_1, \ldots, X_n]$. L'application $\phi^\star$ étant un K-isomorphisme d'ensembles algébriques, nous avons :

  $$\sum_{\beta \in V(\mathcal{J})} \mu(\beta) \phi(p)(\beta) = \sum_{\alpha \in V(\mathcal{I})} \mu((\phi^\star)^{-1}(\alpha)) \phi(p)((\phi^\star)^{-1}(\alpha))$$

  D'après la proposition 4.1 il vient alors :

  $$\sum_{\beta \in V(\mathcal{J})} \mu(\beta) \phi(p)(\beta) = \sum_{\alpha \in V(\mathcal{I})} \mu((\phi^\star)^{-1}(\alpha)) p(\alpha)$$

  et enfin, d'après la définition 4.2 :

  $$\sum_{\beta \in V(\mathcal{J})} \mu(\beta) \phi(p)(\beta) = \sum_{\alpha \in V(\mathcal{I})} \mu(\alpha) p(\alpha)$$

- Il est toutjours possible de définir, pour tout $\gamma \in V(\mathcal{I})$, un polynôme $p_\gamma \in C[X_1, \ldots, X_n]$ tel que $p_\gamma(\gamma) = 1$ et $\forall \alpha \neq \gamma \ , \ \alpha \in V(\mathcal{I}) \ p_\gamma(\alpha) = 0$. En effet, soit α un point de $V(\mathcal{I})$ tel que

  $$\alpha = (\alpha_1, \ldots, \alpha_n) \neq \gamma = (\gamma_1, \ldots, \gamma_n)$$

Nous pouvons trouver un entier k tel que $\gamma_k \neq \alpha_k$. Posons

$$P_{\gamma,\alpha} = \frac{X_k - \alpha_k}{\gamma_k - \alpha_k}$$

Nous aurons alors: $P_{\gamma,\alpha}(\alpha) = 1$ et $P_{\gamma,\alpha}(\alpha) = 0$. Il suffit de poser

$$P_\gamma = \prod_{\alpha \neq \gamma \ , \ \alpha \in V(\mathcal{I})} P_{\gamma,\alpha}$$

pour obtenir le polynôme désiré.

L'application $\phi^\star$ étant une bijection de $V(\mathcal{J})$ dans $V(\mathcal{I})$,

$$\forall \beta \in V(\mathcal{J}) \ , \ \exists \alpha \in V(\mathcal{I}) \ , \ \alpha = \phi^\star(\beta)$$

Ainsi, $\sharp V(\mathcal{J}) = \sharp V(\mathcal{I})$ et

$$\sum_{\alpha \in V(\mathcal{I})} \mu(\alpha) P_\gamma(\alpha) = \sum_{\alpha \in V(\mathcal{I})} \mu((\phi^\star)^{-1}(\alpha)) \phi(P_\gamma)((\phi^\star)^{-1}(\alpha))$$

Comme $\phi(P_\gamma)((\phi^\star)^{-1}(\alpha)) = P_\gamma(\alpha)$ nous avons alors $\mu(\gamma) = \mu((\phi^\star)^{-1}(\gamma))$.

□

Remarque 4.1 *Soient $\mathcal{I} \subset K[X_1, \ldots, X_n]$ et $\mathcal{J} \subset K[Y_1, \ldots Y_m]$, deux idéaux μ-équivalents. Les K-algèbres $K[X_1, \ldots, X_n]/\mathcal{I}$ et $K[Y_1, \ldots, Y_m]/\mathcal{J}$ ne sont pas , en général, isomorphes.*

Considérons par exemple $\mathcal{I} = \langle X_1^2, X_1X_2, X_2^2 \rangle \subset K[X_1, X_2]$ et $\mathcal{J} = \langle Y_1^2 \rangle \subset K[Y_1]$. En posant :

$$\begin{array}{rccc} \phi : & K[X_1, X_2] & \longrightarrow & K[Y_1] \\ & X_1 & \longmapsto & Y_1 \\ & X_2 & \longmapsto & 0 \end{array}$$

on peut voir que $\phi^\star$ est un K-isomorphisme d'ensembles algébriques vérifiant les hypothèses de la définition 4.2 et nous avons alors $\mathcal{I} \simeq_\mu \mathcal{J}$.
Supposons que $\psi : K[Y_1]/\mathcal{J} \longrightarrow K[X_1, X_2]/\mathcal{I}$ soit un morphisme de K-algèbres, et posons $\psi(Y_1) = aX_1 + bX_2$, $a, b \in K$.
Dans ce cas,

$$\psi(Y_1^2) = \psi(Y_1)^2 = a^2X_1^2 + b^2X_2^2 + 2abX_1X_2 = 0 \ mod \ \mathcal{I}$$

et ψ n'est pas injectif.
Il n'existe donc pas d'isomorphisme de K-algèbres entre $K[Y_1]/\mathcal{J}$ et $K[X_1, X_2]/\mathcal{I}$. Pour des raisons évidentes de conservation des multiplicités, l'existence d'un isomorphisme entre $K[X_1, \ldots, X_n]/\sqrt{\mathcal{I}}$ et $K[Y_1, \ldots, Y_m]/\sqrt{\mathcal{J}}$ n'implique pas que les deux idéaux soient μ-équivalents. La réciproque est par contre vraie :

Proposition 4.3 *Soient $\mathcal{I} \subset K[X_1, \ldots, X_n]$ et $\mathcal{J} \subset K[Y_1, \ldots, Y_m]$ deux idéaux zéro -dimensionnels tels que $\mathcal{I} \simeq_\mu \mathcal{J}$. Notons alors $\phi : K[X_1, \ldots, X_n] \longrightarrow K[Y_1, \ldots, Y_m]$ un morphisme de K-algèbres vérifiant les hypothèses de la définition 4.2.*
Si $\tilde{\phi}$ est le morphisme de K-algèbres $\tilde{\phi} : K[X_1, \ldots, X_n] \longrightarrow K[Y_1, \ldots, Y_m]/\sqrt{\mathcal{J}}$ canoniquement déduit de ϕ, $ker(\tilde{\phi}) = \sqrt{\mathcal{I}}$ et $\tilde{\phi}$ induit un isomorphisme de K-algèbres :

$$\phi_{red} : K[X_1, \ldots, X_n]/\sqrt{\mathcal{I}} \longrightarrow K[Y_1, \ldots, Y_m]/\sqrt{\mathcal{J}}$$

Preuve : Comme $\phi^\star$ est, par définition, un K-isomorphisme d'ensembles algébriques, pour tout $\alpha \in V(\mathcal{I})$, $\mu(\alpha) = \mu((\phi^\star)^{-1}(\alpha))$.
L'application $\phi^\star$ étant un K-isomorphisme d'ensembles algébriques, pour tout $p \in \sqrt{\mathcal{I}}$ et tout $\beta \in V(\mathcal{J})$, il existe $\alpha \in V(\mathcal{J})$ tel que $\phi(p)(\beta) = \phi(p)((\phi^\star)^{-1}(\alpha)) = p(\alpha) = 0$. Par conséquent, $\phi(p) \in \sqrt{\mathcal{J}}$.
Inversement, soit $p \in K[X_1, \ldots, X_n]$ tel que $\phi(p) \in \sqrt{\mathcal{J}}$. Pour tout $\alpha \in V(\mathcal{I})$, il existe $\beta \in V(\mathcal{J})$ tel que $(\phi^\star)^{-1}(\alpha) = \beta$. Dans ce cas,

$$p(\alpha) = \phi(p)(\phi^\star)^{-1}(\alpha)) = \phi(p)(\beta) = 0$$

Ainsi, $ker(\tilde{\phi}) = \sqrt{\mathcal{I}}$ et donc $\tilde{\phi}$ se factorise en un isomorphisme injectif

$$\phi_{red} : K[X_1, \ldots, X_n]/\sqrt{\mathcal{I}} \longrightarrow K[Y_1, \ldots, Y_m]/\sqrt{\mathcal{J}}$$

Comme $\sharp V(\mathcal{J}) = \sharp V(\mathcal{I})$, nous avons alors

$$dim_K(K[X_1, \ldots, X_n]/\sqrt{\mathcal{I}}) = dim_K(K[Y_1, \ldots, Y_m]/\sqrt{\mathcal{J}})$$

ce qui montre que ϕ_{red} est bijectif. □

Les diverses propriétés de la μ-équivalence nous conduisent alors à définir ce que nous entendons désormais par *résoudre* un système zéro-dimensionnel :

Definition 4.3 *Un idéal zéro-dimensionnel $\mathcal{I}$ sera dit μ-résolu si il existe un idéal $\mathcal{J} \subset K[T]$ tel que $\mathcal{I} \simeq_\mu \mathcal{J}$. Si ϕ est un morphisme de K-algèbres vérifiant les propriétes de la définition 4.2, nous dirons alors que $(\mathcal{J}, \phi^\star)$ est une μ-résolution de $\mathcal{I}$.*

Remarque 4.2 *Si $(\mathcal{J}, \phi^\star)$ et $(\mathcal{J}, (\phi')^\star)$ sont deux μ-résolutions de $\mathcal{I}$, $\phi^\star$ et $(\phi')^\star$ coincident sur $V(\mathcal{J})$. Par abus de notation, nous écrirons que $\mathcal{J}$ est une μ-résolution de $\mathcal{I}$.*

Le terme de résolution ne parait pas abusif, car la donnée d'une μ-résolution permet de se ramener à un problème en une variable pour lequel beaucoup d'outils algorithmiques sont disponibles tant pour l'approximation que pour le codage des racines. La donnée d'un K-isomorphisme d'ensembles algébriques nous permettant de *remonter* les résultats.
Le résultat que nous nous proposons de montrer dans la suite de ce chapitre est le suivant :

Théorème 4.1 *Tout idéal zéro-dimensionnel $\mathcal{I} \subset K[X_1, \ldots, X_n]$ admet une μ-résolution.*

Pour tout $h \in K[X_1, \ldots, X_n]$, rappelons que m_h désigne l'opérateur *multiplication* par h dans $A = K[X_1, \ldots, X_n]/\mathcal{I}$.
Pour tous $t, v \in K[X_1, \ldots, X_n]$, on définit les ensembles :

$$V(\mathcal{I})_{t(\alpha)} = \{\beta \in V(\mathcal{I}) \ , \ t(\beta) = t(\alpha)\}$$
$$t(V(\mathcal{I})) = \{t(\alpha) \ , \ \alpha \in V(\mathcal{I})\}$$

ainsi que les polynômes :

$$f(t,T) = \prod_{\alpha \in V(\mathcal{I})} (T - t(\alpha))^{\mu(\alpha)}$$
$$g(v,t,T) = \sum_{\alpha \in V(\mathcal{I})} \mu(\alpha) v(\alpha) \prod_{y \in t(V(\mathcal{I})) \setminus \{t(\alpha)\}} (T - y)$$

Lemme 4.1 *Les polynômes $f(t,T)$ et $g(v,t,T)$ sont dans $K[X_1, \ldots, X_n]$. Plus précisément, si S est une variable indépendante de $X_1, \ldots, X_n$, et si , pour $h \in K[X_1, \ldots, X_n]$ fixé, $P_h(T)$ désigne le polynôme caractéristique de m_h,*

- *$f(t,T)$ est le polynôme caractéristique de m_t.*
- *$\forall v \in K[X_1, \ldots, X_n]$, $g(v,t,T) = h(v,t,T)/gcd(f(t,T), f'(t,T))$*
  avec :
$$h(v,t,T) = -\left(\frac{\partial}{\partial S} P_{t+Sv}(T)\right)_{S=0}$$

Preuve : D'après le corollaire 2.2, le polynôme caratéristique de m_t peut s'exprimer par :

$$\prod_{\alpha \in V(\mathcal{I})} (T - t(\alpha))^{\mu(\alpha)}$$

ce qui montre le premier point.
$\forall i = 1, \ldots, n$, $P_{t+Sv}(T) = \prod_{\alpha \in V(\mathcal{I})} (T - t(\alpha) - Sv(\alpha))^{\mu(\alpha)}$, par conséquent :

$$\left(\frac{\partial}{\partial S} P_{t+Sv}(T)\right)_{S=0} = -\sum_{\alpha \in V(\mathcal{I})} \mu(\alpha) v(\alpha) (T - t(\alpha))^{\mu(\alpha)-1} \prod_{\substack{\beta \in V(\mathcal{I}) \\ \beta \neq \alpha}} (T - t(\beta))^{\mu(\beta)}$$

Or $gcd(f(t,T), f'(t,T)) = \prod_{\alpha \in V(\mathcal{I})} (T - t(\alpha))^{\mu(\alpha)-1}$, et donc :

$$-\frac{\left(\frac{\partial}{\partial S} P_{t+Sv}(T)\right)_{S=0}}{gcd(f(t,T), f'(t,T))} = \sum_{\alpha \in V(\mathcal{I})} \mu(\alpha) v(\alpha) \prod_{\substack{\beta \in V(\mathcal{I}) \\ t(\beta) \neq t(\alpha)}} (T - t(\beta)) = g(v,t,T)$$

□

Lemme 4.2 *Si α est une racine de S, alors $t(\alpha)$ est une racine de $f(t,T)$ et*

$$\frac{\sum\limits_{\beta\in V(\mathcal{I})_{t(\alpha)}} \mu(\beta)v(\beta)}{\sum\limits_{\beta\in V(\mathcal{I})_{t(\alpha)}} \mu(\beta)} = \frac{g(v,t,t(\alpha))}{g(t,t(\alpha))}$$

avec $g(t,T) = g(1,t,T)$.

Preuve : Par définition,

$$g(v,t,t(\alpha)) = \sum_{\beta\in V(\mathcal{I})} \mu(\beta)v(\beta) \prod_{y\in t(V(\mathcal{I}))\setminus\{t(\beta)\}} (t(\alpha)-y)$$

Or , on peut remarquer que $\mu(\beta)v(\beta)\left(\prod\limits_{y\in t(V(\mathcal{I}))\setminus\{t(\beta)\}} (t(\alpha)-y)\right)$ est nul si et seulement si il existe $y \in t(V(\mathcal{I})) \setminus \{t(\beta)\}$ tel que $y = t(\alpha)$, ce qui montre que $g(v,t,t(\alpha))$ peut s'écrire :

$$g(v,t,t(\alpha)) = \sum_{\substack{\beta\in V(\mathcal{I}) \\ t(\beta)=t(\alpha)}} \mu(\beta)v(\beta) \prod_{y\in t(V(\mathcal{I}))\setminus\{t(\alpha)\}} (t(\alpha)-y)$$

ou encore :

$$g(v,t,t(\alpha)) = \left(\prod_{y\in t(V(\mathcal{I}))\setminus\{t(\alpha)\}} (t(\alpha)-y)\right)\left(\sum_{\beta\in V(\mathcal{I})_{t(\alpha)}} \mu(\beta)v(\beta)\right)$$

Comme $g(t,T) = g(1,t,T)$ nous avons de même :

$$g(t,t(\alpha)) = \sum_{\substack{\beta\in V(\mathcal{I}) \\ t(\beta)=t(\alpha)}} \mu(\beta)v(\beta) \prod_{y\in t(V(\mathcal{I}))\setminus\{t(\alpha)\}} (t(\alpha)-y)$$

et donc

$$g(t,t(\alpha)) = \left(\prod_{y\in t(V(\mathcal{I}))\setminus\{t(\alpha)\}} (t(\alpha)-y)\right)\left(\sum_{\beta\in V(\mathcal{I})_{t(\alpha)}} \mu(\beta)\right)$$

ce qui démontre la formule. □

Proposition 4.4 (*représentation univariée rationelle*) *Soient $S = \{f_1,\ldots,f_s\}$ un système zéro-dimensionel de $Z[X_1,\ldots,X_n]$ et $V(\mathcal{I}) = \{\alpha_1,\ldots\alpha_d\}$ l'ensemble des solutions distinctes de S.*
Pour tout polynôme $t \in K[X_1,\ldots,X_n]$ séparant $V(\mathcal{I})$, il existe des polynômes :

$$f(t,T)\ ,\ g(t,T)\ ,\ g_1(t,T),\ldots,g_n(t,T) \in K[X_1,\ldots X_n]$$

tels que :

- *Les racines de* $f(t,T)$ *sont les* $t(\alpha_1),\ldots,t(\alpha_d)$ *avec pour multiplicités respectives* $\mu(\alpha_1),\ldots,\mu(\alpha_d)$.
- *Si* α *est une racine de* S, *pour tout* $i = 1\ldots n$:

$$X_i(\alpha) = \frac{g_i(t,t(\alpha))}{g(t,t(\alpha))}$$

Nous dirons que $\{f(t,T)\ ,\ g(t,T)\ ,\ g_1(t,T),\ldots,g_n(t,T)\}$ *est la* **représentation univariée rationnelle** *de* $\mathcal{I}$ *associée à* t.

Preuve : Soit $t \in K[X_1,\ldots,X_n]$ un polynôme séparant $V(\mathcal{I})$ (son existence est prouvée par le lemme 3.1). Nous pouvons remarquer que $V(\mathcal{I})_{t(\alpha)} = \{\alpha\}$ et par conséquent, pour tout $v \in K[X_1,\ldots,X_n]$ et tout $\alpha \in V(\mathcal{I})$, le lemme 4.2 nous donne :

$$\frac{\mu(\alpha)v(\alpha)}{\mu(\alpha)} = v(\alpha) = \frac{g(v,t,t(\alpha))}{g(t,t(\alpha))}$$

Il ne reste alors qu'à poser $g_i(t,T) = g(X_i,t,T)\ ,\ i = 1\ldots n$ pour obtenir le résultat énoncé. □

Le résultat suivant achèvera la démonstration du théorème 4.1 :

Proposition 4.5 *Soient* $\mathcal{I} \subset K[X_1,\ldots,X_n]$ *un idéal zéro-dimensionnel et*

$$\{f(t,T)\ ,\ g(t,T)\ ,\ g_1(t,T),\ldots,g_n(t,T)\}$$

une représentation univariée rationnelle de $\mathcal{I}$. *L'application*

$$\begin{array}{rccl} \gamma^\star : & V(f) & \longrightarrow & V(\mathcal{I}) \\ & \beta & \longmapsto & 1/g(t,\beta)\cdot(g_1(t,\beta),\ldots,g_n(t,\beta)) \end{array}$$

définit un K*-isomorphisme de* $V(f)$ *dans* $V(\mathcal{I})$ *et* $(f,\gamma^\star)$ *est une* μ*-résolution de* $\mathcal{I}$.

Preuve : Par construction, le polynôme $g(t,T)$ est premier avec $f(t,T)$ (on peut en effet remarquer que $g(t,T)$ est la dérivée de la partie sans facteurs carrés de $f(t,T)$). Il existe donc des polynômes $u(T)$ et $v(T)$ tels que

$$u(T)g(t,T) + v(T)f(t,T) = 1 = u(t)g(t,t) + v(t)f(t,t)$$

D'après le lemme 4.1, $f(t,T)$ est le polynôme caractéristique de m_t. En appliquant le théorème de Cayley on peut voir que $f(t,t) \in \mathcal{I}$. $g(t,t)$ est donc inversible modulo $\mathcal{I}$ d'inverse $u(t)$.

En posant, pour tout $i = 1, \ldots, n$ $u_i(t,T) = u(T)g_i(t,T)$, on définit deux morphismes de K-algèbres :

$$\begin{array}{rccl} \phi: & K[X_1,\ldots,X_n] & \longrightarrow & K[T] \\ & X_i & \longmapsto & u_i(t,T)\ ,\ i = 1 \ldots n \\ \psi: & K[T] & \longrightarrow & K[X_1,\ldots,X_n] \\ & T & \longmapsto & t \end{array}$$

et on note $\mathcal{J}$ l'idéal de $K[T]$ engendré par $f(t,T)$.
Pour tout $\alpha \in V(\mathcal{I})$, $\phi^\star(\psi^\star)(\alpha) = \phi^\star(t(\alpha)) = (u_1(t,t(\alpha)),\ldots,u_n(t,t(\alpha)))$. Par construction des polynômes $u_1,\ldots,u_n$, $\phi^\star(\psi^\star)(\alpha) = \alpha$ et donc $\phi^\star \circ \psi^\star|_{V(\mathcal{I})} = Id_{V(\mathcal{I})}$.
De la même façon, pour tout $\beta \in V(\mathcal{J})$, il existe $\alpha \in V(\mathcal{I})$ tel que $\beta = t(\alpha)$. Ainsi,

$$\psi^\star(\phi^\star)(\beta) = t(u_1,t(\alpha),\ldots,u_n(t,t(\alpha))) = t(\alpha) = \beta,$$

et donc $\psi^\star \circ \phi^\star|_{V(\mathcal{J})} = Id_{V(\mathcal{J})}$.
Comme $\phi^\star$ est un K-isomorphisme de $V(f)$ dans $V(\mathcal{I})$, coincidant avec $\gamma^\star$ sur $V(\mathcal{I})$, l'application $\gamma^\star$ est donc un K-isomorphisme de $V(f)$ dans $V(\mathcal{I})$.
Enfin, d'après la proposition 4.4,

$$\forall \alpha \in \mathcal{I}\ ,\ (\gamma^\star)^{-1}(\alpha) = t(\alpha)$$

et

$$\mu(\alpha) = \mu(t(\alpha)) = \mu((\gamma^\star)^{-1}(\alpha))$$

$(\mathcal{J},\gamma^\star)$ est par conséquent une μ-résolution de $\mathcal{I}$.

□

Definition 4.4 *En reprenant les notations de la proposition 4.4 et, d'après ce qui précède, nous dirons que* $(f,\gamma^\star)$ *est la* μ-résolution induite par la *représentation univariée rationelle* de $\mathcal{I}$ associée à t, *où* $\gamma^\star$ *est la fonction rationnelle*

$$\begin{array}{rccl} \gamma^\star: & C & \longrightarrow & C^n \\ & \alpha & \longmapsto & 1/g(t,t(\alpha)) \cdot (g_1(t,t(\alpha)),\ldots,g_n(t,t(\alpha))) \end{array}$$

Nous avons indroduit un procédé (*représentation univariée rationelle*) de construction pour définir une μ-résolution. Montrons maintenant que toute μ-résolution peut s'exprimer par la donnée d'une *représentation univariée rationelle* :

Proposition 4.6 *Soit* $(\langle g(T)\rangle,\phi^\star)$ *une* μ*-résolution d'un idéal zéro dimensionnel* $\mathcal{I} \subset K[X_1,\ldots,X_n]$. *Le polynôme* $g(T)$ *est alors le polynôme caractéristique d'un élément* $t \in K[X_1,\ldots,X_n]$ *séparant* $V(\mathcal{I})$. *Si de plus* $(\mathcal{J}',\gamma^\star)$ *est la* μ*-résolution induite par la représentation univariée rationelle de* $\mathcal{I}$ *associée à* t, $\mathcal{J}' = \langle g(T)\rangle$ *et* $\gamma^\star$ *coincide avec* $\phi^\star$ *sur* $V(g)$.

Preuve : Notons $\phi : K[X_1, \ldots, X_n] \longrightarrow K[T]$ un morphisme de K-algèbres vérifiant les hypothèses de la définition 4.2.
D'après la proposition 4.3 ϕ se factorise en un isomorphisme ϕ_{red} de $A_{red} = K[X_1, \ldots, X_n]/\sqrt{\mathcal{I}}$ dans $B_{red} = K[T]/\sqrt{\langle g(T)\rangle}$, il existe alors $t \in K[X_1, \ldots, X_n]$ tel que $\phi_{red}(t) = T$. En particulier, $\phi(t) = T + q(T)$ qvec $q(T) \in \sqrt{\langle g(T)\rangle}$.

Notons P_t (resp. P_T) le polynôme caractéristique de m_t (resp. m_T) dans $A = K[X_1, \ldots, X_n]/\mathcal{I}$ (resp. $B = K[T]/\langle g(T)\rangle$). Comme $dim_K(A) = dim_K(B)$, P_t et P_T ont mêmes degrés. Les sommes de Newton élémentaires de P_t s'écrivent, d'après le théorème de Stickelberger :

$$N_i(P_t) = \sum_{\alpha \in V(\mathcal{I})} \mu(\alpha) t(\alpha)^i.$$

De même,

$$N_i(P_T) = \sum_{\beta \in V(g)} \mu(\beta)(\beta)^i = \sum_{\beta \in V(g)} \mu(\beta)(\phi(t)(\beta))^i.$$

D'après la proposition 4.2, nous avons alors $N_i(P_t) = N_i(P_T)$ pour tout $i = 1 \ldots D$ où $D = \sum_{\alpha \in V(\mathcal{I})} \mu(\alpha) = \sum_{\beta \in V(g)} \mu(\beta)$ ce qui montre en particulier que P_t et P_T ont mêmes fonctions symétriques élémentaires et par conséquent mêmes coefficients.
Le polynôme P_T étant le polynôme caractéristique de m_T, $P_T(T) \in \langle g(T)\rangle$ et donc $g(T)$ divise $P_T(T)$. Comme de plus $g(T)$ et P_T sont de mêmes degrés, il sont égaux (à multiplication par un scalaire près).
Supposons maintenant que t ne soit pas un élément séparant $V(\mathcal{I})$. Dans ce cas , le nombre de racines de $P_t = \sum_{\alpha \in V(\mathcal{I})} (T - t(\alpha))^{\mu(\alpha)}$ est strictement inférieur à $\sharp V(\mathcal{I})$ et par conséquent, le nombre de racines de $P_T = \sum_{\beta \in V(g)} (T - \beta)^{\mu(\beta)}$ est strictement inférieur à $\sharp V(g) = \sharp V(\mathcal{I})$, ce qui est impossible car $g(T)$ divise P_T.
En reprenant les notations de l'énoncé, ceci prouve en particulier que, par construction de la *représentation univariée rationelle* , $\mathcal{J}' = \langle g(T)\rangle$ et, en utilisant la remarque 4.2, $\gamma^\star$ coincide avec $\phi^\star$ sur $V(g)$. □

5 Propriétés de la Représentation Univariée Rationnelle

Nous avons vu dans la partie précédente que la *représentation univariée rationelle* permet de réduire l'étude des systèmes zéro-dimensionnels à celle d'un polynôme en une variable. Nous montrons maintenant que la μ-résolution permet de préserver le caractère *réel* des racines.

Proposition 5.1 *Soit $\mathcal{I} \subset K[X_1, \ldots, X_n]$ un idéal zéro-dimensionnel, $(\mathcal{J} \subset K[T], \phi^\star)$ une μ-résolution de $\mathcal{I}$ et R la clôture réelle de K. Alors, $\alpha \in V(\mathcal{I}) \bigcap R^n$ si et seulement si $(\phi^\star)^{-1}(\alpha) \in R$.*

Preuve : D'après la proposition 4.6, nous pouvons supposer que $(\mathcal{J}, \phi^\star)$ est la μ-résolution induite par la *représentation univariée rationelle* associée à un polynôme $t \in K[X_1, \ldots, X_n]$ séparant $V(\mathcal{I})$. Par conséquent, toujours d'après la proposition 4.6, $(\phi^\star)^{-1}$ coincide sur $V(\mathcal{I})$ avec le K-morphisme $\psi^\star$ déduit du morphisme d'algèbres :

$$\begin{array}{rccc} \psi : & K[T] & \longrightarrow & K[X_1, \ldots, X_n] \\ & T & \longmapsto & t \end{array}$$

Ainsi, $\forall \alpha \in V(\mathcal{I})$, $(\phi^\star)^{-1}(\alpha) = t(\alpha) \in V(\mathcal{J})$.
Comme $t \in K[X_1, \ldots, X_n]$, $\forall \alpha \in V(\mathcal{I}) \bigcap R^n$, $t(\alpha) \in R \bigcap V(\mathcal{J})$.
Inversement, supposons que $t(\alpha) \in R \bigcap V(\mathcal{J})$, pour $\alpha \in V(\mathcal{I})$ donné. Si α est un zéro de $\mathcal{I}$, son expression conjuguée $\bar{\alpha}$ est également un zéro de $\mathcal{I}$. Comme $t(\alpha) \in R$, $t(\alpha) = t(\bar{\alpha}) = t(\bar{\alpha})$. Comme de plus t sépare $\mathcal{I}$, $\bar{\alpha} = \alpha$ et donc $\alpha \in R^n$.
□

Ce résultat est d'une grande importance puisqu'il permet l'utilisation des nombreux outils réservés à l'étude des polynômes en une variable pour compter, isoler où encore coder *à la Thom* les racines réelles d'un système zéro-dimensionnel, comme nous le verrons dans le chapitre suivant.

Par les algorithmes existants et en particulier les bases de Groebner, le calcul du radical d'un idéal n'est pas une opération facile en pratique. Nous montrons, dans la fin de cette partie, que le calcul d'une μ-résolution du radical $\sqrt{(\mathcal{I})}$ d'un idéal zéro-dimensionnel n'est pas plus difficile que celui d'une μ-résolution de $\mathcal{I}$, puis nous établissons le lien, dans le cas particulier d'idéaux radicaux en position générique, entre la *représentation univariée rationelle* et une base de Groebner pour l'ordre lexicographique.

Definition 5.1 *Un ideal $\mathcal{I} \subset K[X_1, \ldots, X_n]$ est en* position générique *si X_1 est un polynôme séparant $V(\mathcal{I})$.*

Proposition 5.2 *Soit $\mathcal{I} \subset K[X_1, \ldots, X_n]$ un idéal en position générique. Les conditions suivantes sont équivalentes :*

- *(1) $\mathcal{I}$ est radical.*
- *(2) Pour toute μ-résolution $(h(T), \phi^\star)$ de $\mathcal{I}$, h est sans facteurs carrés.*

En particulier, si $\mathcal{I}$ est radical et si $(h(T), \phi^\star)$ est une μ-résolution de $\mathcal{I}$, $K[X_1, \ldots, X_n]/\mathcal{I}$ est isomorphe à $K[T]/h$.

Preuve : Sans perte de généralité, nous pouvons supposer que X_1 est un polynôme séparant $V(\mathcal{I})$. En effet , d'après le lemme 3.1, il existe un changement linéaire de variables tel que $\mathcal{I}$ soit en position générique.
(1) $\Rightarrow$ (2) : Soit $(h(T), \phi^\star)$ une μ-résolution de $\mathcal{I}$. Si $\mathcal{I}$ est radical, d'après la proposition 4.3, $K[X_1, \ldots, X_n]/\mathcal{I}$ est isomorphe à $K[T]/\sqrt{\langle h(T)\rangle}$. Comme de plus

$$dim_K(K[X_1, \ldots, X_n]/\mathcal{I}) = \sum_{\alpha \in V(\mathcal{I})} \mu(\alpha) = \sum_{\beta \in V(h)} \mu(\beta) = dim_K(K[T]/\langle h(T)\rangle$$

alors $\sqrt{\langle h(T)\rangle} = \langle h(T)\rangle$ et $h(T)$ est donc sans facteurs carrés.
(2) $\Rightarrow$ (1) : Soit $(f(T), \phi^\star)$ la μ-résolution induite par la *représentation univariée rationelle* associée à X_1. Rappelons qe dans ce cas, $f(T)$ est le polynôme caractéristique de l'application m_{X_1} et en particulier si d est le degré de f, $d = dim_K(K[X_1, \ldots, X_n]/\mathcal{I})$. Comme f est supposé être sans facteurs carrés, f est également le polynôme minimal de m_{X_1}, ce qui montre que $\{1, X_1, \ldots, X_1^{d-1}\}$ est une une base de $K[X_1, \ldots, X_n]/\mathcal{I}$. D'après le théorème de Cayley, $f(X_1) \in \mathcal{I}$, donc, le morphisme de K-algèbres de $K[X_1, \ldots, X_n]/\mathcal{I}$ dans $K[T]/f$ quit à X_1 associe T est un isomorphisme. L'ideal $\mathcal{I}$ est donc radical.
La dernière assertion de la proposition est une application directe de la proposition 4.3. □

Ceci nous donne alors un moyen simple de trouver une μ-résolution du radical d'un idéal zéro-dimensionnel donné :

Corollaire 5.1 *Soit $\mathcal{I}$ un idéal zéro-dimensionnel. Si $(f, \phi^\star)$ une μ-résolution de $\mathcal{I}$, alors $(f/gcd(f, f'), \phi^\star)$ est une μ-résolution de $\sqrt{\mathcal{I}}$.*

Preuve : D'après la proposition 4.6, il existe un polynôme t séparant $V(\mathcal{I})$ tel que $(f, \phi^\star)$ soit la μ-résolution induite par la *représentation univariée rationelle* de $\mathcal{I}$ associée à t. En remarquant que t sépare également $V(\sqrt{\mathcal{I}})$, si $(g, \psi^\star)$ est la μ-résolution induite par la *représentation univariée rationelle* de $\sqrt{\mathcal{I}}$ associée à t, g est sans facteurs carrés d'après la proposition précédente et g à mêmes racines que f (les $t(\alpha)$, $\alpha \in V(\mathcal{I})$) par construction de la *représentation univariée rationelle* . Par conséquent g est égal (à multiplication par un scalaire près) à la partie sans facteurs carrés de f. □

Remarquons en particulier que le calcul d'une *représentation univariée rationelle* du radical d'un idéal zéro-dimensionnel $\mathcal{I}$ est immédiat si une *représentation univariée rationelle* de $\mathcal{I}$ est connue (le calcul de $f/gcd(f, f')$ est en effet nécessaire pour calculer la *représentation univariée rationelle* de $\mathcal{I}$).
Les bases de Groebner lexicographiques sont souvent considérées comme étant une *résolution* des systèmes zéro-dimensionnels. Dans le cas général, aucune

relation simple n'apparait entre la *représentation univariée rationelle* et les bases de Groebner lexicographiques. Toutefois, nous allons montrer que dans le cas particulier d'un idéal radical en position générique, la *représentation univariée rationelle* permet de retrouver une base de Groebner lexicographique.
Rappelons deux résultats classiques concernant les bases de Groebner lexicographiques (voir [BMMT93],[Fau94],[GM89]):

Proposition 5.3 *Soit I un idéal zéro dimensionnel en position générique. Les conditions suivantes sont équivalentes :*

- (1) *: I est radical.*
- (2) *: $\exists f \in K[X_1]$, $\forall i = 1, \ldots, n \exists f_i \in K[X_1]$ tels que :*
  - *f est sans facteurs carrés.*
  - *$\forall i = 1, \ldots, n$, $deg(f_i) < deg(f)$*
  - *$I = \{f(X_1), X_2 - f_2, \ldots, X_n - f_n\}$*

Preuve :

- (2) $\Rightarrow$ (1) : Comme $I = \{f, X_1 - u_1, \ldots, X_n - u_n\}$, alors $K[X_1, \ldots, X_n]/I$ est isomorphe à $K[X_1]/f$ et donc si f est radical, I l'est aussi.
- (1) $\Rightarrow$ (2) : Soit f un générateur de $I \bigcap K[X_1]$. I étant un idéal radical, $I \bigcap K[X_1]$ l'est donc également et f est par conséquent sans facteurs carrés. Comme I est en position générique, $dim_K(K[X_1]/f) = dim_K(K[X_1, \ldots, X_n]/I)$. Ainsi, si d est le degré de f en X_1, $1, X_1, \ldots, X_1^{d-1}$ est une base de $K[X_1, \ldots, X_n]/I)$. Il ne reste plus alors qu'à exprimer les coordonnées de $X_2, \ldots, X_n$ dans cette nouvelle base pour conclure.

□

Corollaire 5.2 *Soit I un idéal zéro dimensionnel en position générique. Les conditions suivantes sont équivalentes :*

- (1) *: I est radical.*
- (2) *: Sa base de Groebner réduite pour l'ordre lexicographique est donnée par*

$$\{f(X_1), X_2 - f_2(X_1), \ldots, X_n - f_n(X_1)\}$$

avec f sans facteurs carrés et $X_1 < X_2 < \ldots < X_n$.

Preuve : $\{f, X_1 - f_1, \ldots, X_n - f_n\}$ est clairement une base de Groebner pour l'ordre lexicographique avec $X_1 < X_2 < \ldots < X_n$. Elle est réduite par définition $(deg(f_i) < deg(f))$ et d'après la proposition précédente, c'est un système de générateurs de I. □

Etablissons maintenant la relation entre *représentation univariée rationelle* et base de Groebner lexicographique :

Corollaire 5.3 *Soit $\mathcal{I}$ un idéal zéro-dimensionnel radical en position générique de base de Groebner lexixographique $\{f(X_1), X_2 - f_2(X_1), \ldots, X_n - f_n(X_1)\}$ $(X_1 < \ldots < X_n)$ et dont la représentation univariée rationelle associée à X_1 s'écrit $\{h(X_1, X_1)\ ,\ g(X_1, X_1)\ ,\ g_1(X_1, X_1), \ldots, g_n(X_1, X_1)\}$. Alors :*

- $f = h$
- $f' = g$
- $g(X_1)$ *est inversible modulo* $\mathcal{I}$ *et* $\forall i = 2 \ldots n\ f_i = g^{-1} g_i\ mod\ f$

Preuve : Par construction, f est le polynôme caractéristique de m_{X_1} dans $K[X_1, \ldots, X_n]/I$ il coincide donc avec le premier polynôme de la *représentation univariée rationelle* de $\mathcal{I}$ associée à X_1. Comme f est sans facteurs carrés, nous avons également $f' = g$ et par conséquent

$$f' f_i = g_i\ mod\ \mathcal{I} = \sqrt{\mathcal{I}}$$

car d'une part, $\forall \alpha \in V(\mathcal{I})\ X_i(\alpha) = f_i(X_1(\alpha))$ et d'autre part $\forall \alpha \in V(\mathcal{I})\ X_i(\alpha) = g_i(X_1, X_1(\alpha))/g(X_1, X_1(\alpha))$. Par conséquent,$g_i = (f')^{-1} f_i\ mod\ \mathcal{I}$, ou encore comme $g = f'$ est inversible modulo f et donc modulo $\mathcal{I}$ (voir preuve du théorème 4.1), $f_i = g^{-1} g_i\ mod\ \mathcal{I}$. Comme $f, g, g_2, \ldots, g_n, f_2, \ldots, f_n \subset K[X_1]$ alors

$$f_i = g^{-1} g_i\ mod\ (\mathcal{I} \bigcap K[X_1])\ , \forall i = 2 \ldots n$$

$\{f, f_2, \ldots, f_n\}$ étant une base de Groebner, il vient alors :

$$f_i = g^{-1} g_i\ mod\ f\ , \forall i = 2 \ldots n$$

□

6 Fonctions symétriques étendues et calcul de *représentation univariée rationelle*

Pour un idéal zéro-dimensionnel $\mathcal{I}$ donné, nous supposerons connue, dans cette section, une table de multiplication MT de $K[X_1, \ldots, X_n]/\mathcal{I}$, c'est à dire l'ensemble

des produits $\overrightarrow{\omega_i\omega_j}, \overrightarrow{X_k\omega_j} \in K[X_1,\ldots,X_n]/\mathcal{I}$ où $\mathcal{B} = \{\omega_1,\ldots,\omega_D\}$ est une base de $K[X_1,\ldots,X_n]/\mathcal{I}$ donnée.

D'après la proposition 4.4, si nous supposons connu un polynôme $t \in K[X_1,\ldots,X_n]$ séparant $V(\mathcal{I})$, les polynômes :

$$f(t,T) = \prod_{y\in V(\mathcal{I})} (T - t(y))^{\mu(y)}$$
$$g_i(t,T) = \sum_{x\in V(\mathcal{I})} X_i(x) \prod_{y\in V(\mathcal{I}),y\neq x} (T - t(y))$$

permettent de définir entièrement la *représentation univariée rationelle* de $\mathcal{I}$ associée à t.

L'objet de ce qui suit est de fournir un algorithme efficace pour calculer la famille de polynômes $\{f(t,T), g_i(t,T)\ ,\ i = 1\ldots n\}$ lorqu'un polynôme séparant est connu.

Une méthode de calcul est donnée par le lemme 4.1. D'un point de vue pratique, hormis la difficulté de calculer le polynôme caractéristique d'une matrice à coefficients polynômiaux, un nombre important d'informations inutiles sont fournies par cette méthode. En effet seuls les termes de degré 1 des polynômes $det(M_{t+SX_i} - TI)$ sont réellement utilisés alors qu'ils sont entièrement calculés.

L'idée est d'effectuer ce calcul à l'aide d'outils combinatoires pour utiliser, autant que possible,les informations contenues dans MT. Nous étendons les notions classiques de sommes de Newton et de fonctions symétriques élémentaires aux ensembles de points à plusieurs coordonnées et nous établissons alors une formule généralisant la relation de Newton.

La considération de fonctions symétriques et de sommes de Newton à plusieurs coordonnées est déjà présente dans [J93] et plus récement dans [Dal95] et [RRS94] où des formules très générales sont proposées. Dans l'esprit de [GVT95], nous présentons ici des résultats particuliers, adaptés au calcul de la *représentation univariée rationelle* .

6.1 Utilisation de fonctions symétriques étendues

D'après le théorème de Stickelberger, pour $h \in K[X_1,\ldots X_n]$ fixé, les valeurs propres de l'application m_{h^j} , $j \geq 0$ $i \in [1,\ldots,n]$ sont exactement les $h(\alpha)^j$, $\alpha \in V(\mathcal{I})$ avec pour multiplicités, les multiplicités respectives $\mu(\alpha)$ des $\alpha \in V(\mathcal{I})$. Par conséquent les sommes de Newton associées au polynôme $f(t,T)$ peuvent être facilement obtenues si l'on connait les traces : $Trace(m_{t^i})$ et ainsi, on peut déduire facilement, par la formule de Newton, les coefficients de $f(t,T)$ à partir de ces traces.

Le but de cette partie, est de montrer que l'on peut étendre ce processus pour le calcul des autres polynômes intervenant dans la *représentation univariée rationelle* de $\mathcal{I}$ associée à un polynôme séparant donné.

Nous aurons besoin, dans ce qui suit de la notion de multi-ensemble:

Definition 6.1 *Un multi-ensemble $\mathcal{Y} = (E(\mathcal{Y}), \mu_{\mathcal{Y}})$ est la donnée d'un ensemble fini $E(\mathcal{Y})$ et d'une application $\mu_{\mathcal{Y}}$ de $E(\mathcal{Y})$ dans $\mathbb{N}$.*
La cardinalité d'un multi-ensemble $\mathcal{Y}$ est alors définie par : $\sharp\mathcal{Y} = \sum_{y \in E(\mathcal{Y})} \mu_{\mathcal{Y}}(y)$.
Un multi-ensemble $\mathcal{X}$ est inclus dans $\mathcal{Y}$ si:

- $E(\mathcal{X}) \subset E(\mathcal{Y})$
- *Pour tout* $x \in \mathcal{X}$, $\mu_{\mathcal{X}}(x) \leq \mu_{\mathcal{Y}}(x)$

Pour tout entier i, $\mathcal{P}_i(\mathcal{Y})$ est l'ensemble des multi-ensembles de cardinal i contenus dans $\mathcal{Y}$ et $\mathcal{Y}_y$ est le multi-ensemble défini par $(E(\mathcal{Y}), \mu_{\mathcal{Y}_y})$, avec $\mu_{\mathcal{Y}_y}(y) = \mu_{\mathcal{Y}}(y) - 1$ et $\mu_{\mathcal{Y}_y}(z) = \mu_{\mathcal{Y}}(z)$ si $z \neq y$.
Enfin, pour toute famille $\{f_y\ ,\ y \in E(\mathcal{Y})\}$ d'éléments de C^n on notera :

$$\sum_{y \in \mathcal{Y}} f_y = \sum_{y \in E(\mathcal{Y})} \mu_{\mathcal{Y}}(y) f_y \quad et \quad \prod_{y \in \mathcal{Y}} f_y = \prod_{y \in E(\mathcal{Y})} f_y^{\mu_{\mathcal{Y}}(y)}.$$

Definition 6.2 *Soient t un polynôme de $K[X_1, \ldots, X_n]$ et $\mathcal{Y}$ un multi-ensemble de C^n. Nous noterons :*

- $S_i(t, \mathcal{Y}) = \sum_{\mathcal{Z} \subset \mathcal{P}_i(\mathcal{Y})} \prod_{y \in \mathcal{Z}} t(y)$ *la i^e fonction symétrique élémentaire associée au multi-ensemble* $(\{t(\beta), \beta \in E(\mathcal{Y})\}, \mu_{t(\beta)} : t(\beta) \longmapsto \mu_{\mathcal{Y}}(\beta))$.
- $N_i(t, \mathcal{Y}) = \sum_{y \in \mathcal{Y}} t(y)^i$ *la i^esomme de Newton associée au multi-ensemble* $(\{t(\beta), \beta \in E(\mathcal{Y})\}, \mu_{t(\beta)})$.

Pour les besoins de notre algorithme, nous étendons ces définitions classiques :
Etant donnés des polynômes t et $v \in K[X_1, \ldots, X_n]$ et un multi-ensemble $\mathcal{Y} \in C^n$ on definit :

- $S_i(v, t, \mathcal{Y}) = \sum_{y \in \mathcal{Y}} v(y) S_i(t, \mathcal{Y}_y)$
- $N_i(v, t, \mathcal{Y}) = \sum_{y \in \mathcal{Y}} v(y) t(y)^i$

En développant $f(t,T)$ et $h(v,t,T)$ (notations du lemme 4.1) nous pouvons remarquer qu'il est possible d'exprimer leurs coefficients en fonction des fonctions symétriques étendues introduites plus haut :

$$f(t,T) = \sum_{i=0}^{D} (-1)^i S_i(t,\mathcal{Y}) T^{D-i}$$

$$h(v,t,T) = \sum_{i=0}^{D-1} (-1)^i S_i(v,t,\mathcal{Y}) T^{D-i-1}$$

La formule classique de Newton reliant sommes de Newton et fonctions symétriques élémentaires s'écrit :

$$(D-i) S_i(t,\mathcal{Y}) = \sum_{j=0}^{i} (-1)^j N_j(t,\mathcal{Y}) S_{i-j}(t,\mathcal{Y})$$

avec la convention $S_0(t,\mathcal{Y}) = 1$. En utilisant la définition 6.2, la proposition suivante en est une généralisation:

Proposition 6.1

$$S_i(v,t,\mathcal{Y}) = \sum_{j=0}^{i} (-1)^j N_j(v,t,\mathcal{Y}) S_{i-j}(t,\mathcal{Y})$$

Pour prouver ce résultat, nous utiliserons le lemme suivant :

Lemme 6.1 *Pour* $0 \leq k < i$,

$$\sum_{y\in\mathcal{Y}} v(y) t(y)^k S_{i-k}(t,\mathcal{Y}_y) = N_k(v,t,\mathcal{Y}) S_{i-k}(t,\mathcal{Y}) - \sum_{y\in\mathcal{Y}} v(y) t(y)^{k+1} S_{i-k-1}(t,\mathcal{Y}_y)$$

Preuve du lemme : Pour tout entier k, $0 \leq k < i$,

$$N_k(v,t,\mathcal{Y}) S_{i-k}(t,\mathcal{Y}) = \left(\sum_{y\in\mathcal{Y}} v(y) t(y)^k \right) \left(\sum_{I\subset\mathcal{P}_{i-k}(\mathcal{Y})} \prod_{z\in I} t(z) \right)$$

$$= \sum_{y\in\mathcal{Y}} \sum_{I\subset\mathcal{P}_{i-k}(\mathcal{Y})} v(y) t(y)^k \textstyle\prod_{z\in I} t(z)$$

$$= \sum_{y\in\mathcal{Y}} \left(\sum_{I\subset\mathcal{P}_{i-k-1}(\mathcal{Y})} v(y) t(y)^k \prod_{z\in I_y} t(z) + \sum_{I\subset\mathcal{P}_{i-k-1}(\mathcal{Y})} v(y) t(y)^{k+1} \prod_{z\in I_y} t(z) \right)$$

$$= \sum_{y\in\mathcal{Y}} v(y) t(y)^k S_{i-k}(t,\mathcal{Y}_y) + \sum_{y\in\mathcal{Y}} v(y) t(y)^{k+1} S_{i-k-1}(t,\mathcal{Y}_y)$$

□

Preuve de la proposition 6.1 : D'après le lemme 6.1, nous avons :

$$S_i(v,t,\mathcal{Y}) = \sum_{y\in\mathcal{Y}} v(y)S_i(t,\mathcal{Y}_y) = N_0(v,t,\mathcal{Y})S_i(t,\mathcal{Y}) - \sum_{y\in\mathcal{Y}} v(y)t(y)S_{i-1}(t,\mathcal{Y}_y)$$

En utilisant le même argument, il vient alors par induction :

$$S_i(v,t,\mathcal{Y}) = \sum_{j=0}^{i-1}(-1)^j N_j(v,t,\mathcal{Y})S_{i-j}(t,\mathcal{Y}) + (-1)^i \sum_{y\in\mathcal{Y}} v(y)t(y)^i S_0(t,\mathcal{Y}_y)$$

Comme $S_0(t,\mathcal{Y}_y) = 1$ le résultat est prouvé. □

D'après le théorème de Stickelberger,

$$N_i(v,t,\mathcal{Y}) = Trace(m_{vt^i})$$

$$N_i(t,\mathcal{Y}) = Trace(m_{t^i})$$

ce qui amène alors naturellement la proposition :

Proposition 6.2 *Soient $S = \{f_1,\ldots,f_s\}$ un système zéro-dimensionnel $\subset K[X_1,\ldots,X_n]$, D la dimension du K-espace vectoriel $K[X_1,\ldots,X_n]/\langle\mathcal{S}\rangle$ et $t \in [X_1,\ldots,X_n]$.*
Il est possible de calculer les polynômes (notations du lemme 4.1)

$$f(t,T), h(X_1,t,T),\ldots h(X_n,t,T)$$

à partir des traces :

$$Trace(m_{X_j t^i})\ ,\ i = 1\ldots D-1\ ,j = 1,\ldots n$$

$$Trace(m_{t^i})\ ,\ i = 1\ldots D$$

en résolvant n systèmes linéaires triangulaires.
D'après le lemme 4.1, en divisant les polynômes $h(X_i,t,T)$ ainsi que $f'(t,T)$ par $gcd(f,f')$ nous obtenons alors les polynômes

$$f(t,T)\ ,\ g(t,T)\ ,\ g_1(t,T),\ldots g_n(t,T)$$

de la représentation univariée rationelle de $\mathcal{I}$ associée à t.

6.2 Calcul des sommes de Newton étendues

D'après la partie précédente, il existe un moyen simple de calculer la *représentation univariée rationelle* de $\mathcal{I}$ associée à un polynôme séparant t donné à partir des traces : $Trace(m_{vt^i})$, $i = 1, \ldots, D-1$ et $Trace(m_{t^i})$, $i = 1, \ldots, D$.

Pour une base $\mathcal{B} = \{(\omega_1 \ldots \omega_D\}$ de $A = K[X_1, \ldots, X_n]/\mathcal{I}$ donnée, en supposant que nous disposions d'une table contenant tous les produits $\omega_i\omega_j$, il est possible de calculer simplement, toutes les traces de la forme $Trace(m_{vt^i})$, en utilisant le lemme 3.3 .
Pour tout $h \in K[X_1, \ldots X_n]/\mathcal{I}$, notons M_h la matrice de m_h dans la base $\mathcal{B}$.
D'après le lemme 3.3, en posant $Vtr = [Trace(\omega_1), \ldots, Trace(\omega_D)]$, pour tout $i = 1 \ldots D$ et tout $j = 1 \ldots n$ on peut écrire :

$$Trace(t^i) = \overrightarrow{t^i} \cdot Vtr = (M_t \cdot \overrightarrow{t^{i-1}}) \cdot Vtr$$

$$Trace(X_j t^i) = \overrightarrow{X_j t^i} \cdot Vtr = (M_{X_j} \cdot \overrightarrow{t^i}) \cdot Vtr$$

Ainsi, connaissant Vtr, un algorithme simple s'écrira :

Algorithme TracesToExtNewton-0

Entrée: Vtr, M_t, $M_{X_1}, \ldots, M_{X_n}$.

- **Etape 1 :** $t^0 = [1, 0, \ldots, 0]$
- **Etape 2 :** Pour $i = 0 \ldots (D-1)$,
  - $Trace(t^i) = \overrightarrow{t^i} \cdot Vtr$
  - Pour $j = 1 \ldots n$, $Trace(X_j t^i) = (M_{X_j} \cdot \overrightarrow{t^i}) \cdot Vtr$
  - $\overrightarrow{t^{i+1}} = M_t \overrightarrow{t^i}$
- **Etape 3 :** $Trace(t^D) = \overrightarrow{t^D} Vtr$

Sortie: $Trace(t^i)$, $i = 0 \ldots D$ et $Trace(X_j t^i)$, $i = 0 \ldots (D-1)$, $j = 1 \ldots n$

Cette version naive de l'algorithme entraine un nombre d'opérations arithmétiques en $O(n \cdot D^3)$. Il est toutefois possible de combiner plus astucieusement les propriétés de linéarité de l'application $Trace$ pour réduire de façon significative le nombre d'opérations arithmétiques nécessaires pour obtenir un méthode en $O(D^3 + n \cdot D^2)$.

En effet, pour tout $i = 1 \ldots (D-1)$ et tout $j = 1 \ldots n$,

$$Trace(t^{i+1}) = \overrightarrow{t} \cdot Vtr(t^i)$$

$$Trace(X_j t^i) = \overrightarrow{X_j} \cdot Vtr(t^i)$$

où $Vtr(t^i) = [Trace(t^i\omega_1), \ldots, Trace(t^i\omega_D)]$. Pour i fixé, il est donc possible de calculer simultanément $Trace(t^{i+1})$ et $Trace(X_j t^i)$, $j = 1 \ldots n$ dès lors que $Vtr(t^i)$ est connu.
D'après le lemme 3.3,

$$Trace(t^i\omega_k) = \overrightarrow{t\omega_k} \cdot Vtr(t^{i-1})$$

Par conséquent, si $(M_t)^T$ est la transposée de M_t, nous aurons :

$$Vtr(t^i) = (M_t)^T \cdot Vtr(t^{i-1})$$

Ces diverses relations nous donnent alors un algorithme pour obtenir les sommes de Newton étendues nécessaires au calcul de la *représentation univariée rationelle* :

Algorithme TracesToExtNewton

Entrée: Vtr, M_t, $M_{X_1}, \ldots, M_{X_n}$.

- **Etape 1 :** $Trace(t^0) = D$, $Vtr(t^0) = Vtr$
- **Etape 2 :** Pour $i = 0 \ldots (D-1)$,
  - $Trace(t^{i+1}) = \overrightarrow{t} \cdot Vtr(t^i)$
  - Pour $j = 1 \ldots n$, $Trace(X_j t^i) = \overrightarrow{X_j} \cdot Vtr(t^i)$
  - $Vtr(t^{i+1}) = (M_t)^T \cdot Vtr(t^i)$

Sortie: $Trace(t^i)$, $i = 0 \ldots D$ et $Trace(X_j t^i)$, $i = 0 \ldots (D-1)$, $j = 1 \ldots n$

6.3 Le problème de l'élément séparant

Dans cette section, nous proposons un algorithme complet pour le calcul d'une *représentation univariée rationelle* d'un idéal zéro-dimensionnel. Nous avons vu dans une section précédente comment calculer cette représentation à partir d'un polynôme séparant $V(\mathcal{I})$ connu, nous proposons ici une méthode générale.

Il n'apparait pas raisonable d'espèrer trouver un polynôme séparant sans aucun calcul. Nous avons pu voir que l'ensemble des formes linéaires

$$\mathcal{U} = \{X_1 + iX_2 + \ldots + i^{n-1}X_n \ , \ i = 1, \ldots, D\}$$

contient au moins un polynôme séparant $V(\mathcal{I})$.

Une idée simple, mais peu économique, consisterait à calculer tous les polynômes caractéristiques de tous les éléments de $\mathcal{U}$, pour garder un de ceux dont le polynôme caractéristique admet un nombre maximum de racines (i.e : dont le degré de la partie sans facteurs carrés est maximum).

Comme un polynôme générique est séparant, notre but est ici de fournir un test de validité a postériori, venant après le calcul de la *représentation univariée rationelle* associée à un polynôme quelconque, pour détecter si celui-ci est séparant où non.

Soient $\{f(t,T), g(t,T), g_1(t,T), \ldots, g_n(t,T)\}$ les polynômes donnés par la proposition 4.4. Le lemme suivant sera à la base des divers résultats de cette partie :

Lemme 6.2 *Un polynôme $t \in K[X_1, \ldots, X_n]$ est séparant pour $V(\mathcal{I})$ si et seulement si:*

$$\forall i = 1 \ldots n \ , \ u_i(t) = g(t,t)X_i - g_1(t,t) \in \sqrt{\mathcal{I}}.$$

Preuve :

- $\Rightarrow$: Supposons que t soit séparant. Nous avons alors,

$$\forall \beta \in V(\mathcal{I}) \ , \ X_i(\beta) = \frac{g_i(t, t(\beta))}{g(t, t(\beta))}.$$

  Ainsi, $u_i(t(\beta)) = 0$ et donc, $u_i(t) \in \sqrt{\mathcal{I}}$.

- $\Leftarrow$: Supposons que t ne soit pas séparant et que $\forall i = 1, \ldots, n \ u_i(t) \in \sqrt{\mathcal{I}}$. Soient alors α et β deux racines distintes de $\mathcal{S}$ telles que $t(\alpha) = t(\beta)$. Comme $\alpha \neq \beta$,il existe un indice i tel que $X_i(\alpha) \neq X_i(\beta)$. Toutefois, $u_i(t) \in \sqrt{\mathcal{I}}$ et donc, $u_i(t(\alpha)) = u_i(t(\beta)) = 0$. Par définition de u_i et comme $g(t,t)$ ne s'annule pas sur $V(\mathcal{I})$, nous avons :

$$X_i(\beta) = \frac{g_i(t, t(\beta))}{g(t, t(\beta))}$$

$$X_i(\alpha) = \frac{g_i(t, t(\alpha))}{g(t, t(\alpha))}$$

  Mais $t(\alpha) = t(\beta) \Rightarrow X_i(\beta) = X_i(\alpha)$, ce qui contredit es hypothèses.

□

Le problème de vérifiation est maintenant ramené à un test d'appartenance au radial d'un idéal. En adaptant la proposition 3.2 à notre problème , nous obtenons alors le corollaire suivant :

Corollaire 6.1 *Soient* $t \in K[X_1, \ldots, X_n]$ *et* $g_1(t,T), \ldots, g_n(t,T)$ *les polynômes définissant une représentation univariée rationelle . En posant, pour tout* $h \in K[X_1, \ldots, X_n]$, $Vtr(h) = [Trace(m_{h\omega_1}), \ldots Trace(m_{\omega_D})]$, *d'après la proposition 3.2 l'élément* t *est séparant si et seulement si :*

$$Vtr(u_i(t)) = 0$$

pour tout $i = 1 \ldots n$. *En posant :*

- $d = degree(f(t))$
- $g(t,t) = \sum_{j=1}^{d-1} a_j t^j$ *et* $g_i(t,t) = \sum_{j=1}^{d-1} a_j^i t^j$.

cette condition peut être traduite par :

$$M_{X_i}^T \left(\sum_{j=1}^{d-1} a_j Vtr(t^j) \right) - \sum_{j=1}^{d-1} a_j^i Vtr(t^j) = 0$$

pour tout $i = 1 \ldots n$.

Preuve : En utilisant la linéarité de l'appliation $Trace$, on peut écrire :

$$\begin{aligned} Vtr(u_i(t)) &= Vtr(g(t)X_i) - Vtr(g_i(t)) \\ &= [Trace(g(t)X_1\omega_1), \ldots, Trace(g(t)X_1\omega_D)] - \textstyle\sum_{j=1}^{d-1} a_j^i Vtr(t^j) \\ &= [\overrightarrow{X_i\omega_1} Vtr(g(t)), \ldots, \overrightarrow{X_i\omega_D} Vtr(g(t))] - \textstyle\sum_{j=1}^{d-1} a_j^i Vtr(t^j) \\ &= M_{X_i}^T Vtr(g(t)) - \textstyle\sum_{j=1}^{d-1} a_j^i Vtr(t^j) \\ &= M_{X_i}^T \left(\textstyle\sum_j = 1^{d-1} a_j Vtr(t^j) \right) - \textstyle\sum_{j=1}^{d-1} a_j^i Vtr(t^j) \end{aligned}$$

□

Remarque 6.1 *Si l'algorithme* **TracesToExtNewton** *à été utilisé pour calculer la représentation univariée rationelle , tous les vecteurs* $Vtr(t^j)$ *sont déjà connus (voir preuve de l'algorithme) ce qui rend ce test performant.*
Si $g(t,T)$ *est de degré* $D-1$, $f(t,T)/gcd(f(t,T), f'(t,T))$ *est forcement de degré maximum. Dans ce cas* t *est séparant et l'on sait de plus que* $\mathcal{I}$ *est radical.*

Ceci nous donne un algorithme pour tester, a postériori, si un polynôme arbitrairement choisi est séparant où non :

Algorithme TestSep

Entrée: Une table de multiplication MT de $K[X_1,\ldots,X_n]/\mathcal{I}$, la *représentation univariée rationelle* associée à un polynôme t :

$$\{f(t,t), g(t,t), g_1(t,t), \ldots, g_n(t,t)\}$$

(avec : $g(t,t) = \sum_{j=1}^{d-1} a_j t^j$ et $g_i(t,t) = \sum_{j=1}^{d-1} a_j^i t^j$, pour tout $i = 1\ldots n$), ainsi que les vecteurs $Vtr(t^j)$ pour $j = 0,\ldots,D-1$.

- **Etape 0** : Si $g(t,T)$ est de degré $D-1$, t est séparant.
- **Etape 1** : Calcul de $Vtr(g(t,T)) = \sum_{j=1}^{d-1} a_j Vtr(t^j)$.
- **Etape 2** : Pour $i = 1,\ldots,n$, calcul de :
  - $Vtr(g(t,T)X_i) = M_{X_i}^T Vtr(g(t,T))$
  - $Vtr(g_i(t)) = \sum_{j=1}^{d-1} a_j^i Vtr(t^j)$
  - $Vtr(u_i(t)) = Vtr(g(t,T)X_i) - Vtr(g_i(t))$

Sortie: **Vrai** si t est séparant (c'est à dire si $Vtr(u_i(t)) = 0$, pour tout $i = 1\ldots n$ ou si $g(t,T)$ est de degré $D-1$), **Faux** sinon.

Si nous faisons un bilan des différents résultats abordés dans ce chapitre, nous pouvons exhiber un algorithme complet pour le calcul de la *représentation univariée rationelle* d'un système zéro-dimensionnel. En supposant que le point d'entrée est une table de multiplication MT de $K[X_1,\ldots,X_n]/\mathcal{I}$, c'est à dire la donnée d'une base $\mathcal{B} = \{\omega_1,\ldots,\omega_D\}$ de $K[X_1,\ldots,X_n]/\mathcal{I}$ et de tous les produits réduits $\overrightarrow{\omega_i\omega_j}$, nous suggérons l'algorithme :

Algorithme RUR

Entrée: MT

- **Etape 1** : Choix d'une forme linéaire (lemme 3.1) t parmi :

$$\{X_1 + iX_2 + \ldots + i^{n-1}X_n \ , \ i = 1,\ldots,D\}$$

- **Etape 2** : Calcul des Traces (TracesToExtNewton)
- **Etape 3** : Déduction des polynômes (formule de Newton étendue)

$$f(t,T), u_1(t,T), \ldots, u_n(t,T)$$

- **Etape 4** : Calcul de :

$$g(t,t) = f'/gcd(f(t,T), f'(t,T))$$

et, pout tout $i = 1,\ldots,n$, de :

$$g_i(t,T) = h(X_i,t,T)/gcd(f(t,T), f'(t,T))$$

- **Etape 5** : Test de l'élément séparant (TestSep). Si t n'est pas séparant, retourner à l'étape **1**.

Sortie: Un polynôme t séparant $V(\mathcal{I})$ et la *représentation univariée rationelle* $g(t,T), g_1(t,T), \ldots, g_n(t,T)$ correspondante.

7 Complexité

L'entrée de l'algorithme *représentation univariée rationelle* étant une table de multiplication MT associée à l'idéal zéro-dimensionnel que nous étudions, il est naturel de ne considérer que les paramêtres liés à cette représentation.

Proposition 7.1 *Soit $\mathcal{I} \subset K[X_1, \ldots, X_n]$ un idéal zéro-dimensionnel et MT une table de multiplication de $K[X_1, \ldots, X_n]/\mathcal{I}$. Notons D la dimension de l'espace vectoriel $K[X_1, \ldots, X_n]/\mathcal{I}$ dont une base sera notée $[\omega_1, \ldots, \omega_D]$ et supposons donné un polynôme t séparant $\mathcal{I}$. La représentation univariée rationelle de $\mathcal{I}$ associée à t se déduit de MT en*

$$O(D^3 + nD^2)$$

opérations arithmétiques.
Dans le cas où aucun vecteur séparant n'est connu a priori, le processus utilisera alors au maximum

$$O(n^2 d^2 D^3)$$

opérations arithmétiques où d est le nombre de racines distinctes du système.

Preuve : énumérons une à une les diverses étapes décrites plus haut pour le calcul de la *représentation univariée rationelle* de $\mathcal{I}$ associé à t :

- Le calcul préalable à l'algorithme TracesToExtNewton consiste à former le vecteur

  $$[Trace(\omega_1), \ldots, Trace(\omega_D)]$$

  Chaque trace $Trace(\omega_i)$ requiert D additions lorsque la table MT est connue. Le nombre d'opérations induites par cette étape est donc $O(D^2)$.

- Calcul des sommes de Newton étendues : L'algorithme TracesToExtNewton utilise clairement D multiplications Matrice-Vecteur de dimension D et $D(n+1)$ produits scalaires de deux vecteurs de dimension D. Le nombre d'opérations induites par cette étape est donc $O(D^3 + nD^2)$.

- Le calcul des coefficients des différents polynômes $\{f, h(X_1, t, T), \ldots, h(X_n, t, T)\}$ (voir lemme 4.1) s'effectue en résolvant $n+1$ systèmes triangulaires. Le nombre d'opérations induites par cette étape est donc $O(nD^2)$ et d'après le lemme 4.1 les polynômes de la *représentation univariée rationelle* se déduisent en $O(nD^2)$ opérations arithmétiques.

En ce qui concerne le processus global, il faut inclure :

- Le test a postériori de validité de l'élément séparant est en $O(nD^2)$ et ne modifie en rien la complexité de l'algorithme.
- Le nombre de polynômes potentiellement non séparants que nous pouvons avoir à tester:
$$(n-1)d(d-1)/2$$
si d est le nombre de racines complexes distinctes.

□

Dans le cas des systèmes à coefficients entiers où rationnels, nous pouvons également mesurer les tailles des représentations binaires des entiers apparaissant dans le résultat d'une représentation univariée rationnelle. En reprenant les notations du lemme 4.1, nous nous attachons dans un premier temps à l'étude du calcul de la famille de polynômes :

$$\mathcal{R} = \{f, h(X_1, t, T), \ldots, h(X_n, t, T)\}$$

Proposition 7.2 *Soient $\mathcal{I} \subset \mathbb{Z}[X_1, \ldots, X_n]$ un idéal zéro-dimensionnel et MT une table de multiplication de $\mathbb{Q}[X_1, \ldots, X_n]/\mathcal{I}$. Notons D la dimension de l'espace vectoriel $\mathbb{Q}[X_1, \ldots, X_n]/\mathcal{I}$ et $\mathcal{T}_1$ la taille maximale d'un coefficient apparaissant dans le sous-ensemble de MT :*

$$\{X_i\omega_j \ , \ i = 1..n \ , \ j = 1 \ldots D\}$$

($\mathcal{T}_1 \geq \mathcal{T}$). La taille maximale d'un coefficient apparaissant dans les polynômes de $\mathcal{R}$ est en

$$O(D(\mathcal{T}_1 + log(D)))$$

lorsque l'un des X_i sépare $V(\mathcal{I})$, et en

$$O(D(\mathcal{T}_1 + nlog(nD)))$$

lorsqu'un polynôme t séparant $\mathcal{I}$ est choisi dans l'ensemble

$$\{X_1 + iX_2 + \ldots + i^{n-1}X_n \ i = 0 \ldots (n-1)d(d-1)/2\}.$$

Preuve : Les polynômes $\{f, h(X_1, t, T), \ldots, h(X_n, t, T)\}$ peuvent être obtenus par des calculs de polynômes caractéristiques. Si $\mathcal{T}_2$ est la taille maximale des coefficients apparaissant dans les matrices $M_t, M_{X_1}, \ldots, M_{X_n}$, la taille d'un coefficient apparaissant dans les determinants de la forme $Det(M_{t+SX_i} - TI)$ est alors en $O(D(\mathcal{T}_2 + log(D)))$ et par conséquent la taile maximum d'un coefficient apparaissant dans $\mathcal{R}$, (c'est à dire dans les expressions $\left(\frac{\partial}{\partial S} Det(M_{t+SX_i})\right)_{S=0}$) est en $O(D(\mathcal{T}_2 + log(D)))$. Si t est l'un des X_i, $\mathcal{T}_2 = \mathcal{T}_1$. Dans le cas contraire, la matrice M_t est une combinaison linéaire des matrices M_{X_i} de la forme $\sum_{i=1}^{n} a_i M_{X_i}$ où les a_i sont des entiers inférieurs à $(nD^2)^n$, par conséquent $\mathcal{T}_2 = O(\mathcal{T}_1 + nlog(nD))$. □

Nous avons calculé le nombre d'opérations arithmétiques utilisées lorsque l'algorithme **RUR** est appliqué pour calculer la *représentation univariée rationelle* d'un système et nous avons fourni une borne sur la taille des coefficients du résultat. Nous montrons maintenant le bon comportement de cet algorithme en calculant la taille des coefficients intervenant en cours de calcul :

Proposition 7.3 *En reprenant les notations de la proposition précédente, la taille des coefficients apparaissant dans le calcul de $\mathcal{R}$ par l'algorithme RUR est*

$$O(D(\mathcal{T}_1 + log(D)))$$

lorsque l'un des X_i sépare $V(\mathcal{I})$, et en

$$O(D(\mathcal{T}_1 + nlog(nD)))$$

dans le cas général.

Preuve : Reprenons une à une les différentes étapes du calcul de $\mathcal{R}$ par l'algorithme RUR pour étudier le comportement des données dans les calculs intermédiaires dans le cas général :

- Le calcul préalable à l'algorithme TracesToExtNewton consiste à former le vecteur
$$Vtr = [Trace(\omega_1), \ldots, Trace(\omega_D)]$$
Chaque trace $Trace(\omega_i) = \sum_{i=1}^{D} (\omega_i \omega_j)_j$ requiert D additions de coefficients dont la taille est $O(D\mathcal{T}_1)$ (taille des coeficients apparaissant dans la table de multiplication - voir [R96]), les coefficients apparaissant dans Vtr sont par conséquent de taille $O(D\mathcal{T}_1 + log(D))$.

- Calcul des sommes de Newton étendues : La construction des vecteurs $Vtr(t^i)$ s'effectue itérativement par la formule :
$$Vtr(t^i) = M_t^T \cdot Vtr(t^{i-1})$$

avec $Vtr(t^0) = Vtr$.

D'après la démonstration de la proposition précédente, la taille d'un coefficient apparaissant dans M_t est en $O(\mathcal{T}_1 + nlog(nD))$ et par conséquent la taille maximale d'un coefficient apparaissant dans $Vtr(t^i)$, $i = 1 \ldots D$ est en $O(D(\mathcal{T}_1 + nlog(nD)))$. Les traces $Trace(X_j t^i)$ et $Trace(t^{i+1})$ étant calculées par la formules : $Trace(X_j t^i) = \overrightarrow{X_i} \cdot Vtr(t^i)$ et $Trace(t^{i+1}) = \overrightarrow{t} \cdot Vtr(t^i)$, leur taille est également en $O(D(\mathcal{T} + nlog(nD)))$.

- Les coefficients des différents polynômes de $\mathcal{R}$ sont obtenus en résolvant $n+1$ systèmes triangulaires par subsitutions successives (par une méthode sans fractions). Comme la taille des entiers intervenant dans le résultat est en $O(D(\mathcal{T}_1 + nlog(nD)))$ et que les coefficients apparaissant dans l'expression des systèmes sont de taille $O(D(\mathcal{T}_1 + nlog(nD)))$, les calculs intermédiaires feront intervenir des entiers de taille maximale $O(D(\mathcal{T}_1 + nlog(nD)))$.

Le même raisonnement s'applique dans le cas où l'un des X_i sépare $V(\mathcal{I})$. La taille maximum d'un coefficient apparaissant dans M_t étant dans ce cas en $O(\mathcal{T}_1 + log(D))$, les calculs intermédiaires feront alors intervenir des entiers de taille maximale $O(D(\mathcal{T}_1 + log(D)))$. □

Lorsque toutes les racines du système sont simples, $\mathcal{R}$ coincide avec une *représentation univariée rationelle* de $\mathcal{I}$, mais dans le cas contraire, rappelons que la *représentation univariée rationelle* est obtenue en divisant les polynômes $f', h(X_1, t, T), \ldots, h(X_r$ par $gcd(f, f')$. Une analyse rapide de la complexité nous donne une taille maximale de coefficients en $O(D^2(\mathcal{T}_1 + nlog(nD)))$ dans le cas général.
Notons que dans ce cas, le calcul de pgcd ($gcd(f, f')$), les n divisions nécessaires pour le calcul des polynômes de la représentation univariée rationnelle ainsi que le test (TestSep) sont effectués en utilisant des entiers de taille $O(D^2(\mathcal{T}_1 + nlog(nD)))$. Ces $O(nD^2)$ opérations ne peuvent par conséquent plus être négligés par rapport au reste ($O(D^3 + nD^2)$ opérations arithmétiques sur des entiers de taille $O(D(\mathcal{T}_1 + nlog(nD)))$).
En pratique toutefois, les coefficients d'un pgcd sont en général plus petit que ceux des polynômes considérés et cette analyse ne correspond donc pas avec les résultats observées, les coefficients des polynômes de la *représentation univariée rationelle* étant en général plus petits que ceux des polynômes de $\mathcal{R}$.

8 Cas des systèmes à coefficients entiers

Nous revenons dans cette partie sur certaines étapes de l'algorithme RUR dans le cas de systèmes à coefficients entiers, et en particulier sur le problème de l'élément séparant. L'idéal de $\mathbb{Z}[X_1, \ldots X_n]$ considéré sera noté $\mathcal{I}$, D sera la dimension de

$\mathbb{Z}[X_1,\ldots,X_n]/\mathcal{I}$ et le nombre de racines distinctes du système (dans $\mathbb{C}^n$) sera noté $d = \sharp V(\mathcal{I})$.
La pratique montre que, pour obtenir des expressions finales plus simples, nous devons considérer en priorité les polynômes de la forme X_i , $i = 1\ldots n$ comme séparant potentiellement $V(\mathcal{I})$. Il est toutefois fréquent qu'un polynôme séparant $V(\mathcal{I})$ ne soit pas de la forme X_i , $i = 1\ldots n$. Dans ce cas, l'algorithme RUR sera exécuté (au moins $n+1$ fois) dans sa totalité en prenant t dans la famille $\{X_1,\ldots,X_n, X_1+iX_2+\ldots+i^{n-1}X_n$, $i = 1\ldots(n-1)d(d-1)/2\}$ jusqu'à l'obtention d'une représentation univariée de $\mathcal{I}$.
Compte tenu du coût, en pratique, de l'algorithme RUR, nous proposons ici une prédiction, par un calcul modulaire (donc rapide), d'un polynôme séparant et une autre méthode pour vérifier a posteriori si celui-ci sépare effectivement $V(\mathcal{I})$.
Comme pour tout algorithme utilisant une technique modulaire, il nous faut, dans un premier temps définir une notion d'*entier premier de bonne réduction*, en nous limitant toutefois au cas où l'idéal $\mathcal{I}$ est représenté par une base de Groebner pour un ordre arbitraire (que nous noterons $>$) sur les monômes.

8.1 Entiers de bonne réduction pour la *représentation univariée rationelle*

Si on applique l'algorithme de Buchberger classique pour calculer la base de Groebner d'un idéal de $\mathbb{Z}[X_1,\ldots,X_n]$ (pour un ordre fixé $>$) , nous obtenons une famille de polynômes de $\mathcal{G} \subset \mathbb{Q}[X_1,\ldots,X_n]$. Toutefois, nous pouvons remarquer que pour tout $a \in \mathbb{Z}$, $a \neq 0$, si $\mathcal{G}$ est une base de Groebner de $\mathcal{I}$, l'ensemble $\{ag$, $g \in \mathcal{G}\}$ est encore une base de Groebner de $\mathcal{I}$ pour $>$. En choisissant cet entier de façon correcte, nous pouvons donc supposer que pour l'ordre $>$, $\mathcal{G} \subset \mathbb{Z}[X_1,\ldots,X_n]$.

Malgré ce changement, pour tout $h \in \mathbb{Z}[X_1,\ldots,X_n]$, le résultat de la réduction de h modulo $\mathcal{G}$ est encore un élément de $\mathbb{Q}[X_1,\ldots,X_n]$, mais comme dans le cas des polynômes en une variable , on peut facilement remarquer que le reste de la division de $lc(g)^{tdeg(f)-tdeg(g)+1}h$ par g est lui un polynôme de $\mathbb{Z}[X_1,\ldots,X_n]$, ce qui nous conduit à énoncer le lemme :

Lemme 8.1 *Pour tout polynôme $h \in \mathbb{Z}[X_1,\ldots,X_n]$, il existe des entiers positifs n_g , $g \in \mathcal{G}$ tels que ;*

$$NF((\prod_{g\in\mathcal{G}} lc(g)^{n_g})\cdot h, \mathcal{G}) \in \mathbb{Z}[X_1,\ldots,X_n]$$

et des polynômes q_g , $g \in \mathcal{G}$, $q_g \in \mathbb{Z}[X_1,\ldots,X_n]$ tels que

$$(\prod_{g\in\mathcal{G}} lc(g)^{n_g})\cdot h = NF((\prod_{g\in\mathcal{G}} lc(g)^{n_g})\cdot h, \mathcal{G}) + \sum_{g\in\mathcal{G}} q_g \cdot g$$

Notation 8.1 *Pour tout $p \in \mathbb{Z}$ premier, nous noterons $\mathbb{Z}_p$ le localisé de $\mathbb{Z}$ en $p\mathbb{Z}$, c'est à dire le sous anneau de $\mathbb{Q}$:*

$$\mathbb{Z}_p = \{a/b\ ,\ a \in \mathbb{Z}\ , b \in \mathbb{Z}\ | p \text{ ne divise pas } b\},$$

$GF(p)$ le corps fini d'ordre p,$\mathbb{Z}/p\mathbb{Z}$ et $\overline{GF(p)}$ sa clôture algébrique.
$\phi_p : \mathbb{Z}_p[X_1, \ldots, X_n] \longrightarrow GF(p)[X_1, \ldots, X_n]$ sera alors le morphisme canonique tel que $\forall a/b \in \mathbb{Z}_p\ ,\ \phi_p(a/b) = (a \bmod p)(b \bmod p)^{-1}$.

Definition 8.1 *Nous dirons qu'un entier premier p est $\mathcal{G}$-compatible (pour l'ordre $>$), si p ne divise aucun des $lc(g)$, $g \in \mathcal{G}$.*

Proposition 8.1 *Soit $\mathcal{G}$ une base de Groebner réduite d'un idéal zéro-dimensionnel $\mathcal{I} \subset \mathbb{Z}[X_1, \ldots, X_n]$ pour un ordre $>$. Si p est un entier premier $\mathcal{G}$-compatible pour $>$, alors $\phi_p(\mathcal{G})$ est une base de Groebner de $\langle \phi_p(\mathcal{G}) \rangle$ (pour $>$) et $\phi_p(NF(f, \mathcal{G})) = NF(\phi_p(f), \phi_p(\mathcal{G}))$*

Pour établir cette proposition, nous aurons besoin d'un résultat intermédiaire :

Lemme 8.2 *Soit $\mathcal{G} \in \mathbb{Z}[X_1, \ldots, X_n]$ une base de Groebner réduite d'un idéal zéro-dimensionnel $\mathcal{I}$ pour $>$ et p un entier premier $\mathcal{G}$-compatible pour $>$. Pour tout $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ l'expression suivante est unique :*

$$f = \sum_{g \in \mathcal{G}} q_g g + r_f$$

avec r_f tel que aucun de ses monômes ne soit divisible par l'un des $lm(g)$, $g \in \mathcal{G}$, et de plus :

- *(1) $\forall g \in \mathcal{G}\ ,\ q_g \in \mathbb{Z}_p[X_1, \ldots, X_n]$*
- *(2) $r_f \in \mathbb{Z}_p[X_1, \ldots, X_n]$*
- *(3) Pour tout $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$, on peut ordonner les polynômes de $\mathcal{G}$ de telle sorte que :*

$$\phi_p(NF(f, \mathcal{G})) = NF(\phi_p(f), \phi_p(\mathcal{G}))$$

Preuve : Supposons dans un premier temps que f soit un polynôme de $\mathbb{Z}[X_1, \ldots X_n]$. Comme $\mathcal{G}$ est une base de Groebner réduite de $\mathcal{I}$, l'expression

$$f = \sum_{g \in \mathcal{G}} q_g g + r_f$$

est unique. En reprenant les notations du lemme 8.1, il existe des entiers positifs n_g , $g \in \mathcal{G}$ tels que ;

$$NF((\prod_{g\in\mathcal{G}} lc(g)^{n_g}) \cdot h, \mathcal{G}) \in \mathbb{Z}[X_1, \ldots, X_n]$$

et des polynômes q_g , $g \in \mathcal{G}$, $q_g \in \mathbb{Z}[X_1, \ldots, X_n]$ tels que

$$(\prod_{g\in\mathcal{G}} lc(g)^{n_g}) \cdot h = NF((\prod_{g\in\mathcal{G}} lc(g)^{n_g}) \cdot h, \mathcal{G}) + \sum_{g\in\mathcal{G}} q_g \cdot g.$$

Comme p est $\mathcal{G}$-compatible, $NF(f, \mathcal{G}) \in \mathbb{Z}_p[X_1, \ldots, X_n]$. Si f est maintenant un polynôme de $\mathbb{Z}_p[X_1, \ldots X_n]$, on peut trouver un entier a non divisible par p et un polynôme $f' \in \mathbb{Z}[X_1, \ldots X_n]$ tels que $f = af'$ la $\mathbb{Q}$-linéarité de l'application $NF(., \mathcal{G})$ nous permet alors de montrer les points (1) et (2).
Nous supposons que p est $\mathcal{G}$-compatible et que les polynômes de $\mathcal{G}$ sont unitaires dans $\mathbb{Z}_p[X_1, \ldots, X_n]$ ($\forall g \in \mathcal{G}$, $\phi_p(g)$ est donc bien défini). L'algorithme de réduction de f modulo $g \in \mathcal{G}$ fait apparaître une suite de polynômes : $f_0 = f$, $f_i = f_{i-1} - lc(f_{i-1})t_i g$ si $f_{i-1} \neq 0$ et si $lm(f_{i-1})$ est divisible par $lm(g)$ et $f_i = f_{i-1}$ sinon, où t_i est un monôme unitaire de $\mathbb{Z}[X_1, \ldots, X_n]$. Si f est un élément de $\mathbb{Z}_p[X_1, \ldots, X_n]$ la suite (f_i) est donc dans $\mathbb{Z}_p[X_1, \ldots, X_n]$.
Plus généralement, l'algorithme de réduction modulo la famille ordonnée $\mathcal{G}$ fait apparaître une suite de polynômes de $\mathbb{Z}_p[X_1, \ldots, X_n]$:

$$f_0 = f \ , \ f_i = f_{i-1} - lc(f_{i-1})t_i g_{k_i}$$

où les g_{k_i} sont des éléments de $\mathcal{G}$. Le système de générateurs $\mathcal{G}$ étant une base de Groebner, nous pouvons supposer $\mathcal{G} = \{g_1, \ldots, g_u\}$ ordonnée de telle sorte que $i \geq j \Rightarrow k_i > k_j$.
Soit e l'indice du dernier polynôme ainsi défini. Nous avons alors $NF(f, \mathcal{G}) = f_e$.
De la même façon on définit la suite $(f_i^{(p)})$ par :

$$f_0 = \phi_p(f) \ , \ f_i^{(p)} = f_{i-1}^{(p)} - lc(f_{i-1}^{(p)})t_i \phi_p(g_{l_i}),$$

et on note s l'indice le plus élevé dans la suite $(f_i^{(p)})$ tel que $f_i^{(p)} = \phi_p(f_i)$.
Comme $\mathcal{G}$ est une base de Groebner réduite, aucun des $lm(g)$, $g \in \mathcal{G}$ ne divise l'un des monômes de f_e. Comme p est $\mathcal{G}$-compatible, aucun des $lm(\phi_p(g))$, $g \in \mathcal{G}$ ne divise l'un des monômes de $\phi_p(f_e)$, par conséquent $s \leq e$.
Si $\phi_p(lc(f_s)) \neq 0$, alors $f_{s+1}^{(p)} = f_s^{(p)} - lc(f_s^{(p)})\phi_p(g_{l_s}) = \phi_p(f_s) - \phi_p(lc(f_s))\phi_p(g_{k_s})$ et donc $f_{s+1}^{(p)} = \phi_p(f_{s+1})$ par conséquent, $\phi_p(lc(f_s)) = 0$. Dans ce cas, $f_s = f'_s + pf_p$ avec $\phi_p(lc(f'_s)) \neq 0$ et $\phi_p(NF(f, \mathcal{G})) = \phi_p(NF(f'_s, \mathcal{G}))$ ce qui montre que $s = e$ et donc que $\phi_p(NF(f, \mathcal{G})) = NF(\phi_p(f), \phi_p(\mathcal{G}))$. □

Ce résultat montre en particulier que si $f \in \mathcal{I}$ alors $\phi_p(f) \in \langle \phi_p(\mathcal{G}) \rangle$. En fait nous pouvons alors montrer la proposition 8.1:

Preuve de la proposition 8.1: Soient g et g' deux polynômes de $\mathcal{G}$ et $S(g,g')$ le S-polynôme qui leur est associé. Comme $\phi_p(S(g,g')) = S(\phi_p(g), \phi_p(g'))$, et comme $\mathcal{G}$ est une base de Groebner pour $>$, $NF(S(\phi_p(g), \phi_p(g'), \mathcal{G}) = 0$ et $\phi_p(\mathcal{G})$ est donc une base de Groebner de $\langle \phi_p(\mathcal{G}) \rangle$ pour $>$. Enfin si $\mathcal{G}$ est une base de Groebner réduite, $\phi_p(\mathcal{G})$ est a fortiori réduite si p est $\mathcal{G}$-compatible. □

Rappelons qu'une *représentation univariée rationelle* peut être calculée à l'aide de polynômes caractéristiques d'endomorphismes de multiplication par un polynôme. Il convient alors de regarder le comportement de ces quantités lors d'une projection dans $GF(p)[X_1, \ldots, X_n]$.

Proposition 8.2 *Soient $\mathcal{I}$ un idéal zéro-dimensionnel de $\mathbb{Z}[X_1, \ldots, X_n]$, $\mathcal{G}$ une base de Groebner réduite de $\mathcal{I}$ (pour un ordre $>$), et $p > D$ un entier premier $\mathcal{G}$-compatible pour $>$. Notons $\langle \phi_p(\mathcal{G}) \rangle$ l'idéal engendré par $\phi_p(\mathcal{G})$ et, pour tout $t \in \mathbb{Z}[X_1, \ldots, X_n]$, P_t (resp. $P_{\phi_p(t)}$) le polynôme caractéristique de m_t (supposé unitaire) (resp. $m_{\phi_p(t)}$) dans $\mathbb{Q}[X_1, \ldots, X_n]/\mathcal{I}$ (resp. $GF(p)[X_1, \ldots, X_n]/\langle \phi_p(\mathcal{G}) \rangle$). Alors :*

- $dim_{GF(p)}(GF(p)[X_1, \ldots, X_n]/\langle \phi_p(\mathcal{G}) \rangle) = dim_{\mathbb{Q}}(\mathbb{Q}[X_1, \ldots, X_n]/\mathcal{I})$
- *Pour tout $t \in \mathbb{Z}[X_1, \ldots, X_n]$, le polynôme P_t est à coefficients dans $\mathbb{Z}_p$ et $\phi_p(P_t) = P_{\phi_p(t)}$.*

Preuve : Rappelons qu'une base de monômes de $\mathbb{Q}[X_1, \ldots, X_n]/\mathcal{I}$ peut être définie par l'ensemble des monômes unitaires $\mathcal{B} = \{\omega_1, \ldots, \omega_D\} \in \mathcal{M}[X_1, \ldots, X_n]$ ne divisant aucun des $\{lc(g)\ ,\ g \in \mathcal{G}\}$. Comme p est un entier premier $\mathcal{G}$-compatible, $\phi_p(\mathcal{G})$ est donc une base de Groebner réduite de $\langle \phi_p(\mathcal{G}) \rangle$ et par conséquent $\mathcal{B}$ est également une base de $GF(p)[X_1, \ldots, X_n]/\langle \phi_p(\mathcal{G}) \rangle$. En particulier, si $NF(f, \mathcal{G}) = \sum_{i=1\ldots D} a_i \omega_i$ ($a_i \in \mathbb{Z}_p$ pour tout $i = 1, \ldots, D$), alors

$$\phi_p(NF(f, \mathcal{G})) = \sum_{i=1\ldots D} \phi_p(a_i)\omega_i = NF(\phi_p(f), \phi_p(\mathcal{G})).$$

Pour tout $t \in \mathbb{Z}[X_1, \ldots, X_n]$, soit M_t (resp. $M_{\phi_p(t)}$) la matrice de m_t (resp. $m_{\phi_p(t)}$ dans $\mathbb{Q}[X_1, \ldots, X_n]/\mathcal{I}$ (resp. $GF(p)[X_1, \ldots, X_n]/\langle \phi_p(\mathcal{G}) \rangle$). Dans ce cas,

$$\phi_p(NF(t\omega_i, \mathcal{G})) = NF(\phi_p(t)\omega_i, \phi_p(\mathcal{G}))$$

pour tout $i = 1, \ldots D$. La matrice M_t prend ses valeurs dans $\mathbb{Z}_p$, P_t est donc à coefficients dans $\mathbb{Z}_p$ et $\phi_p(M_t) = M_{\phi_p(t)}$. Par linéarité de ϕ_p, on obtient également $\phi_p(Trace(M_{t^i})) = Trace(M_{(\phi_p(t))^i})$ pour tout $i = 0 \ldots D$, ce qui montre que les

sommes de Newton de P_t ont pour images les sommes de Newton de $P_{\phi_p(t)}$. Par la formule de Newton, les coefficients de P_t peuvent s'obtenir à partir des sommes de Newton de P_t en résolvant un système triangulaire tel que le déterminant ($D!$) de la matrice associée est non nul modulo p (car $P > D$). Les coefficients de $P_{\phi_p(t)}$ s'obtiendront par conséquent en résolvant l'image par ϕ_p de ce système, et donc $\phi_p(P_t) = P_{\phi_p(t)}$. □

Corollaire 8.1 *Si $p > D$ est un entier premier $\mathcal{G}$-compatible, alors pour tout $t \in \mathbb{Z}[X_1, \ldots, X_n]$:*

$$gcd(P_t, P_t') \in \mathbb{Z}_p[X_1, \ldots, X_n],$$
$$deg(gcd(P_t, P_t')) \leq deg(gcd(P_{\phi_p(t)}, P'_{\phi_p(t)}))$$

et par conséquent,

$$deg(P_t/gcd(P_t, P_t')) \geq deg(P_{\phi_p(t)}/gcd(P_{\phi_p(t)}, P'_{\phi_p(t)}))$$

En particulier, ceci montre que $\sharp V(\mathcal{I}) \geq \sharp V(\langle \phi_p(\mathcal{G}) \rangle)$.

Preuve: Comme $P_t \in \mathbb{Z}_p[X_1, \ldots, X_n]$ (supposé unitaire), il existe un entier a tel que $\phi_p(a) \neq 0$ et $aP_t \in \mathbb{Z}[X_1, \ldots, X_n]$ et tel que aP_t soit de contenu égal à 1. Dans ce cas $gcd(P_t, P_t') = 1/a(gcd(aP_t, (aP_t)')$, ce qui montre que $Q = gcd(P_t, P_t') \in \mathbb{Z}_p[X_1, \ldots, X_n]$.
Comme $Q \in \mathbb{Z}_p[X_1, \ldots, X_n]$ divise P_t et P_t', $\phi_p(Q)$ divise $P_{\phi_p(t)}$ et $P'_{\phi_p(t)}$ est donc un diviseur de $gcd(P_{\phi_p(t)}, P'_{\phi_p(t)})$.

Rappelons que si t (resp. $\phi_p(t)$) sépare $V(\mathcal{I})$ (resp. $V(\langle \phi_p(\mathcal{G}) \rangle)$) alors le degré de la partie sans facteurs carrés de P_t (rep. $P_{\phi_p(t)}$) est maximal, donc $\sharp V(\mathcal{I}) \geq \sharp V(\langle \phi_p(\mathcal{G}) \rangle)$.

□

Ceci nous donne alors un résultat important pour la recherche d'éléments séparants :

Proposition 8.3 *Soit p un entier premier $\mathcal{G}$-compatible. Si $\sharp V(\mathcal{I}) = \sharp V(\phi_p(\mathcal{G}))$ et si $t_p \in GF(p)[X_1, \ldots, X_n]$ sépare $V(\phi_p(\mathcal{G}))$ alors tout $t \in \mathbb{Z}[X_1, \ldots, X_n]$ tel que $\phi_p(t) = t_p$ sépare $V(\mathcal{I})$.*

Preuve : Comme t_p sépare $V(\phi_p(\mathcal{G}))$, $P_{t_p}/gcd(P_{t_p}, P'_{t_p})$ est de degré maximal égal à $\sharp V(\phi_p(\mathcal{G}))$. Pour $t \in \mathbb{Z}[X_1, \ldots, X_n]$,

$$deg(P_t/gcd(P_t, P_t')) \leq \sharp V(\mathcal{I}).$$

Or, d'après la proposition 8.1,

$$deg(P_t/gcd(P_t, P_t')) \geq deg(P_{t_p}/gcd(P_{t_p}, P'_{t_p})).$$

Comme $\sharp V(\mathcal{I}) = \sharp V(\phi_p(\mathcal{G}))$, $deg(P_t/gcd(P_t, P_t')) = \sharp V(\mathcal{I})$ et t sépare $V(\mathcal{I})$. □

Dès lors qu'il est possible de trouver un entier premier p tel que l'égalité de la proposition précédente soit vérifiée, nous avons alors une technique modulaire pour déterminer un élément séparant $V(\mathcal{I})$. Attachons nous maintenant à la caractérisation des entiers p premiers pour lesquels cette égalité n'est pas vérifiée. En particulier, la proposition 8.3 fournira un algorithme complet si ce nombre d'entiers est fini.

Definition 8.2 *Soit $\mathcal{I} \subset \mathbb{Z}[X_1, \ldots, X_n]$ un idéal zéro-dimensionnel, et $\mathcal{G}$ une base de Groebner de $\mathcal{I}$. Un entier premier sera de bonne réduction pour le calcul d'une représentation univariée rationelle de $\mathcal{I}$ si il est $\mathcal{G}$-compatible et si $\sharp V(\mathcal{I}) = \sharp V(\phi_p(\mathcal{G}))$.*

Rappelons que l'algorithme de Hermite permet, dans le cas d'un système à coefficients dans un corps de caractéristique nulle, de calculer le nombre de racines, nous donnant par conséquent le degré de la partie sans facteurs carrés du polynôme caractéristique d'un élément séparant. Dans le cas des systèmes à coefficients entiers, nous avions renoncé à utiliser en pratique cette stratégie à cause du coût des calculs engendrés. Toutefois le nombre d'opérations arithmétiques de l'algorithme de Hermite n'excède pas celui de l'algorithme RUR , ce qui montre que ces calculs sont coûteux à cause d'une forte croissance de la taille des entiers apparaissant en cours d'algorithme. Ce problème ne se posant pas en calcul modulaire, nous pouvons penser à utiliser une telle stratégie.

Nous n'allons pas reprendre ici la démonstration complète du théorème de Hermite, nous nous contentons de présenter les conditions sur p pour qu'il puisse s'appliquer avec des systèmes zéro-dimensionnels à coefficients dans $GF(p)$. Les deux principaux théorèmes utilisés dans la démonstration pour des coefficients dans un corps de caractéristique zéro sont le théorème des zéros de Hilbert et celui de Stickelberger. Le théorème des zéros de Hilbert restant valide en caractéristique quelconque , il nous suffit de remarquer que celui de Stickelberger s'applique avec des coefficients dans $GF(p)$ pour tout premier $p > \sharp V(\mathcal{I})$ pour énoncer la proposition suivante :

Proposition 8.4 *Soient, un idéal zéro-dimensionnel $I_p = (f_1, \ldots, f_s)$ de $GF(p)[X_1, \ldots, X_n]$ et un polynôme $h \in \mathbb{Z}[X_1, \ldots, X_n]$. Notons $V(I_p) \subset \overline{GF(p)}^n$ l'ensemble des zéros de I_p.*

$$\rho(Q_{\phi_p(h)}) = \sharp\{\alpha \in V(I_p) | \phi_p(h)(\alpha) \neq 0\}$$

où $\rho(Q_{\phi_p(h)})$ désigne le rang de $Q_{\phi_p(h)}$.

Remarque 8.1 *En utilisant les mêmes arguments que dans les démonstrations du lemme 8.2 et de la proposition 8.2, on peut montrer que si p est $\mathcal{G}$-compatible, alors*

$$\phi_p(Q_h) = Q_{\phi_p(h)}$$

où Q_h est la forme quadratique de Hermite généralisée associée à 1 dans $K[X_1, \ldots, X_n]/\mathcal{I}$.

De même, nous pouvons étendre le lemme 3.1 :

Lemme 8.3 *Soit $\mathcal{X}$ un ensemble de points de $\overline{GF(p)}^n$ tel que $\sharp\mathcal{X} = d$. Si $p \geq (n-1)^{\frac{d(d-1)}{2}}$, la famille de formes linéaires $\mathcal{U}_p = \{X_1 + \phi_p(i)X_2 + \ldots + \phi_p(i)^{n-1}X_n \ , \ 0 \leq i \leq n^{\frac{d(d-1)}{2}}\}$ contient au moins un élément séparant $\mathcal{X}$.*

Le résultat suivant ne sera démontré que dans le prochain chapitre (partie ??) mais il nous sera toutefois nécessaire pour l'étude de la complexité de notre algorithme :

Proposition 8.5 *Soit $\mathcal{I} \subset \mathbb{Z}[X_1, \ldots, X_n]$ un idéal zéro-dimensionnel, et $\mathcal{G}$ une base de Groebner de $\mathcal{I}$. Si $\mathcal{T}_1$ désigne la taille maximale d'un entier intervenant dans l'expression des matrices M_{X_i}, le nombre d'entiers premiers (de taille unitaire) de mauvaise réduction pour le calcul d'une représentation univariée rationelle de $\mathcal{I}$ est $O(D^2\mathcal{T}_1)$.*

8.2 L'algorithme

La définition 8.2 nous indique quels sont exactement les entiers premiers de mauvaise réduction pour l'algorithme RUR lorsque les polynômes potentiellement séparants sont choisis dans une famille finie $\mathcal{U}$ de polynômes contenant au moins un élément séparant $V(\mathcal{I})$. La proposition 8.5 montre en particulier que le nombre d'entiers premiers de mauvaise réduction est fini et que pour tout entier premier $\mathcal{G}$-compatible de mauvaise réduction, $\sharp V(\mathcal{I}) > \sharp V(\phi_p(\mathcal{G}))$.
La proposition 8.3 montre que si de plus que si p est de bonne réduction et si il existe $t_0 \in \mathcal{U}$ tel que $\phi_p(t_0)$ sépare $V(\phi_p(\mathcal{G}))$, alors t_0 sépare $V(\mathcal{I})$.
Enfin, le lemme 8.3 montre que si

$$\mathcal{U} = \{X_1 + iX_2 + \ldots + i^{n-1}X_n \ , \ 0 \leq i \leq n\frac{d(d-1)}{2}\},$$

$\phi_p(\mathcal{U})$ contient un tel élément t_0.
Bien entendu, nous ne pouvons pas trouver d'entier premier de bonne réduction a priori (leur caratérisation se faisant en fonction du résultat). Toutefois, nous disposons d'un test efficace (a posteriori) permettant de vérifier si un polynôme t choisi arbitrairement sépare $V(\mathcal{I})$ ou pas.
Le principe de base de l'algorithme que nous proposons est de supposer que le nombre d'entiers premiers de mauvaise réduction est très faible (ce qui est d'ailleurs vérifié en pratique).
L'idée est de fixer un entier premier p $\mathcal{G}$-compatible (test facile à réaliser et peu coûteux), de trouver un élément séparant $V(\phi_p(\mathcal{G}))$ de la forme $\phi_p(t)$, $t \in \mathcal{U}$ (le degré de la partie sans facteurs carrés de $P_{\phi_p(t)}$, $t \in \mathcal{U}$ doit être égal au cardinal de $V(\phi_p(\mathcal{G}))$ lui-ême étant égal au rang de $\phi_p(Q_1)$), puis de calculer la *représentation*

univariée rationelle en supposant que p est séparant par les fonctione symétriques étendues. En utilisant alors le test présenté précédement, nous pouvons vérifier simplement et efficac sommes assurés que p est un entier premier de mauvaise réduction, que $\sharp V(\mathcal{I}) > \sharp V(\phi_p(\mathcal{G}))$ et que t ne sépare pas $V(\mathcal{I})$. Dans ce cas nous changeons d'entier premier en prenant soin de choisir un entier p' tel que $\sharp V(\phi_{p'}(\mathcal{G})) > \sharp V(\phi_p(\mathcal{G}))$ et nous réitérons le procédé en prenant soin de retirer t de $\mathcal{U}$. Nous sommes sûr que l'algorithme s'arrête puisque nous avons montré que le nombre d'entiers premiers de mauvaise réduction est fini.
En langage de description, ceci nous donne l'algorithme :

Algorithme RUR-Int

Entrée : MT

Sortie : Un élément t séparant $V(\mathcal{I})$ et les polynômes $g(t,T), g_1(t,T), \ldots, g_n(t,T)$ correspondants.

- **Étape 0** : Initialisation : $d_0 = 1$ (cardinal minimum de $V(\mathcal{I})$, car si $D = 0$ la *représentation univariée rationelle* est triviale, sinon nous sommes assurés que $\sharp V(\mathcal{I}) > 0$),

  $$\mathcal{U} = \{X_1, \ldots, X_n, X_1 + iX_2 + \ldots + i^{n-1}X_n \ , \ i = 1, \ldots, nD(D-1)/2\}$$

- **Étape 1** : Prédiction modulaire.
  - **Étape a** : Choix d'un entier premier p $\mathcal{G}$-compatible.
  - **Étape b** : Calcul du nombre de racines d_p de $\langle \phi_p(\mathcal{G}) \rangle$ par Hermite. Si $d_p < d_0$, retourner à l'étape **1-a**, sinon, $d_0 := d_p + 1$.
  - **Étape c** : Calcul de $\phi_p(M_{X_i})$, $i = 1, \ldots, n$.
  - **Étape d** : Choix d'un polynôme t (lemme 3.1) parmi les polynômes de $\mathcal{U}$.
  - **Étape e** : Calcul de $P_{\phi_p(t)}$ (polynôme caractéristique de d'une combinaison linéaire de matrices de la forme $\sum_{i=1}^{n} \phi_p(a_i)\phi_p(M_{X_i})$ par la méthode de Hessenberg). Si $deg(P_{\phi_p(t)}) \neq d_p$ retourner à l'étape **1-d**.
- **Étape 4** : On prend pour élément séparant t tel que $\phi_p(t)$ sépare $V(\phi_p(\mathcal{I}))$.
- **Étape 5** : Calcul des Traces (Compute-Traces)

- **Étape 6** : Déduction des polynômes (formule de Newton étendue)

$$f(t,T), h_1(t,T), \ldots, h_n(t,T)$$

et de

$$g(t,t) = f'/gcd(f(t,T), f'(t,T))$$

- **Étape 7** : Pour $i = 1, \ldots, n$, calcul de

$$g_i(t,T) = h_i(t,T)/gcd(f(t,T), f'(t,T))$$

- **Etape 8** : Si $degre(g) = D-1$, t est forcément séparant. Sinon, on effectue le test de l'élément séparant (corollaire 6.1). Si t n'est pas séparant, retirer t de $\mathcal{U}$ et retourner à l'étape **1** (Entier premier de mauvaise réduction).

8.3 Complexité

L'étude de complexité de l'algorithme RUR-Int est un peu plus ardue que celle de l'algorithme RUR. Pour distinguer le coût des opérations modulaires de celui des opérations sur les entiers, nous somme conduits à parler *d'opérations machine.* Le coût d'une opération de base sur des entiers de taille $\mathcal{T}$ sera noté $M(\mathcal{T}) > \mathcal{T}$, celui des opérations de base dans $GF(p)$ sera supposé unitaire et une opération fasant intervenir un entier de taille $\mathcal{T}$ et une entier premier p sera supposé proportionnelle à $\mathcal{T}$.
Rappelons que si $\mathcal{T}$ désigne la taille des entiers intervenant dans les M_{X_i} , $i = 1, \ldots, n$, l'algorithme RUR exige $O(D^3 M(D\mathcal{T}) + nD^2 M(D^2\mathcal{T}))$ opérations machine si un vecteur séparant est connu et $O(nD^2(D^3 M(D\mathcal{T}) + nD^2 M(D^2\mathcal{T})))$ sinon. Rappelons également que si l'on suppose que les coefficients d'un pgcd sont en général plus petits que ceux des polynômes considérés ou si l'idéal étudié est radical, cette complexité devient $O(M(D\mathcal{T})(D^3 + nD^2))$ lorsqu'un élément séparant est connu et $O(nD^2 M(D\mathcal{T})(D^3 + nD^2))$ sinon.

En pratique, pour obtenir des expressions finales plus simples, nous devons considérer en priorité les polynômes de la forme X_i , $i = 1 \ldots n$ comme séparant potentiellement $V(\mathcal{I})$. Ainsi, même si un polynôme t générique sépare $V(\mathcal{I})$, il est toutefois fréquent que celui-ci ne soit pas de la forme X_i , $i = 1 \ldots n$ (l'idéal n'est pas en position générique). Dans ce cas, l'algorithme RUR sera exécuté (au moins $n+1$ fois) dans sa totalité en prenant t dans la famille $\mathcal{U} = \{X_1, \ldots, X_n, X_1 + iX_2 + \ldots + i^{n-1}X_n$, $i = 1 \ldots (n-1)d(d-1)/2\}$ jusqu'à l'obtention d'une représentation univariée de $\mathcal{I}$. Une bonne estimation de la complexité pratique de l'algorithme RUR est alors $O(nM(D\mathcal{T})(D^3 + nD^2))$ opérations machine.

Proposition 8.6 *Si p est un entier premier de bonne réduction pour la représentation univariée rationelle (c'est à dire si il est $\mathcal{G}$-compatible pour $>$ et si pour $t \in \mathcal{U}$, $deg(gcd(P_t, P_t')) = deg(gcd(\phi_p(P_t), \phi_p(P_t'))))$ alors, en effectuant la prédiction d'un élément séparant dans $GF(p)$, le coût de l'algorithme RUR-Int est $O((D^3 + nD^2)M(\mathcal{T}))$ pour ce choix de p.*

Preuve : Supposons qu'un entier premier de bonne réduction soit connu. Si on ne tient pas compte des manipulations dues au calcul modulaire, la complexité de l'algorithme est $O(D^3M(D\mathcal{T}) + nD^2M(D^2\mathcal{T}))$ opérations machine (complexité de l'algorithme RUR-Int dans le cas ou un élément séparant est connu).

Nous pouvons dors et déjà négliger le coût des calculs occasionnés par l'application de ϕ_p sur :

- La forme quadratique de Hermite : réduction modulo p de D^2 entiers de taille $O(D\mathcal{T})$, car si la taille de p est $O(1)$, le coût de cette opération est alors $O(D^3\mathcal{T})$.
- Les matrices $\phi_p(M_{X_i})$: réduction modulo p de nD^2 entiers de taille $O(\mathcal{T})$.

Vérfier que p est $\mathcal{G}$-compatible nécessite de diviser le terme de tête (de taille $O(\mathcal{T})$ de chaque élément de la base de Groebner par p. Le nombre d'éléments de la base de Groebner étant majoré par nD le coût de cette opération est $O(nD\mathcal{T})$. La recherche d'un élément séparant $V(\langle\phi_p(\mathcal{G})\rangle)$ nécessite le calcul du nombre de zéros $V(\langle\phi_p(\mathcal{G})\rangle)$ par la méthode de Hermite soit un coût de $O(D^3)$ opérations machine. Il faut ensuite calculer au plus nD^2 polynômes caractéristiques pour déterminer l'élément séparant, ce qui requiert nD^2D^3 opérations arithmétiques machine par la méthode de Hessenberg.

En terme d'opérations machine, toutes ces opérations peuvent être négligées par rapport à $O(D^3M(D\mathcal{T}) + nD^2M(D^2\mathcal{T}))$. □

En pratique, le nombre d'entiers premiers de mauvaise réeduction est très faible lorsque les entiers premiers considérés sont suffisement grands (codables toutefois sur un mot machine - i.e inférieurs à 2^{32} sur une station 32 bits) et cette complexité est à l'image des observations. En effet, sur notre panel d'exemples, jamais aucun entier de mauvaise réduction n'a été détecté. Il est intéressant alors de constater que le problème de l'élément séparant n'influe pas sur le comportement global de l'algorithme.
Dans l'absolu, le nombre d'entiers premiers de mauvaise réduction est en $O(D^2\mathcal{T})$, ainsi les étapes **1-a** et **1-b** seront répétées $O(D^2\mathcal{T})$ alors que les autres le seront qu plus D fois (le nombre d'éléments de $V(\mathcal{G})$ croit à chaque étape). Ceci nous donne alors une complexité théorique en $O(D^3(D^2\mathcal{T}^2 + DM(D\mathcal{T}) + nM(D^2\mathcal{T})))$ opérations machine.

9 Comportement pratique

Dans tous les exemples qui suivent, la première variable est séparante. Nous pouvons donc comparer le calcul de la *représentation univariée rationelle* à celui d'une base de Groebner lexicographique. Nous nous attardons bien sûr sur les temps de calcul mais surtout sur la taille des représentations univariées fournies qui conditionera l'utilisation de la sortie des algorithmes.

Le calcul direct d'une base de Groebner lexicographique par l'algorithme de Buchberger étant en pratique très coûteux, nous comparerons les temps de calcul de la *représentation univariée rationelle* à celui d'un algorithme calculant les bases de Groebner lexicographiques par changement d'ordre. Le principe est de calculer un base de Groebner pour un ordre du degré (efficace en pratique - voir [Fau94]) et d'en déduire une base lexicographique par des techniques d'algèbre linéaire (algorithme FGLM - [FGLM94]).

Pour que cette comparaison soit juste, la méthode utilisée pour le calcul de la table de multiplication nécessaire à notre algorithme prend en entrée la même base de Groebner que l'algorithme FGLM.

Notons au passage que la table de multiplication pourrrait être calculée par d'autres méthodes pourvu qu'il soit fourni un moyen de multiplier par une variable modulo l'idéal étudié (voir [R96] [Car93], [CDS], [BCRS94]).

Attention : Cette première série de test à été effectuée sur une staion Sun/sparc 40 Mhz nettement moins puissante que la station DEC/Alpha utilisée dans toutes les autres mesures et avec des versions de Gb et RealSolving datant de 1994. Compte tenu des temps de calculs observés, nous n'avons pas tenu à recommencer les mesures. En particulier, la version de l'algorithme RUR utilisée n'incluait pas la recherche modulaire d'éléments séparants.

Legende :

- G.B : Calcul de bases de Gröbner pour l'ordre *degré lexicographique inverse* via Gb[2].
- MT : Une table de multiplication de $K[X_1, \ldots, X_n]/\mathcal{I}$.
- RUR : Calcul d'une *représentation univariée rationelle* du système.
- Racines :
  - R : nombre de racines réelles distinctes.
  - C : nombre de racines complexes distinctes.

[2]Gb est un logiciel implanté par J.C. Faugère dédié au calcul de bases de Groebner (voir [Fau94])

- FGLM : Algorithme FGLM pour le calcul des bases de Groebner lexicographiques par changement d'ordre (fonction *totolex* de Gb).
- T. : temps de calcul en secondes
- X : Calcul arrêté après plus de 12 heures.
- L. : taille binaire du plus grand entier apparaissant dans le résultat (i.e: le plus petit entier i tel que 2^{32i} soit supérieur à la valeur absolue de l'entier considéré).

	G.B.		MT		RUR		MT+RUR	FGLM		Racines	
Name	T.	L.	T.	L.	T.	L.	T.	T.	L.	R	C
cassou	28	5	0.8	6	0.2	4	1	1.6	12	4	16
sendra	0.2	5	4	16	4	5	8	2379	78	6	46
katsura 5	1.2	7	9	15	10	4	19	1065	73	18	32
katsura 7	631	10	1672	15	662	19	2334	X		44	128
discret 3	6	9	930	13	376	26	1306	X		128	128
planM2I	6	16	15	26	23	26	38	2846	274	0	32
planMV	4	19	3	27	6	23	9	92	127	0	16
planN3I	15	18	34	27	29	32	63	12711	431	0	40
spatV2A	221	21	30	72	60	30	90	3088	365	0	16
spatAV2I	5035	65	144	101	144	48	288	48432	543	0	24
spat2A2I	757	43	186	66	85	32	171	X		0	32

On peut remarquer que la taille du résultat à la sortie de la *représentation univariée rationelle* est nettement inférieure à celle obtenue à la sortie de *FGLM*, le rapport allant de 1 à 10. Si $(f, g, g_1, \ldots, g_n)$ est une *représentation univariée rationelle* de $\mathcal{I}$, il est possible de déduire une base lexicographique en multipliant les polynômes g_i intervenant dans la *représentation univariée rationelle* par l'inverse du polynôme g modulo f. L'application de l'algorithme d'Euclide pour faire ce calcul entraine une croissance des coefficients, cette observation n'est donc pas surprenante.

Les techniques d'algèbre linéaire employées lors du calcul de *FGLM* sont de complexités (en nombre d'opérations arithmétiques) sensiblement équivalentes aux méthodes employées dans le calcul de la *représentation univariée rationelle* . Par conséquent, les fortes différences de temps de calcul ne peuvent s'expliquer que par un meilleur contrôle de la taille des entiers dans l'algorithme *représentation univariée rationelle* .

Remarquons enfin que le calcul des prérequis est, dans bon nombre de cas, au moins aussi coûteux en temps que le calcul de la représentation univariée rationnelle.

Nous nous attachons maintenant à étudier de fçon plus détaillée le comportement de l'algorithme RUR-Int.
Les performances actuelles, sur station station DEC/Alpha , de l'algorithme RUR-Int sur notre série d'exemples habituelle sont données par la table suivante :

	GR	MT	RUR		MT+RUR
Ex.	L.	T.	T	L.	T.
e1	1	1,31	3,65	9	4,96
e2	5	0,24	0,43	1	0,67
e3	3	0,73	2,1	5	2,83
e4	6	2,68	3,4	4	6,08
e5	10	401,52	114,93	19	516,45
e6	1	2,31	3,15	5	5,46
e7	2	143,79	116,75	20	260,54
e8	9	223,81	84,1	26	307,92
e9	7	6,52	5,71	32	12,23
e10	51	6,28	3,46	30	9,74
e11	43	26,52	16,79	38	43,31
e12	65	26,28	27,54	53	53,82
e13	91	180,64	460	40	640,64
e14	101	219,69	135,2	77	354,89
e15	5	9,87	3,65	8	13,52

La figure 1 montre que la répartition des temps de calculs entre la table de multiplication et le calcul de la représentation unvariée rationnelle est relativement équitable

En ce qui concerne les tailles de coefficients, la figure 2 montre une croissance des coefficients est plus forte dans l'expression de la *représentation univariée rationelle* lorsque l'élément séparant est non trivial (exemples e1,e6,e8). Enfin, on peut également remarquer que la taille des coefficients intervenant dans la *représentation univariée rationelle* peut être inférieure à celle des coefficients intervenant dans la base de Groebner.

References

[ABRW94] M. E. Alonso, E. Becker, M.-F. Roy. T. Wörmann: *Zero's, Multiplicities and Idempotents for Zero Dimensional Systems*, to appear in MEGA 94.

[AMNR92] Alonso M.E., Mora T., Niesi G.F.,Raimondo M.: Local Parametrizations of Space Curves at Singular Points. In Computer Graphics and Mathematics, Springer-Verlag 1992.

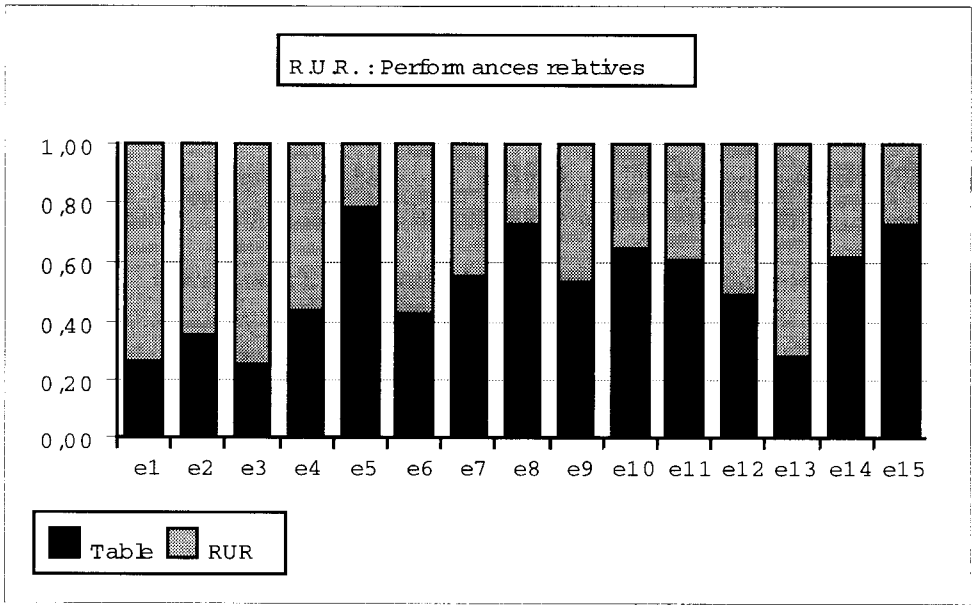

Figure 1: Table / RUR : temps de calcul

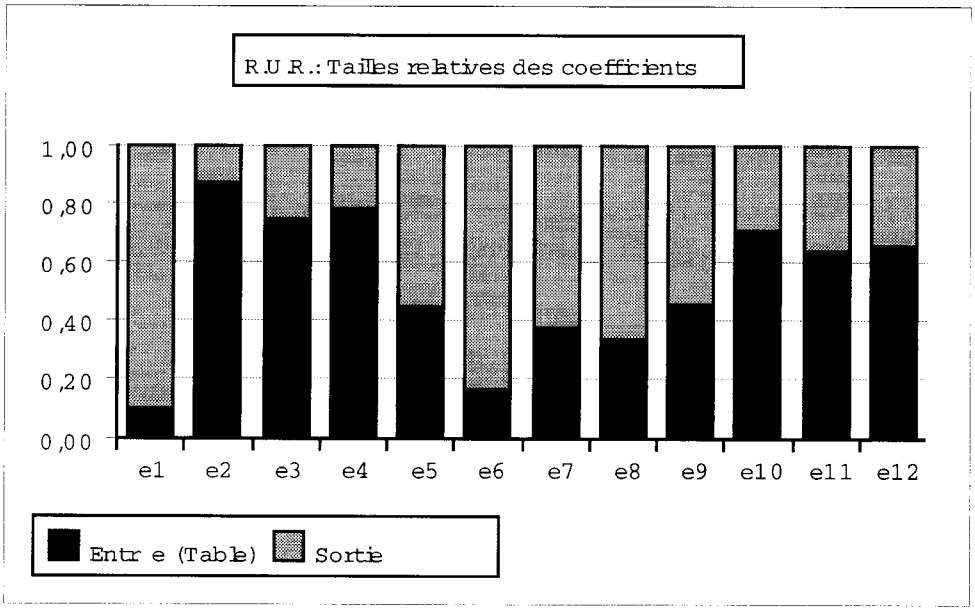

Figure 2: Table / RUR : croissance des coefficients

[AS88] W. Auzinger and H. J. Stetter: *An Elimination Algorithm for the Computation of all Zeros of a System of Multivariate Polynomial Equations.* Int. Series in Numerical Mathematics **86**, 11–30, Birkhäuser (1988).

[B68] E.H. Bareiss: *Sylvester's identity and multistep integer-preserving gaussian elimination.* Math. Comp., 22:565- 578, 1968.

[BCR87] J. Bochnak, M. Coste and M. F. Roy: *Géometrie algébrique réelle.* Ergebnisse der Mathematik. Berlin: Springer-Verlag (1987).

[BCL82] B. Buchberger, G.E. Collins and R.Loos *Computer Algebra Symbolic and Algebraic Computation*, second edition Springer-Verlag. (1982)

[BCRS94] E. Becker, J.P. Cardinal, M.F. Roy and Z. Szafraniec: *Multivariate Bezoutians, Kronecker Symbol and Eisenbud-Levine formula.* To appear in the proceedings of MEGA-94 Conference to be published in the series Progress in Mathematics of Birkhausser (1994).

[BMMT93] E. Becker, M. G. Marinari, T. Mora and C. Traverso: it The shape of the Shape Lemma. Proceedings of ISSAC–94, 129–133, ACM Press (1993).

[BW92] E.Becker, T.Wörmann: *On the Trace Formula for Quadratic Forms.* Proc. RAGSQUAD (1992), to appear in Contemp. Math. (1993)

[BW93] E.Becker, T.Wörmann: *Radical Computations of Zero-dimensional Ideals and Real Root Counting.* to appear in Mathematics and Computers in Simulation.

[Ca88] J.F. Canny: *Some algebraic and geometric computations in PSPACE.* In Proc. Twentieth ACM Symp. on Theory of Computing, 460-467,(1988).

[Car93] J.-P. Cardinal :*Dualité et algorithmes itératifs pour la résolution des systèmes polynômiaux.* Doctoral Thesis. Université de Rennes I (1993).

[CDS] E. Cattani, A. Dickenstein and B.Sturmfels: *Computing Multidimensional Residues.* To appear in the book *Algorithms in Algebraic Geometry and Applications.*

[CR88] M. Coste and M.F. Roy: *Thom's lemma, the coding of real algebraic numbers and the topology of semialgebraic sets.* Journal of Symbolic Computation 5, 121-129 (1988).

[Dal95] J. Dalbec *Geometry and combinatorics of chow forms, thesis.* Cornell University (1995).

[FGLM94] J.C. Faugère, P. Gianni, D. Lazard and T. Mora: *Efficient Computation of Zero-dimensional Gröbner Basis by Change of Ordering.* J. Symbolic Computation 1994.

[Fau94] J.C. Faugère : *Résolution des systèmes d'équations polynômiales*, thèse (1994).

[GH91a] M. Giusti and J. Heintz: *La determination des points isoles et de la dimension d'une variete algebrique peut se faire en temps polynomial.* To appear in the Proc. of the International Meeting on Computational Commutative Algebra, 1991.

[GH91b] M. Giusti and J. Heintz: *Algorithmes - disons rapides - pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles*, Proc. Effective Methods in Algebraic Geometry, MEGA '90 (T. Mora - C. Traverso ed.), Progress in Mathematics **94**, Birkhäuser (1991), 169-193.

[GHMP95] M. Giusti, G-Heintz-Morais-Pardo : *When Polynomial Equation Systems can be "solved" fast?*, Actes de AAECC-11, Lecture Notes in Computer Science 948, Springer Verlag, 1995.

[GM89] P. Gianni and T. Mora: *Algebraic solution of polynomial equations using Gröbner bases.* Proceedings AAECC-5. Lectures Notes in Computer Science **359**, 247-257, Springer-Verlag (1989).

[GLRR89] L. González-Vega, H. Lombardi, T. Recio and M.-F. Roy: *Sturm-Habicht Sequence.* ISSAC-89 Proceedings (Portland), 136–146, ACM-Press (1989).

[GMT88] P. Gianni, G. Miller and B. Trager: *Decomposition of Algebras.* Lecture Notes in Computer Science 356, 300–308, Springer-Verlag (1988).

[GV92] L.González-Vega : *The computation of the radical for a zero dimensional ideal in a polynomial ring through the determination of the trace for its quotient algebra.* Preprint, 1992.

[GVT95] L.Gonzalez-Vega and G. Trujillo: *Using symmetric functions to describe the solution set of a zero-dimensional ideal*, Proceedings AAECC-11. Lectures Notes in Computer Science **948**, 232-247, Springer-Verlag (1995).

[J93] F. Junker: *Uber symmetrische Funktionen von mehreren Reihen von Veränderlichen*, Mathematische Annalen, **43** (1893), 225-270.

[Lak91] Y. N. Lakshman and D. Lazard: *On the Complexity of Zero–dimensional Algebraic Systems.* Effective Methods in Algebraic Geometry. Progress in Mathematics **94**, 217–225, Birkhauser (1991).

[Laz92] D. Lazard : *Solving Zero - dimensional algebraic systems.* J. Symb. Comp. 13:117-132, 1992.

[Mac79] I. G. Macdonald: *Symmetric functions and Hall polynomials.* Oxford University Press (1979).

[Ped91] P.Pedersen *Counting Real Zeros, thesis.* Courant institute, New York University, (1991).

[PRS93] P.Pedersen, M.-F.Roy, A.Szpirglas: *Counting Real Zeros in the Multivariate Case*, Computational Algebraic Geometry, Frédéric Eyssette, André Galligo (editors), 203-223 (1993), Birkhäuser.

[Re92] J. Renegar: *On the computational complexity and geometry of the first-order theory of the reals*, parts I, II and III. Journal of Symbolic Computation, 13(3):255–352, 1992.

[Ron90] L. Ronyai: *Computing the Structure of Finite Algebras. Journal of Symbolic Computation*, 9, 3, 127–145 (1990).

[R95] F. Rouillier *PoSSo-RealSolving.* Proceedings of the PoSSo-workshop. Paris 1995.

[R96] F. Rouillier *Doctoral Thesis.* In preparation.

[RRS94] F. Rouillier, M.F.Roy, A. Szpirglas: *Multivariate symmetric functions and polynomial system solving.* Preprint. 1994.

[Yoko92] K. Yokoyama, M. Noro and T. Takeshima: *Solutions of Systems of Algebraic Equations and Linear Maps on Residue Class Rings.* Journal of Symbolic Computation **14**, 399–417 (1992).