Approche matricielle de la résolution d'équations polynomiales

23 Mars 1999

B. Mourrain

INRIA, SAGA
BP 93, 06902 Sophia Antipolis
`mourrain@sophia.inria.fr`
`http://www.inria.fr/saga/mourrain/`

Voici un support issu d'un cours

Méthodes Effectives en Géométrie Algébrique :
de la théorie à la pratique.

en collaboration avec M. Elkadi.

CHAPITRE 4

ALGÈBRE DE DIMENSION 0

L'idée que nous voulons développer dans ce chapitre est la suivante. Pour résoudre un système d'équations polynomiales, nous faisons comme si les inconnues vérifiaient ces équations et toutes celles qui en découlent. En d'autres termes, nous travaillons modulo l'idéal engendré par ces équations, c'est-à-dire dans l'algèbre quotient. En étudiant les propriétés de cette algèbre quotient, nous allons voir comment retrouver la géométrie des solutions, c'est-à-dire être en mesure de les compter, de les calculer, d'analyser leur multiplicité...

Tout au long de ce chapitre I est un idéal zéro-dimensionnel de $\mathbb{K}[\mathbf{x}]$, l'algèbre quotient $\mathbb{K}[\mathbf{x}]/I$ sera notée $\mathcal{A}$.

3.1. Le cas en une variable

Nous commençons par le cas facile où I est l'idéal engendré par un polynôme $f = f_d x^d + \cdots + f_1 x + f_0$ de degré d ($f_d \neq 0$), dans $\mathbb{K}[x]$. Nous supposons ici que $\mathbb{K}$ est algébriquement clos. Notons $\mathcal{A} = \mathbb{K}[x]/(f)$ le quotient par f. C'est un espace vectoriel de dimension d, de base $(1, x, \ldots, x^{d-1})$. Supposons dans un premier temps que les racines $\zeta_i \in \overline{\mathbb{K}} = \mathbb{K}$ de f soient simples : $f = f_d \prod_i (x - \zeta_i)$, avec $\zeta_i \neq \zeta_j$ si $i \neq j$.

Considérons l'opérateur M_x de multiplication par x, dans $\mathcal{A}$:

$$\begin{aligned} M_x : \mathcal{A} &\rightarrow \mathcal{A} \\ a &\mapsto a\,x \end{aligned}$$

Sa matrice dans la base monomiale $(\overline{1},\ldots,\overline{x}^{d-1})$ est la matrice compagnon :

$$\mathtt{M}_x = \begin{pmatrix} 0 & \cdots & 0 & -\frac{f_0}{f_d} \\ 1 & \ddots & \vdots & \vdots \\ & \ddots & 0 & \vdots \\ 0 & & 1 & -\frac{f_{d-1}}{f_d} \end{pmatrix}.$$

La dernière colonne de $\mathtt{M}_x$ correspond à la division euclidienne de x^d par f. Il est bien connu que le polynôme caractéristique de $\mathtt{M}_x$ est f et que ses valeurs propres sont les racines ζ_i de f. Comme ces valeurs propres sont distinctes, la matrice $\mathtt{M}_x$ est diagonalisable. Ce qui implique que, pour tout $p \in \mathbb{K}[x]$, les valeurs propres de la multiplication $\mathtt{M}_p$ par un élément $p \in \mathbb{K}[x]$ sont les $p(\zeta_i)$, $i = 1,\ldots,d$, car $\mathtt{M}_p = p(\mathtt{M}_x)$.

Comme $\mathtt{M}_p = p(\mathtt{M}_x)$, ces matrices de multiplication sont donc diagonalisables dans une même base, que nous allons décrire maintenant. Notons

$$\mathbf{e}_i(x) = \prod_{i=1}^{d} \frac{x-\zeta_j}{\zeta_i-\zeta_j},$$

le i$^{\text{ème}}$ *polynôme d'interpolation de Lagrange* associé aux racines de f. Pour tout i et tout $j \neq i$, nous vérifions que $\mathbf{e}_i(x)\mathbf{e}_j(x)$, $\mathbf{e}_i(x)(\mathbf{e}_i(x)-1)$, et $(x-\zeta_i)\mathbf{e}_i(x)$ s'annulent aux racines ζ_i de f. Ces polynômes sont donc divisibles par f, ce qui implique :

$$\mathbf{e}_i\mathbf{e}_j \equiv 0,\ \mathbf{e}_i^2 \equiv \mathbf{e}_i,\ x\,\mathbf{e}_i = \zeta_i\mathbf{e}_i,$$

dans $\mathcal{A}$. Nous avons de plus, $\mathbf{e}_1+\cdots+\mathbf{e}_d = 1$. Nous vérifions, en exercice, que ceci implique la décomposition suivante :

$$\mathcal{A} = \mathbb{K}\,\mathbf{e}_1 \oplus \cdots \oplus \mathbb{K}\,\mathbf{e}_d.$$

Les éléments $(\mathbf{e}_i)_{i=1,\ldots,d}$ forment donc *une base d'idempotents orthogonaux.* De plus, comme $(x-\zeta_i)\,\mathbf{e}_i \equiv 0$, ou encore $x\,\mathbf{e}_i \equiv \zeta_i\,\mathbf{e}_i \equiv 0$ dans $\mathcal{A}$, $\mathbf{e}_i$ est également un vecteur propre de M_x pour la valeur propre ζ_i. Les matrices de multiplication $\mathtt{M}_p$ $(p \in \mathbb{K}[x])$ se décomposent donc dans cette base, sous la forme diagonale

$$\begin{pmatrix} p(\zeta_1) & & 0 \\ & \ddots & \\ 0 & & p(\zeta_d) \end{pmatrix}.$$

La structure de l'algèbre quotient, dans le cas de polynômes univariables dont les racines sont **simples**, se décrit donc complètement en terme de ces idempotents, ceux-ci étant en correspondance avec les racines du polynôme f.

Intéressons-nous maintenant au dual $\widehat{\mathcal{A}}$ de cette algèbre, c'est-à-dire à l'ensemble des formes linéaires Λ de $\mathcal{A}$ dans $\mathbb{K}$. C'est un espace vectoriel de dimension d et de base, la base duale de la base monomiale $(x^i)_{i=0,\ldots,d-1}$. Notons cette base duale $(\mathbf{d}^i)_{i=0,\ldots,d-1}$. Toute forme linéaire $\Lambda \in \widehat{\mathcal{A}}$ se décompose dans cette base, sous la forme

$$\Lambda = \Lambda(1)\mathbf{d}^0 + \cdots + \Lambda(x^{d-1})\mathbf{d}^{d-1}.$$

Pour calculer $\Lambda(g)$ $(g \in \mathbb{K}[x])$, nous calculons le représentant canonique $r = r_0+\cdots+r_d\,x^{d-1}$ de g dans $\mathcal{A}$ (ie. le reste de la division euclidienne de g par f). Comme $g \equiv r$, on a

$$\Lambda(g) = \Lambda(r) = r_0\,\Lambda(1) + \cdots + r_{d-1}\,\Lambda(x^{d-1}).$$

Parmi les éléments de $\widehat{\mathcal{A}}$, nous considérerons en particulier les évaluations $\mathbf{1}_\zeta : p \mapsto p(\zeta)$, où ζ est une racine de f.

Considérons maintenant l'application

$$\begin{array}{rcl} M_x^t : \widehat{\mathcal{A}} & \rightarrow & \widehat{\mathcal{A}} \\ \Lambda & \mapsto & \Lambda \circ M_x \end{array}$$

qui consiste à multiplier d'abord par x, puis à appliquer Λ. Nous vérifions directement que la matrice de M_x^t dans la base duale $(\delta^i)_{i=0,\dots,d-1}$ est la transposée de la matrice de M_x dans la base $(x^i)_{i=0,\dots,d-1}$ de $\mathcal{A}$.

La formule d'interpolation de Lagrange nous dit que tout polynôme r de degré $\leq d-1$ s'écrit

$$r(x) = \sum_{i=1}^{d} r(\zeta_i)\, \mathbf{e}_i(x) = \sum_{i=1}^{d} \mathbf{1}_{\zeta_i}(r)\, \mathbf{e}_i(x).$$

En d'autres termes, les coefficients de r dans la base $(\mathbf{e}_i)_{i=1,\dots,d}$ sont les $\mathbf{1}_{\zeta_i}(r)$, ce qui veut donc dire que $(\mathbf{1}_{\zeta_i})_{i=1,\dots,d}$ est la base duale de $(\mathbf{e}_i)_{i=1,\dots,d}$.

Vérifions que l'évaluation $\mathbf{1}_{\zeta_i}$ est aussi vecteur propre de M_x^t, pour la valeur propre ζ_i : $\forall p \in \mathbb{K}[x]$

$$M_x^t(\mathbf{1}_{\zeta_i})(p) = \mathbf{1}_{\zeta_i}(x\,p) = \zeta_i \mathbf{1}_{\zeta_i}(p), \quad \text{ie. } M_x^t(\mathbf{1}_{\zeta_i}) = \zeta_i \mathbf{1}_{\zeta_i}.$$

Nous déduisons immédiatement que $\mathbf{1}_{\zeta_i}$ est également un vecteur propre de M_p^t pour tout $p \in \mathbb{K}[x]$. Ceci nous donne donc une description complète des opérateurs de multiplications et de leurs transposés.

Nous allons voir dans la section suivante que toutes ces notions se généralisent naturellement au cas de plusieurs variables.

3.2. Idéaux de dimension zéro

Notons $R = \mathbb{K}[x_1, \dots, x_n] = \mathbb{K}[\mathbf{x}]$, $R_{\overline{\mathbb{K}}} = \overline{\mathbb{K}}[\mathbf{x}]$, I l'idéal de R engendré par $f_1, \dots, f_m$, $I_{\overline{\mathbb{K}}}$ l'idéal de $R_{\overline{\mathbb{K}}}$ engendré par ces mêmes éléments et $\mathcal{A}_{\overline{\mathbb{K}}} = R_{\overline{\mathbb{K}}}/I_{\overline{\mathbb{K}}}$. Rappelons qu'un idéal I définit une variété $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$ de dimension 0, si $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$ est fini. Par abus de langage, nous dirons que I est « de dimension zéro ».

Théorème 3.2.1. — *Les conditions suivantes sont équivalentes pour un idéal I de $\mathbb{K}[x_1, \dots, x_n]$:*

(i) *La variété $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$ est finie (c.à.d. $\dim \mathcal{Z}_{\overline{\mathbb{K}}}(I) = 0$).*

(ii) *Pour tout $i \in \{1, \dots, n\}$, il existe $p_i(x_i) \in I_{\mathbb{K}} - \{0\}$.*

(iii) *La dimension du $\mathbb{K}$-espace vectoriel $\mathbb{K}[\mathbf{x}]/I$ est finie.*

Démonstration. On suppose $\mathcal{Z}_{\overline{\mathbb{K}}}(I) \neq \emptyset$, sinon ce théorème provient de la proposition **??**(vi) .

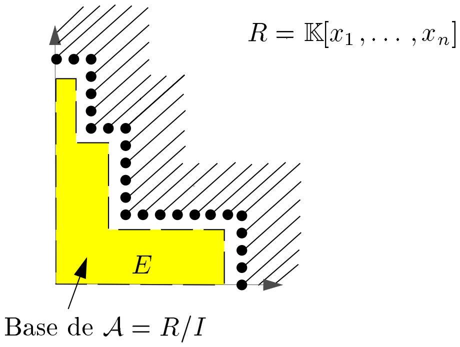
(i) (ii) Notons $\mathcal{Z}_{\overline{\mathbb{K}}}(I) = \{\zeta_1, \dots, \zeta_d\}$. Fixons $i \in \{1, \dots, n\}$, les i$^{\text{èmes}}$ coordonnées $\zeta_{1,i}, \dots, \zeta_{d,i}$ de $\zeta_1, \dots, \zeta_d$ sont dans $\overline{\mathbb{K}}$. Il existe donc $g_i \in \overline{\mathbb{K}}[x_i]$ non nul tel que $g_i(\zeta_{j,i}) = 0$, pour $j \in \{1, \dots, d\}$. Le polynôme g_i s'annulant sur $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$, d'après le théorème des zéros de Hilbert (voir [**4**] p. 175), il existe $m_i \in \mathbb{N}$ tel que $f_i := g_i^{m_i} \in I_{\overline{\mathbb{K}}}$, ce qui montre (ii), pour $\overline{\mathbb{K}}$.

(ii) (iii) Soit d_i le degré de $p_i(x_i) \in I_{\overline{\mathbb{K}}}$. Nous vérifions que $\mathcal{A}_{\overline{\mathbb{K}}} = \overline{\mathbb{K}}[x_1, \dots, x_n]/I$ est engendré par les monômes $x_1^{a_1} \cdots x_n^{a_n}$ pour $0 \leq a_i \leq d_i - 1$. L'algèbre $\mathcal{A}_{\overline{\mathbb{K}}}$ est donc un espace vectoriel de dimension finie. Il en est de même pour $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$, la dimension ne changeant pas par extension des scalaires.

(iii) (i) Notons $D = \dim_{\mathbb{K}}(\mathbb{K}[\mathbf{x}]/I) = \dim_{\mathbb{K}}(\mathcal{A}_{\mathbb{K}})$. Pour $i \in \{1, \dots, n\}$, les éléments $1, x_i, \dots, {x_i}^D$ sont liés dans $\mathcal{A}_{\mathbb{K}}$. On peut donc trouver des scalaires $c_0, \dots, c_D \in \mathbb{K}$ non tous nuls vérifiant $c_0 + c_1 x_i + \cdots + c_D x_i^D = p_i(x_i) \in I$, ce qui montre (ii) pour le corps $\mathbb{K}$. Soit $\zeta_i = (\zeta_{i,1}, \dots, \zeta_{i,n}) \in \mathcal{Z}_{\overline{\mathbb{K}}}(I)$. Ses coordonnées vérifient $c_0 + c_1 \zeta_{i,j} + \cdots + c_d \zeta_{i,j}^d = 0$, ainsi l'ensemble $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$ est fini. Ce qui montre donc (i). □

Dans la suite, nous noterons $\mathcal{Z}_{\overline{\mathbb{K}}}(I) = \{\zeta_1, \ldots, \zeta_d\}, \dim_{\mathbb{K}} \mathcal{A} = D$ et $(\mathbf{x}^\alpha)_{\alpha \in E}$ (avec card(E) = D) une base monomiale de $\mathcal{A}$.

Pour $n = 2$, la figure ci-dessous représente un exemple de base $(\mathbf{x}^\alpha)_{\alpha\in E}$. Les monômes situés au dessus des gros points noirs se réduisent à des combinaisons linéaires des éléments $(\mathbf{x}^\alpha)_{\alpha\in E}$, modulo l'idéal I.



Exemple 3.2.2. — *Soit I l'idéal de $\mathbb{K}[x_1, x_2]$ engendré par*

```
f1 := 13*x[1]^2+8*x[1]*x[2]+4*x[2]^2-8*x[1]-8*x[2]+2:
f2 := x[1]^2+x[1]*x[2]-x[1]-1/6:
```

Le quotient $\mathcal{A} = \mathbb{K}[x_1, x_2]/I$ est un espace vectoriel de dimension 4, de base $1, x_1, x_2, x_1x_2$. Nous vérifions par exemple que

```
expand(x[1]*x[1] -f2);
```

$$x_1^2 \equiv -x_1x_2 + x_1 + \frac{1}{6}$$

```
expand(x[1]*(x[1]*x[2])+1/9*x[1]*f1-(5/9+13/9*x[1]+4/9*x[2])*f2);
```

$$x_1^2x_2 \equiv -x_1x_2 + \frac{55}{54}x_1 + \frac{2}{27}x_2 + \frac{5}{54}.$$

Il est « facile » de vérifier algorithmiquement si une variété est de dimension 0, à partir d'une base de Gröbner $\{g_1, \ldots, g_t\}$ de I :

Proposition 3.2.3. — *Soit $\{g_1, \ldots, g_t\}$ est une base de Gröbner de I, pour un ordre monomial. La variété $\mathcal{Z}_{\mathbb{K}}(I)$ est de dimension 0 si et seulement si, pour tout $i \in \{1, \ldots, n\}$, il existe $(j, m_j) \in \mathbb{N} \times \mathbb{N}$ tel que $md(g_j) = x_i^{m_j}$.*

Démonstration. D'après l théorème 3.2.1, $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$ est de dimension finie, si et seulement si, $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ est un espace vectoriel de dimension finie, donc si et seulement si, $\mathbb{K}[\mathbf{x}]/md(I) = \mathbb{K}[\mathbf{x}]/(md(g_1), \ldots, md(g_t))$ est de dimension finie (voir chap. 2). Le quotient par un idéal monomial est de dimension finie, si et seulement si, cet idéal contient une puissance de chaque variable, ce qui montre la proposition. □

Nous avons par ailleurs un résultat plus précis si on choisit l'ordre lexicographique :

Corollaire 3.2.4. — *Si l'idéal I est zéro-dimensionnel et $\{g_1, \ldots, g_t\}$ est une base de Gröbner de I pour l'ordre lexicographique tel que $x_1 < \cdots < x_n$, alors on peut réordonner $g_1, \ldots, g_t$ pour que $g_1 \in \mathbb{K}[x_1], g_2 \in \mathbb{K}[x_1, x_2]$ et $md(g_2)$ soit une puissance de $x_2, \ldots, g_n \in \mathbb{K}[x_1, \ldots, x_n]$ et $md(g_n)$ soit une puissance de x^n.*

Démonstration. D'après la proposition 3.2.3, il existe $(m_1, \dots, m_n) \in \mathbb{N}^n$ tel que $md(g_i) = x_i^{m_i}, 1 \le i \le n$. Comme l'ordre choisi est l'ordre lexicographique $x_1 < \cdots < x_n$, $g_i \in \mathbb{K}[x_1. \dots, x_i], 1 \le i \le n$. □

On peut donc utiliser ce corollaire pour transformer la résolution d'un système d'équations polynomiales de $\mathbb{K}[\mathbf{x}]$ ayant un nombre fini de solutions en la résolution d'un système triangulaire, c'est-à-dire en la *résolution de polynômes en une variable.* Ce calcul de base de Gröbner lexicographique est en général coûteux et donc peu utilisé en pratique. Nous verrons, plus loin, que l'on peut transformer ce problème de manière, plus économique, en un problème de *valeurs et vecteurs propres.*

3.3. Le dual de $\mathcal{A}$

Un ingrédient important de l'approche matricielle que nous présentons est la dualité au sens classique. Nous supposerons ici $\mathbb{K} = \overline{\mathbb{K}}$ algégriquement clos.

Notons R l'anneau $\mathbb{K}[\mathbf{x}]$ et $\mathcal{A} = R/I$ l'algèbre quotient que nous supposons de dimension finie D sur $\mathbb{K}$, de base $(\mathbf{x}^\alpha)_{\alpha \in E}$ où $E \subset \mathbb{N}^n$. Le $\mathbb{K}$-espace vectoriel des formes linéaires sur R (resp. $\mathcal{A}$) sera noté $\widehat{R}$ (resp. $\widehat{\mathcal{A}}$). La base duale dans $\widehat{\mathcal{A}}$ de la base $(\mathbf{x}^\alpha)_{\alpha \in \mathbb{N}^n}$ de R sera notée $(\mathtt{d}^\alpha)_{\alpha \in \mathbb{N}^n}$. La base duale dans $\widehat{\mathcal{A}}$ de la base monomiale $(\mathbf{x}^\alpha)_{\alpha \in E}$ sera notée $(\delta^\alpha)_{\alpha \in E}$. Toute forme linéaire $\Lambda \in \widehat{\mathcal{A}}$ s'écrit donc

$$\Lambda = \sum_{\alpha \in E} \Lambda(\mathbf{x}^\alpha)\delta^\alpha.$$

Le dual $\widehat{\mathcal{A}}$ s'identifie (naturellement) à l'ensemble des éléments de $\widehat{R}$ qui s'annulent sur l'idéal I. Aussi, il sera parfois noté $I^\perp$. Si $p \in R$, $\delta^\alpha(p)$ est le coefficient $r_{\mathbf{a}}$ de $\mathbf{x}^\alpha$ dans la forme normale de p dans la base $(\mathbf{x}^\alpha)_\alpha$ de $\mathcal{A}$. Si cette base $\mathbf{x}^\alpha$ est obtenue à partir d'une base de Gröbner, $\delta^\alpha(p)$ est le coefficient de $\mathbf{x}^\alpha$ dans le reste r de la division de p par la base de Gröbner de I.

Remarquons que $\widehat{\mathcal{A}}$ est muni d'une structure naturelle de $\mathcal{A}$-module de la façon suivante : $\forall a \in \mathcal{A}, \forall \Lambda \in \widehat{\mathcal{A}}$,

$$\begin{array}{rcl} a \cdot \Lambda : \mathcal{A} & \to & \mathbb{K} \\ b & \mapsto & a \cdot \Lambda(b) = \Lambda(ab). \end{array}$$

Parmi les éléments de $\widehat{\mathcal{A}}$, considérons, pour $\zeta \in V(I)$, la forme linéaire

$$\begin{array}{rcl} \mathbf{1}_\zeta : \mathcal{A} & \to & \mathbb{K} \\ a & \mapsto & a(\zeta), \end{array}$$

appelée *évaluation en* ζ. Comme $\zeta \in V(I)$, $\mathbf{1}_\zeta$ s'annule sur I et est donc bien un élément de $\widehat{\mathcal{A}} = I^\perp$. Il s'écrit dans la base $(\delta^\alpha)_{\mathbf{a} \in E}$ sous la forme

$$\mathbf{1}_\zeta = \sum_{\alpha = (\mathbf{a}_1, \dots, \mathbf{a}_n) \in E} \zeta_1^{\mathbf{a}_1} \cdots \zeta_n^{\mathbf{a}_n} \delta^\alpha \ .$$

3.4. Les opérateurs de multiplication

Si $a \in \mathcal{A}$, nous allons nous intéresser à l'opérateur de multiplication par a dans $\mathcal{A}$,

$$\begin{array}{rcl} M_a \ : \ \mathcal{A} & \to & \mathcal{A} \\ b & \mapsto & M_a(b) = a\, b. \end{array}$$

$\mathtt{M}_a$ désignera la matrice de M_a dans la base $(\mathbf{x}^{\mathbf{a}})_{\mathbf{a}\in E}$. L'endomorphisme M_a induit l'application $\mathbb{K}$-linéaire,

$$\begin{array}{rcl} M_a^t \ : \widehat{\mathcal{A}} & \to & \widehat{\mathcal{A}} \\ \Lambda & \mapsto & M_a^t(\Lambda) = a \cdot \Lambda = \Lambda \circ M_a. \end{array}$$

La matrice de M_a^t dans la base $(\delta_\alpha)_{\mathbf{a}\in E}$ est la transposée de la matrice $\mathtt{M}_a$. Ainsi les deux endomorphismes M_a et M_a^t ont les mêmes valeurs propres.

La résolution des systèmes polynomiaux par des méthodes matricielles est basée sur le résultat suivant :

Théorème 3.4.1. —

1. *Pour tout $a \in \mathcal{A}$, les valeurs des opérateurs M_a sont $a(\zeta_1), \dots, a(\zeta_d)$. En particulier, les valeurs propres de $M_{x_i}, 1 \le i \le d$, sont les $i^{\text{èmes}}$ coordonnées des racines $\zeta_1, \dots, \zeta_d$ de $V(I)$.*
2. *Les vecteurs propres communs à tous les endomorphismes $(M_a^t)_{a\in\mathcal{A}}$ sont (à un scalaire non-nul près) les éléments $\mathbf{1}_{\zeta_1}, \dots, \mathbf{1}_{\zeta_d}$, pour les valeurs propres $a(\zeta_1), \dots, a(\zeta_d)$.*

Démonstration. Soit $a \in \mathcal{A}$. Pour tout b dans $\mathcal{A}$ et tout $i = 1, \dots, d$, nous avons

$$M_a^t(\mathbf{1}_{\zeta_i})(b) = \mathbf{1}_{\zeta_i}(a\, b) = a(\zeta_i)\, \mathbf{1}_{\zeta_i}(b), \text{ ie. } M_a^t(\mathbf{1}_{\zeta_i}) = a(\zeta_i)\, \mathbf{1}_{\zeta_i}.$$

Ceci nous montre que l'ensemble des valeurs propres de M_a contient $a(\zeta_1), \dots, a(\zeta_d)$ et que les évaluations aux racines $\mathbf{1}_{\zeta_i}$ sont des vecteurs propres communs à tous les M_a^t.

Montrons inversement qu'une valeur propre de M_a est de la forme $a(\zeta_i)$. Considérons pour cela le polynôme

$$p(\mathbf{x}) = \prod_{\zeta\in\mathcal{Z}(I)} (a(\mathbf{x}) - a(\zeta)).$$

Il s'annule sur $\mathcal{Z}(I)$, donc d'après le théorème des zéros de Hilbert (voir [**4**] p. 175), il existe $d ß n \mathbb{N}$ tel que $p^d(\mathbf{x}) \in I : \prod_{\zeta\in\mathcal{Z}(I)} (a(\mathbf{x}) - a(\zeta))^d \equiv 0$ modulo I. On en déduit donc que

$$\prod_{\zeta\in\mathcal{Z}(I)} (M_a - a(\zeta)\, \mathbb{I})^d = 0.$$

Le polynôme minimal de M_a divise donc $\prod_{\zeta\in\mathcal{Z}(I)} (T - a(\zeta))^d$ et les valeurs propres de M_a sont dans l'ensemble $\{a(\zeta), \zeta \in \mathcal{Z}(I)\}$.

Montrons maintenant le point 2. Soit $\Lambda \in \widehat{\mathcal{A}}$ un vecteur propre non-nul, commun aux $(M_{x_i}^t)_{i=1,\dots,n}$ (et donc à tous les M_a^t, $a \in \mathcal{A}$) pour les valeurs propres $(\gamma_i)_{i=1,\dots,n} : M_{x_i}^t(\Lambda) - \gamma_i \Lambda = 0$. On en déduit que pour tout monôme $\mathbf{x}^\alpha$ de R, nous avons

$$M_{x_i}^t(\Lambda)(\mathbf{x}^\alpha) = \Lambda(x_i\, \mathbf{x}^\alpha) = \gamma_i \Lambda(\mathbf{x}^\alpha),$$

et donc si $\mathbf{x}^{\mathbf{a}} = x_i\, \mathbf{x}^{\mathbf{a}'}$, $\Lambda(\mathbf{x}^{\mathbf{a}}) = \gamma_i\, \mathbf{x}^{\mathbf{a}'}$. Par récurrence, ceci implique que $\Lambda(\mathbf{x}^\alpha) = \gamma_1^{\alpha_1} \cdots \gamma_n^{\alpha_n}\, \Lambda(1) = \Lambda(1)\, \mathbf{1}_\gamma(\mathbf{x}^\alpha)$ et donc que $\Lambda = \Lambda(1)\, \mathbf{1}_\gamma$, où $\gamma = (\gamma_1, \dots, \gamma_n)$ et $\mathbf{1}_\gamma \in \widehat{R}$ est l'évaluation en γ. Comme $\Lambda \in \widehat{\mathcal{A}} \equiv I^\perp$, on doit avoir pour tout $p \in I$, $\mathbf{1}_\gamma(p) = p(\gamma) = 0$, ce qui veut dire que $\gamma \in V(I)$ est l'un des points ζ_i. □

Remarque 3.4.2. — *Pour tout $a \in R$, l'ensemble des vecteurs propres de M_a est $\cup_i (I : a - a(\zeta_i))/I$.*

D'après le théorème précédent, nous pouvons donc calculer les racines simples par un seul calcul de vecteurs propres, si la base choisie $(\mathbf{x}^\alpha)_\alpha$ de $\mathcal{A}$ contient $1, x_1, \dots, x_n, \dots$.

3.4.1. CALCUL DES RACINES PAR LES VECTEURS PROPRES.

```
Supposons que la base de 𝒜 contienne 1, x1, ..., xn. Soit a ∈ R et Ma la matrice de
la multiplication par x1 dans cette base.
  1. Calculer les vecteurs propres Λ = [Λ1, Λx1, ..., Λxn, ...] de M^t_xi dans la base
     duale de cette base.
  2. Pour tout vecteur propre Λ pour lequel Λ1 ≠ 0, calculer
                         ζ = (Λx1/Λ1, ..., Λxn/Λ1)
Les points ζ ainsi calculés contiennent les racines simples de I.
```

Définition 3.4.3. — *Un vecteur $a \in R$ est dit séparant pour $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$ si l'application*

$$\begin{array}{rcl} \mathcal{Z}_{\overline{\mathbb{K}}}(I) & \to & \overline{\mathbb{K}} \\ \xi & \mapsto & a(\xi) \end{array}$$

est injective.

Si les racines sont simples et a sépare les racines, alors l'algorithme ci-dessus donne exactement les racines de $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$.

Exemple 3.4.4. — *Reprenons les données de l'exemple 3.2.2 et la base $(1, x_1, x_2, x_1x_2)$ du quotient $\mathcal{A}$. Calculons la matrice de multiplication par x_1 dans cette base:*

$$\begin{array}{rcl} 1 \times x_1 & \equiv & x_1, \\ x_1 \times x_1 & \equiv & -x_1x_2 + x_1 + \dfrac{1}{6}, \\ x_2 \times x_1 & \equiv & x_1x_2, \\ x_1x_2 \times x_1 & \equiv & x_1x_2 + \dfrac{55}{54}\,x_1 + \dfrac{2}{27}\,x_2 + \dfrac{5}{54}. \end{array}$$

Deux produits se calculent facilement (ceux à l'intérieur de la base) et pour les autres, nous utilisons les calculs de l'exemple précédent. La matrice de M_{x_1} dans cette base est donc

```
M1 := matrixof([x[1],  x[1]*x[1] -f2,  x[1]*x[2],
    x[1]*(x[1]*x[2])+1/9*x[1]*f1-(5/9+13/9*x[1]+4/9*x[2])*f2],
     [x[1],x[2]], [1,x[1],x[2],x[1]*x[2]]);
```

$$M_{x_1} = \begin{bmatrix} 0 & \frac{1}{6} & 0 & \frac{5}{54} \\ 1 & 1 & 0 & \frac{55}{54} \\ 0 & 0 & 0 & \frac{2}{27} \\ 0 & -1 & 1 & -1 \end{bmatrix}.$$

Nous vérifions, de même, que la matrice de multiplication par x_2 est

```
M2 := matrixof([x[2],  x[1]*x[2] ,
    x[2]*x[2]-1/4*f1+13/4*f2,
    x[1]*x[2]^2-1/9*x[1]*f1+1/9*(13*x[1]-5*x[2]+5)*f2],
    [x[1],x[2]],[1,x[1],x[2],x[1]*x[2]]);
```

$$M_{x_2} = \begin{bmatrix} 0 & 0 & -\frac{25}{24} & -\frac{5}{54} \\ 0 & 0 & -\frac{5}{4} & -\frac{55}{54} \\ 1 & 0 & 2 & \frac{5}{54} \\ 0 & 1 & \frac{5}{4} & 2 \end{bmatrix}.$$

Calculons les valeurs propres, multiplicités et vecteurs propres (en normalisant leur première coordonnée à 1) de la transposée $M_{x_1}^t$, :

```
neigenvects(transpose(M1),1);
```

$$[-\frac{1}{3}, 2, \left\{[1, -\frac{1}{3}, \frac{5}{6}, -\frac{5}{18}]\right\}], [\frac{1}{3}, 2, \left\{[1, \frac{1}{3}, \frac{7}{6}, \frac{7}{18}]\right\}].$$

Comme la base choisie est $(1, x_1, x_2, x_1x_2)$, le théorème précédent nous dit que les coordonnées des solutions du système sont les deuxièmes et troisièmes coordonnées de ces vecteurs : $\zeta_1 = (-\frac{1}{3}, \frac{5}{6})$, $\zeta_2 = (\frac{1}{3}, \frac{7}{6})$. Nous vérifions sur ce calcul que la quatrième coordonnée des vecteurs propres (correspondant à x_1x_2) est le produit des deuxièmes et troisièmes coordonnées.

Dans le cas où a coincïde pour deux racines ou dans le cas de racines multiples, les espaces propres associés sont de dimension ≥ 1 et les vecteurs propres sont des combinaisons linéaires de générateurs, ce qui permet de paramétrer les points conduisant à des solutions du système sans pour autant les donner explicitement.

Pour remédier à ce problème, nous pouvons remarquer que les matrices de multiplication $\mathtt{M}_{x_i}$ commutent, et utiliser la propriété suivante :

Proposition 3.4.5. — *Les matrices $\mathtt{M}_{x_i}$ se décomposent sous forme triangulaire T_i dans une même base. Notons $t_{i,i}^j$ le $i^{ème}$ élément sur la diagonale de T_j. Alors les points $\mathtt{t}_i = (t_{i,i}^1, \ldots, t_{i,i}^n)$, $i = 1, \ldots, D$ sont les racines de I, comptées avec multiplicité.*

Démonstration. Comme les matrices $\mathtt{M}_{x_i}$ commutent, elles se décomposent sous forme triangulaire $\mathtt{T}_{x_i}$ dans une même base. Pour tout $p \in I$, nous avons $\mathtt{M}_p = p(\mathtt{M}_{x_1}, \ldots, \mathtt{M}_{x_n}) = 0$ et donc $p(\mathtt{T}_{x_1}, \ldots, \mathtt{T}_{x_n}) = 0$. Nous en déduisons que les éléments diagonaux $\mathtt{t}_i = (t_{i,i}^1, \ldots, t_{i,i}^n)$ des matrices $\mathtt{T}_{x_i}$ vérifient aussi $p(t_{i,i}^1, \ldots, t_{i,i}^n) = 0$. Ce sont donc des racines de I.

Inversement, montrons que toute racine ζ de $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$ est l'un des vecteurs $\mathtt{t}_i$. Quitte à prendre une combinaison linéaire convenable $s = \sum_{i=1}^n \lambda_i x_i$, nous pouvons supposer que s sépare les points de $\mathcal{Z}_{\overline{\mathbb{K}}}(I)$: $s(\zeta_i) \neq s(\zeta_j)$ si $i \neq j$. Les valeurs propres de M_s sont les termes diagonaux de la matrices $\mathtt{T}_s = \sum_{j=1}^n \lambda_j \mathtt{T}_{x_j}$, c'est-à-dire les $s(\mathtt{t}_i)$, $i = 1, \ldots, D$. D'après le théorème 3.4.1, pour chaque racine $\zeta \in \mathcal{Z}_{\overline{\mathbb{K}}}(I)$, $s(\zeta_i)$ est valeur propre de M_s. Il existe donc $i_0 \in \{1, \ldots, D\}$ tel que $s(\zeta) = s(\mathtt{t}_{i_0})$. Comme $\mathtt{t}_{i_0} \in \mathcal{Z}_{\overline{\mathbb{K}}}(I)$ et s est séparant, $\zeta = \mathtt{t}_{i_0}$, ce qui montre la proposition. □

Ce qui conduit à l'algorithme suivant :

3.4.2. CALCUL DES RACINES PAR TRIANGULATION SIMULTANÉE.

1. Calculer les matrices $\mathtt{M}_{x_i}$ dans une base de $\mathcal{A}$.
2. Calculer une décomposition de Schur telle que $\mathtt{T}_{x_1} = \mathtt{P}\mathtt{M}_{x_1}\mathtt{P}^{-1}$ soit triangulaire.
3. Calculer les matrices $\mathtt{T}_{x_i} = \mathtt{P}\mathtt{M}_{x_i}\mathtt{P}^{-1}$, $i = 2, \ldots, n$ qui sont aussi triangulaires.

Les racines sont les vecteurs diagonaux $\mathtt{t}_i = (t_{i,i}^1, \ldots, t_{i,i}^n)$ des matrices $\mathtt{T}_{x_i}$, $i = 1, \ldots, n$.

3.5. Décomposition de l'algèbre $\mathcal{A}$

L'idéal I est toujours supposé de dimension 0, ce qui d'après **[2]** [chap. 4], implique la décomposition primaire

$$I = Q_1 \cap \cdots \cap Q_d$$

où Q_i est primaire pour l'idéal maximal $\mathbf{m}_{\zeta_i} = (x_1 - \zeta_{i,1}, \ldots, x_n - \zeta_{i,n})$. Notons $\pi : \mathbb{K}[\mathbf{x}] \longrightarrow \mathcal{A}$ la projection canonique et $\mathcal{A}_i$ le transporteur de Q_i dans $\mathbf{0} = \{0\}$, $(\mathcal{A}_i = (\mathbf{0} : Q_i) = \{a \in \mathcal{A} : a\, q = 0, \forall q \in Q_i\})$. Les $\mathcal{A}_i$ sont des idéaux de $\mathcal{A}$.

Lemme 3.5.1. — *Si Q, Q', S sont des idéaux d'un anneau quelconque A, alors*
i) $(J : Q) \cap (J : Q') = (J : Q + Q')$
ii) *Si de plus $Q + Q' = A$, alors $(J : Q) + (J : Q') = (J : Q \cap Q')$.*

Démonstration. Si $Q + Q' = A$, il existe $(q, s) \in Q \times Q' : 1 = q + s$. Pour tout $a \in (J : Q \cap Q')$, on a $a = aq + as$. On en déduit que $a\, q \in (J : Q')$ et $a\, s \in (J : Q)$, par suite $(J : Q \cap Q') \subset (J : Q) + (J : Q')$. Le reste du lemme est immédiat. □

Nous allons utiliser ce lemme pour montrer le théorème de structure suivant :

Théorème 3.5.2. — *L'algèbre $\mathcal{A}$ est la somme directe des sous-algèbres $\mathcal{A}_1, \ldots, \mathcal{A}_d$:*

$$\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \cdots \oplus \mathcal{A}_d. \tag{1}$$

Démonstration. Vérifions d'abord que $\mathcal{A} = \mathcal{A}_1 + \cdots + \mathcal{A}_d$. En effet, d'après le lemme 3.5.1, on a

$$\mathcal{A}_1 + \cdots + \mathcal{A}_d \equiv (\mathbf{0} : Q_1) + \cdots + (\mathbf{0} : Q_d) \equiv (\mathbf{0} : Q_1 \cap \ldots \cap Q_d) \equiv \mathcal{A},$$

(l'égalité dans $\mathcal{A}$ étant notée $\equiv$), car $Q_i + Q_j = R$.

Montrons que la somme est directe : soit $i \in \{1, \ldots, d-1\}$,

$$\begin{aligned} \mathcal{A}_{i+1} \cap (\mathcal{A}_1 + \ldots + \mathcal{A}_i) &\equiv (\mathbf{0} : Q_{i+1}) \cap \Big((\mathbf{0} : Q_1) + \ldots + (\mathbf{0} : Q_i)\Big) \\ &\equiv (\mathbf{0} : Q_{i+1} + (Q_1 \cap \ldots \cap Q_i)) \equiv (\mathbf{0} : \mathcal{A}) \equiv \mathbf{0}, \end{aligned}$$

ce qui implique la décomposition (1). □

Dans le cas univariable où $R = \mathbb{K}[x]$ et I est engendré par le polynôme $f = \prod_{i=1}^{d}(x - z_i)^{\mu_i}$, ce théorème est une conséquence directe du théorème des restes chinois :

$$\mathcal{A} = \oplus_{i=1}^{d} \mathcal{A}_i,$$

où $\mathcal{A}_i \sim \mathbb{K}[x]/(x - z_i)^{\mu_i}$, les polynômes $(x - z_i)^{\mu_i}$, $i = 1, \ldots, d$ étant premiers entre eux.

Définition 3.5.3. — *La multiplicité de la racine ζ_i est la dimension du sous-espace vectoriel $\mathcal{A}_i$ de $\mathcal{A}$. Elle sera notée μ_{ζ_i} ou μ_i.*

La racine $\mathbf{x}_i$ sera dite simple si $\mu_i = 1$ et multiple si $\mu_i > 1$.

Si l'idéal I admet « localement [1] » un système de n générateurs $f_1, \ldots, f_n$, la multiplicité μ_i correspond de manière plus intuitive, au nombre de solutions voisines de ζ_i du système perturbé $f_1(x) - \epsilon_1 = \cdots = f_n(x) - \epsilon_n = 0$, $\epsilon_1, \ldots, \epsilon_n$, étant assez petits (voir [**1**]).

La définition précédente conduit au résultat classique suivant :

Théorème 3.5.4. — *La dimension du $\mathbb{K}$-espace vectoriel $\mathcal{A}$ est le nombre de racines $\zeta \in V(I)$, comptées avec multiplicité.*

Démonstration. Remarquons pour cela que $\dim_{\mathbb{K}} \mathcal{A} = \sum_{i=1}^{d} \dim \mathcal{A}_i = \sum_{i=1}^{d} \mu_i$. □

Le nombre d de racines distinctes est inférieur à la dimension de $\mathcal{A}$. Il y a égalité si et seulement si les racines de $f_1, \ldots, f_s$ sont simples.

1. en localisant par l'ensemble des fonctions qui ne s'annullent pas en ce point

3.6. Les idempotents de $\mathcal{A}$

D'après le théorème 3.5.2, il existe des éléments uniques $\mathbf{e}_i \in \mathcal{A}_i, 1 \leq i \leq d$, tels que $1 \equiv \mathbf{e}_1 + \cdots + \mathbf{e}_d$. Donc

$$\mathbf{e}_1 + \cdots + \mathbf{e}_d \equiv 1 \equiv 1^2 \equiv \mathbf{e}_1^2 + \ldots + \mathbf{e}_d^2 + 2 \sum_{1 \leq i < j \leq d} \mathbf{e}_i \mathbf{e}_j.$$

Comme $\mathcal{A}_i \cap \mathcal{A}_j = \mathbf{0}$ si $i \neq j$ (théorème 3.5.2), on a donc $\mathbf{e}_i \, \mathbf{e}_j \equiv 0$. Les $\mathbf{e}_i$ sont des idempotents orthogonaux de $\mathcal{A}$ (i.e. $\mathbf{e}_i^2 \equiv \mathbf{e}_i, \ \mathbf{e}_i \mathbf{e}_j \equiv 0$ si $i \neq j$).

Proposition 3.6.1. — *La sous-algèbre $\mathcal{A}_i$ de $\mathcal{A}$ coincïde avec $\mathbf{e}_i \mathcal{A}$ et $\mathbf{e}_i$ est l'élément neutre de $\mathcal{A}_i$.*

Démonstration. Soit $a \in \mathcal{A}_i, a \equiv a \cdot 1 \equiv a \, \mathbf{e}_1 + \ldots + a \, \mathbf{e}_d \equiv a \mathbf{e}_i$ (car $\mathcal{A}_i \cap \mathcal{A}_j = \mathbf{0}$ si $i \neq j$). Réciproquement, si $a \in \mathcal{A}$, alors $a \, \mathbf{e}_i \in \mathcal{A}_i$ (car $\mathcal{A}_i$ est un idéal de $\mathcal{A}$). On a donc $\mathcal{A}_i = \mathbf{e}_i \mathcal{A}$.

Par ailleurs, on vient de voir que pour tout $a \in \mathcal{A}_i, a = a \, \mathbf{e}_i$. Il s'ensuit que $a \mathbf{e}_i \equiv a \mathbf{e}_i^2 \equiv a \mathbf{e}_i \equiv a$. □

Proposition 3.6.2. — *Les idempotents $\mathbf{e}_1, \ldots, \mathbf{e}_d$ vérifient*

$$\mathbf{e}_i(\zeta_j) = \delta_{ij},$$

δ_{ij} désignant le symbole de Kronecker.

On rappelle que si $a \in \mathcal{A}$ et $\zeta_i \in \mathcal{Z}_{\overline{\mathbb{K}}}(I)$, $a(\mathbf{x}_i) := p(\mathbf{x}_i)$, où p est un représentant quelconque de a dans $\mathbb{K}[\mathbf{x}]$ $(a \equiv p)$.

Démonstration. Comme $\{\zeta_i\} = \mathcal{Z}(Q_i)$, pour tout $\zeta_j \neq \zeta_i$, il existe un polynôme $q \in Q_i$ tel que $q(\zeta_j) \neq 0$. Or $q \, \mathbf{e}_i \equiv 0$ par définition de $\mathcal{A}_i$. Donc $q(\zeta_j) \, \mathbf{e}_i(\zeta_j) = 0$ et $\mathbf{e}_i(\zeta_j) = 0$.

Pour tout $i \in \{1, \ldots, n\}$, notons $e_i \in R$ est un représentant de $\mathbf{e}_i$. Comme $1 - (e_1 + \ldots + e_d) \in I$, on a $1 = \mathbf{e}_1(\zeta_i) + \ldots + \mathbf{e}_d(\zeta_i) = \mathbf{e}_i(\zeta_i)$. □

Les idempotents $\mathbf{e}_i$ jouent donc un rôle dual des évaluations

$$\begin{array}{rcl} \mathbf{1}_{\mathbf{x}_i} : \mathcal{A} & \to & \mathcal{A} \\ a & \mapsto & \mathbf{1}_{\mathbf{x}_i}(a) = a(\zeta_i), \end{array}$$

c'est-à-dire celui d'une base pour les *polynômes d'interpolations* aux points $\zeta_1, \ldots, \zeta_d$.

Ainsi, si $n = 1$ et I est un idéal engendré par un polynôme f ayant des racines simples, nous avons vu que les idempotents sont les polynômes d'interpolation de Lagrange de f.

3.7. Description des composantes $\mathcal{A}_i$

Considérons l'application surjective

$$\begin{array}{rcl} M_{\mathbf{e}_i} : \mathcal{A} & \to & \mathcal{A}_i \\ a & \mapsto & a \, \mathbf{e}_i. \end{array}$$

Son noyau nous permet de calculer la composante primaire associée à ζ_i :

Proposition 3.7.1. — *Son noyau est* $\ker(M_{\mathbf{e}_i}) = Q_i$.

Démonstration. Pour tout élément $a \in \mathcal{A}$, $M_{\mathbf{e}_i}(a) = a \, \mathbf{e}_i$ est la projection de a sur $\mathcal{A}_i$, donc le noyau de $M_{\mathbf{e}_i}$ est

$$\oplus_{j \neq i} \mathcal{A}_j = \oplus_{j \neq i} (\mathbf{0} : Q_j) = \sum_{j \neq i} (I : Q_j)/I.$$

D'après le lemme 3.5.1,

$$\begin{aligned}\sum_{j\neq i}(I:Q_j) &= (I:\cap_{j\neq i}Q_j) = \cap_{l=1}^{d}(Q_l:\cap_{j\neq i}Q_j)\\ &= (Q_i:\cap_{j\neq i}Q_j) = \sum_{j\neq i}(Q_i:Q_j) = Q_i\ ,\end{aligned}$$

car $(Q_i : Q_j) = Q_i$, les idéaux premiers associés à Q_i et Q_j étant distincts. □
Ceci nous permet maintenant d'identifier la sous-algèbre $\mathcal{A}_i$ avec le quotient par l'idéal primaire Q_i :

Corollaire 3.7.2. — *L'application*

$$\begin{aligned}\phi_i : R/Q_i &\rightarrow \mathcal{A}_i\\ a &\mapsto a\,\mathbf{e}_i\end{aligned}$$

est un isomorphisme.

Démonstration. Considérons l'application

$$\begin{aligned}\pi_i : \mathbb{K}[\mathbf{x}] &\rightarrow \mathcal{A}_i\\ p &\mapsto p\mathbf{e}_i.\end{aligned}$$

Comme $\pi_i(I) = \mathbf{0}$, cette application se factorise en $\pi_i = M_{\mathbf{e}_i} \circ \pi$, où $\pi : \mathbb{K}[\mathbf{x}] \rightarrow \mathcal{A}$ est la projection canonique. Le noyau de π_i est donc l'image réciproque par π du noyau Q_i de $M_{\mathbf{e}_i}$. C'est donc $Q_i + I = Q_i$. L'application π_i induit donc un isomorphisme ϕ_i de R/Q_i vers $\mathcal{A}_i$. □
Par cet isomorphisme, l'image de 1 est l'unité $\mathbf{e}_i$ de $\mathcal{A}_i$.

Proposition 3.7.3. — *$\mathcal{A}_i$ est un anneau local d'idéal maximal $\mathbf{m}_{\zeta_i}$.*

Démonstration. Il suffit pour cela de vérifier que $\mathbf{m}_{\zeta_i}$ est le seul idéal maximal de $\mathcal{A}_i$. Or d'après le corollaire 3.7.2, tout idéal maximal $\mathbf{m}'$ de $\mathcal{A}_i$ induit un idéal maximal (aussi noté $\mathbf{m}'$) dans R, contenant Q_i. On a donc $\sqrt{Q_i} = \mathbf{m}_{\zeta_i} \subset \mathbf{m}'$ et $\mathbf{m}_{\zeta_i} = \mathbf{m}'$ car $\mathbf{m}'$ est maximal. □
Ceci implique en particulier le corollaire suivant :

Corollaire 3.7.4. — *Pour tout $a \in \mathcal{A}$, $(a - a(\zeta_i))\mathbf{e}_i$ est nilpotent.*

Démonstration. Comme $(a - a(\zeta_i))$ est dans $\mathbf{m}_{\zeta_i}$, il existe $N \in \mathbb{N}$ tel que $(a - a(\zeta_i))^N \equiv 0$ dans R/Q_i. Son image $(a - a(\zeta_i))\mathbf{e}_i$ par ϕ_i est donc également nilpotente. □

La proposition 3.7.1 permet, de plus, de construire explicitement un système de générateurs de la composante primaire Q_i par l'algorithme suivant :

3.7.3. COMPOSANTES PRIMAIRES DE L'IDÉAL ZÉRO-DIMENSIONNEL I.

1. Calculer les idempotents $\mathbf{e}_i$.
2. Pour chaque idempotent $\mathbf{e}_i$,
   (a) calculer la matrice de $M_{\mathbf{e}_i}$,
   (b) calculer une base de son noyau $q_i, \ldots, q_{D-\mu_i}$.

L'idéal $I + (q_i, \ldots, q_{D-\mu_i})$ est la composante primaire Q_i.

3.8. Décomposition des opérateurs de multiplication

Comme les sous-algèbres $\mathcal{A}_i$ de $\mathcal{A}$ sont stables par multiplication par les éléments de $\mathcal{A}$, les opérateurs M_a s'y décomposent en blocs de Jordan.

Théorème 3.8.1. — *Il existe une base de $\mathcal{A}$ telle que pour tout $a \in R$, l'opérateur de multiplication M_a se décompose dans cette base sous la forme*

$$\begin{bmatrix} \mathtt{N}_a^1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \mathtt{N}_a^d \end{bmatrix} \text{ avec } \mathtt{N}_a^i = \begin{bmatrix} a(\zeta_i) & & \star \\ & \ddots & \\ \mathbf{0} & & a(\zeta_i) \end{bmatrix}$$

$\mathtt{N}_a^i$ étant la matrice de multiplication par a dans une base convenable de $\mathcal{A}_i$.

Démonstration. Comme les sous-algèbres $\mathcal{A}_i$ sont stables par multiplication et $\mathcal{A}_i\mathcal{A}_j \equiv 0$ si $i \neq j$, les matrices des opérateurs M_a se décomposent suivant les $\mathcal{A}_i$, de manière diagonale par blocs. Le bloc correspondant à $\mathcal{A}_i$ est noté $\mathtt{N}_a^i$. Par ailleurs, comme ces opérateurs commutent, quitte à choisir convenablement la base de $\mathcal{A}_i$, nous pouvons supposer que les $\mathtt{N}_a^i$ sont triangulaires supérieurs, pour tout $a \in R$. D'après le corollaire 3.7.2 et le théorème 3.4.1, la valeur propre de la multiplication par a dans $\mathcal{A}_i$ est $a(\zeta_i)$. Ce qui explique la forme des blocs $\mathtt{N}_a^i$. □

Sur la diagonale du bloc associé à $\mathcal{A}_i$, $a(\zeta_i)$ apparaît donc autant de fois que la multiplicité de ζ_i. Cependant si $a(\zeta_i) = a(\zeta_j)$ pour $i \neq j$, la multiplicité de $a(\zeta_i)$ sera plus grande que la multiplicité de la racine ζ_i.

Ce théorème nous montre que $\mathtt{N}_a^i - a(\zeta_i)\,\mathbb{I}$ est une matrice nilpotente. L'indice de nilpotence et les blocs de Jordan de $\mathtt{N}_a^i$ peuvent varier suivant a comme le montre l'exemple suivant :

Exemple 3.8.2. — *$R = \mathbb{K}[x_1, x_2]$ et $I = (x_1^2, x_2^2)$, $V(I) = \{(0,0)\}$. Il y a une seule composante primaire et une seule composante dans la décomposition de l'algèbre $\mathcal{A}$. Une base de $\mathcal{A}$ est $(1, x_1, x_2, x_1x_2)$ et la multiplicité de $(0,0)$ est 4. L'algèbre $\mathcal{A}$ est donc une algèbre locale d'idéal maximal $\mathbf{m}_0 = (x_1, x_2)$. La matrice de M_{x_1} dans la base $(x_1x_2, x_2, x_1, 1)$ a deux blocs de Jordan*

$$\mathtt{M}_{x_1} = \left[\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

La matrice de M_{x_2} dans la base $(x_1x_2, x_2, x_1, 1)$ est également triangulaire supérieure :

$$\mathtt{M}_{x_2} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Cette matrice a également deux blocs de Jordan de taille 2, dans la base $(x_1x_2, x_1, x_2, 1)$.

La matrice de multiplication par $x_1 + x_2$ dans la base $\{x_1 - x_2, 2\,x_1\,x_2, x_1 + x_2, 1\}$ est

$$\left[\begin{array}{c|ccc} 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

Nous voyons sur cet exemple que les blocs de Jordan ne sont pas forcément de taille constante. En fait la taille maximale d'un tel bloc d'une matrice $\mathtt{N}_s$ est le plus petit indice *tel que $s^k \equiv 0$. Ici pour $p = x_1 + x_2$, $p^3 = 0$ et $p^2 \neq 0$ et tout élément $s \in \mathbf{m}_0$ vérifie $s^3 \neq 0$. L'indice minimal k tel $\mathbf{m}_0^k \neq 0$ (ici 3) est appelé l'indice de* nilpotence.

Ce théorème de structure va nous permettre de calculer la forme de Chow de $\mathcal{Z}(I)$:

Définition 3.8.3. — *La forme de Chow de $\mathcal{Z}(f_1, .., f_m) = \mathcal{Z}(I)$ est le polynôme des variables $\mathbf{u} = (u_1, \dots, u_n)$ suivant :*

$$\mathcal{C}_I(\mathbf{u}) = \prod_{\zeta \in \mathcal{Z}_{\overline{\mathbb{K}}}(I)} (u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)^{\mu_\zeta}$$

où μ_ζ est la multiplicité de $\zeta \in \mathcal{Z}(I)$.

Proposition 3.8.4. — *La forme de Chow de $\mathcal{Z}(I)$ est le déterminant de la multiplication par $u_0 + u_1\, x_1 + \cdots + u_n\, x_n$ dans $\mathcal{A}_{K(\mathbf{u})}$.*

Démonstration. D'après le théorème 3.8.1, les matrices de multiplication par x_i se décomposent (dans une même base) diagonalement en blocs triangulaires $\mathtt{N}_{x_i}^{\zeta}$, $\zeta \in \mathcal{Z}(I)$. Le déterminant de $M_{u_0+u_1\,x_1+\cdots+u_n\,x_n}$ est donc le produit des déterminants $\det(u_0\,\mathbb{I} + u_1\mathtt{N}_{x_1}^{\zeta} + \cdots + u_n\,\mathtt{N}_{x_n}^{\zeta})$, pour $\zeta \in \mathcal{Z}(I)$. Les blocs $\mathtt{N}_{x_i}^{\zeta}$ étant triangulaires de taille la multiplicité μ_ζ de ζ (voir définition 3.5.3) et les termes de leur diagonale étant la i^{ème} coordonnée de la racine ζ, nous avons donc

$$\det(M_{u_0+u_1\,x_1+\cdots+u_n\,x_n}) = \prod_{\zeta \in \mathcal{Z}(I)} (u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)^{\mu_\zeta}.$$

□

Ceci nous montre en particulier que $\mathcal{C}_I(\mathbf{u}) \in \mathbb{K}[\mathbf{u}]$. Nous noterons

$$\tilde{\mathcal{C}}_I(\mathbf{u}) = \prod_{\zeta \in \mathcal{Z}_{\overline{\mathbb{K}}}(I)} (u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n),$$

sa partie sans facteur carré. Nous l'appellerons *la forme de Chow réduite*. C'est aussi un polynôme de $\mathbb{K}[\mathbf{u}]$, qui s'obtient par calcul du pgcd de $\mathcal{C}_i(\mathbf{u})$ et de $\frac{\partial}{\partial_{u_0}}(\mathcal{C}_i(\mathbf{u}))$.

3.9. Représentation univariée rationnelle

L'idée de la représentation univariée rationnelle est de décrire les solutions d'un système zéro-dimensionel de $\mathbb{K}[\mathbf{x}]$ comme les images par une application rationnelle des zéros d'un polynôme en une variable. Nous allons, pour cela, utiliser la forme de Chow $\mathcal{C}_I(\mathbf{u})$.

Théorème 3.9.1. — *Soit $\Delta(\mathbf{u})$ un multiple de la forme de Chow $\mathcal{C}_I(\mathbf{u})$. Alors pour un choix générique de $t = (t_0, \dots, t_n) \in \mathbb{K}^{n+1}$, nous avons*

$$\frac{\Delta}{pgcd(\Delta, \frac{\partial \Delta}{\partial u_0})}(t+u) = d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0) + r(\mathbf{u})$$

avec $r(\mathbf{u}) \in (u_1, \dots, u_n)^2$, $pgcd(d_0(u_0), d_0'(u_0)) = 1$ et pour tout $\zeta = (\zeta_1, \dots, \zeta_n) \in V$, il existe ζ_0 racine de $d_0(u_0) = 0$ telle que

$$d_0'(\zeta_0)\zeta_i - d_i(\zeta_0) = 0\ ,\ i = 1, \dots, n.$$

Ce théorème décrit les coordonnées des points $\zeta \in V$ comme les valeurs des fractions rationnelles $\frac{d_i(u_0)}{d_0'(u_0)}$ en certaines racines de $d_0(u_0) = 0$. Cette approche remonte à F.S. Macaulay, qui l'utilise pour calculer une décomposition primaire d'un idéal (voir la note en bas de la page **[8]**[p. 88]). Nous reviendrons plus loin sur l'extension de cette méthode au cas non zéro-dimensionnel. Pour montrer le théorème précédent, nous avons besoin du lemme suivant :

Lemme 3.9.2. — *Soient $A(\mathbf{u}), B(\mathbf{u}) \in \mathbb{K}[u_0, \dots, u_n]$ premiers entre eux. Alors pour $t = (t_0, t_1, \dots, t_n) \in \mathbb{K}^{n+1}$ générique et pour $w = (t_0 + u_0, t_1, \dots, t_n)$, $A(w)$ et $B(w) \in \mathbb{K}[u_0]$ sont premiers entre eux.*

Démonstration. Les racines de $A(w)$ et (resp $B(w)$) correspondent aux points d'intersections de la droite $L_t(u_0) = (t_0 + u_0, t_1, \dots, t_n)$ avec $\mathcal{Z}(A(\mathbf{u}) = 0)$ (resp $\mathcal{Z}(B(\mathbf{u}) = 0)$). Comme $A(\mathbf{u})$ et $B(\mathbf{u})$ sont premiers entre eux, l'intersection est de codimension ≥ 2 dans $\mathbb{K}^{n+1}$. Donc pour t générique, L_t ne coupe pas la variété et les polynômes $A(w)$ et $B(w)$ n'ont pas de racines communes dans $\overline{\mathbb{K}}$, ce qui prouve le lemme. □

Démonstration du théorème. Décomposons $\Delta(\mathbf{u})$ en

$$\Delta(\mathbf{u}) = \prod_{\zeta \in \mathcal{Z}_{\overline{\mathbb{K}}}(I)} (u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)^{n_\zeta} H(\mathbf{u})$$

avec $\prod_{\zeta \in \mathcal{Z}_0}(u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)^{n_\zeta}$ et $H(\mathbf{u})$ premiers entre eux.
On note $d(\mathbf{u}) = \frac{\Delta(\mathbf{u})}{\mathrm{pgcd}(\Delta(\mathbf{u}), \frac{\partial \Delta}{\partial u_0}(\mathbf{u}))}$

$$d(\mathbf{u}) = \prod_{\zeta \in \mathcal{Z}_0} (u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n) h(\mathbf{u})$$

où $\prod_{\zeta \in \mathcal{Z}_0}(u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)$ et $h(\mathbf{u})$ sont premiers entre eux.

Soit $t = (t_0, \dots, t_n)$ générique,

$$\begin{aligned} d(t+u) &= d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0) + r(\mathbf{u}) \\ &= \prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n) h(t+u) \\ h(t+u) &= h_0(u_0) + u_1 h_1(u_0) + \cdots + u_n h_n(u_0) + s(\mathbf{u}) \end{aligned}$$

où $t(\zeta) = t_0 + t_1\zeta_1 + \cdots + t_n\zeta_n$ et $r(\mathbf{u}), s(\mathbf{u}) \in (u_1, \dots, u_n)^2$. Par identification des coefficients, on obtient

$$\begin{aligned} d_0(u_0) &= \prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0) h_0(u_0), \\ d_i(u_0) &= \left(\sum_{\zeta \in \mathcal{Z}_0} \zeta_i \prod_{\zeta' \neq \zeta} (t(\zeta') + u_0) \right) h_0(u_0) + \prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0) h_i(u_0). \end{aligned}$$

On a donc

$$d_0'(u_0) = \left(\sum_{\zeta \in \mathcal{Z}_0} \prod_{\zeta' \neq \zeta} (t(\zeta') + u_0) \right) h_0(u_0) + \prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0) h_0'(u_0).$$

D'après le lemme 3.9.2, $\prod_{\zeta \in \mathcal{Z}_0} (t(\zeta) + u_0)$ et $h_0(u_0)$ sont premiers entre eux pour t générique car $\prod_{\zeta \in \mathcal{Z}_0} (u_0 + u_1\zeta_1 + \cdots + u_n\zeta_n)$ et $h(\mathbf{u})$ sont premiers entre eux. Ils n'ont donc pas de racine commune.

Soit $\zeta_0 = -t(\zeta)$ une racine de $d_0(u_0)$, ce qui implique d'après ci-dessus que $(h_0(\zeta_0) \neq 0)$:

$$\begin{aligned} d_0'(\zeta_0) &= \left(\prod_{\zeta' \neq \zeta} (t(\zeta') - t(\zeta))\right) h_0(\zeta_0) \\ d_i(\zeta_0) &= \zeta_i \left(\prod_{\zeta' \neq \zeta} (t(\zeta') - t(\zeta))\right) h_0(\zeta_0) \end{aligned}$$

Comme t est générique, on a pour tout $\zeta' \neq \zeta, t(\zeta') \neq t(\zeta)$, et $d_0'(\zeta_0) \neq 0$, donc

$$\zeta_i = \frac{d_i(\zeta_0)}{d_0'(\zeta_0)}.$$

□

Cette représentation n'est pas minimale. En effet, toutes les racines de $d_0(u_0) = 0$ ne définissent pas nécessairement des racines $\in \mathcal{Z}(I)$. Notons cependant que, comme les polynômes $d_0(u_0)$ et $d_0'(u_0)$ sont premiers entre eux, les fractions $\zeta_i(u_0) = \frac{d_i(u_0)}{d_0'(u_0)}$ $(i = 0, \ldots, n)$ sont bien définies aux racines de $d_0(u_0)$.

Les bonnes racines sont celles pour lesquelles $g_i(u_0) = f_i(\zeta_1(u_0), \ldots, \zeta_n(u_0)) = 0$, c'est-à-dire les racines des facteurs irréductibles de $d_0(u_0)$, qui divisent les numérateurs des $g_i(u_0)$. Pour récupérer une représentation minimale de $\mathcal{Z}(I)$, on pourra donc

- factoriser $d_0(u_0)$ en facteurs irréductibles $p_1, \ldots, p_s$,
- substituer x_i dans $f_1, \ldots, f_n$, par $\frac{d_i(u_0)}{d_0'(u_0)}$, pour obtenir les fractions rationnelles $g_i(u_0)$,
- enfin on gardera les $p_j(u_0)$ qui divisent les numérateurs des $g_i(u_0)$.

Dans le cas où $\Delta(\mathbf{u})$ est exactement la forme de Chow $\mathcal{C}_I(\mathbf{u})$, nous pouvons être plus précis :

Proposition 3.9.3. — *Avec les notations du théorème précédent, si $\Delta(\mathbf{u}) = \mathcal{C}_I(\mathbf{u})$ et t est séparant, alors il y a bijection entre les racines de $d_0(u_0) = 0$ et celles de $\mathcal{Z}(I)$.*

Démonstration. La démonstration est laissée en exercice. □

3.9.4. REPRÉSENTATION RATIONNELLE DES ZÉROS $\mathbf{x}_1, \ldots, \mathbf{x}_d$ DE L'IDÉAL ZÉRO-DIMENSIONNEL I.

1. Calculer un multiple $\Delta(\mathbf{u})$ de la forme de Chow réduite $\tilde{\mathcal{C}}_I(\mathbf{u})$ et enlever les facteurs carrés (en calculant $d(\mathbf{u}) = \frac{\Delta(\mathbf{u})}{\mathrm{pgcd}(\Delta(\mathbf{u}), \frac{\partial \Delta}{\partial u_0}(\mathbf{u}))}$).
2. Choisir un élément générique $t \in \mathbb{K}^{n+1}$ et calculer les coefficients $d_0(u_0), d_1(u_0), \ldots, d_n(u_0)$ du développement de $d(t + u)$, (en vérifiant que $d_0(u_0)$ est sans facteur carré),
3. En déduire une représentation rationnelle $\zeta_i = \frac{d_i(u_0)}{d_0'(u_0)}, i = 1, \ldots, n,$ $d_0(u_0) = 0$,
4. Factoriser $d_0(u_0)$ et ne garder que les facteurs premiers qui divisent les numérateurs des $g_i(u_0) = f_i(\zeta_1(u_0), \ldots, \zeta_n(u_0))$, pour obtenir une représentation minimale.

Cet algorithme nous fournit encore une autre méthode pour calculer les solutions d'un système d'équations polynomiales, en résolvant dans un premier temps une équation en une variable, puis en reportant la solution dans les fractions rationnelles représentant les coordonnées des racines. Cette approche se prête bien à des calculs exacts, et sur des nombres algébriques. Nous pouvons ainsi décrire le quotient $\mathcal{A} = R/I$, à partir des nombres algébriques définis par les bons facteurs premiers de $d_0(u_0)$. Cette méthode peut être utilisée dès qu'une base de Gröbner, pour un ordre quelconque est calculée. Il suffit alors de calculer les matrices de multiplication $\mathtt{M}_{x_i}$ dans une base quelconque, puis les premiers termes du développement du déterminant $\det(u_0 + u_1\,\mathtt{M}_{x_1} + \cdots + u_n\,\mathtt{M}_{x_n})$ en un point t.

Remarquons que le calcul d'une base de Gröbner pour l'ordre lexicographique nous fournit également une représentation du même type, c'est-à-dire un ensemble de polynômes triangulaire, dont le premier élément dépend d'une variable, et dans les bons cas (projection générique), dont les autres polynômes sont de degré 1 en la nouvelle variable qu'ils font apparaître. Ce calcul se prête également à une arithmétique exacte ou avec des nombres algébriques, mais se révèle souvent plus coûteux que la méthode précédente. Dans le cas où x_1 est séparant (c'est-à-dire $u_0 = -x_1$), nous pouvons passer de la représentation rationnelle à la base de Gröbner, en inversant dans le quotient $\mathcal{A}$ le dénominateur $d_0'(-x_1)$.

Si nous disposons des matrices $\mathtt{M}_{x_i}$ des opérateurs de multiplications par les variables x_i dans une base quelconque, nous avons vu que nous pouvons résoudre le système d'équations $f_1 = \cdots = f_m = 0$ en calculant les vecteurs propres communs à ces matrices. Comparée à la représentation rationnelle, qui nécessite le calcul d'un déterminant, cette méthode sera plus avantageuse (numériquement) si les coefficients des matrices $\mathtt{M}_{x_i}$ sont connus avec une certaine incertitude.

Exemple 3.9.4. — *Reprenons les données de l'exemple 3.2.2. La forme de Chow est*

$$1/36\ (6\,u_0 + 2\,u_1 + 7\,u_2)^2\,(6\,u_0 - 2\,u_1 + 5\,u_2)^2\,.$$

Nous allons appliquer la méthode précédente, même si ici, les coordonnées des racines se lisent directement dans la factorisation de la forme de Chow. Après avoir enlevé les facteurs carrés,

```
d := C/gcd(C,diff(C,u[0]));
```

$$\frac{1}{36}\,(2\,u_1 + 7\,u_2 + 6\,u_0)\,(-2\,u_1 + 5\,u_2 + 6\,u_0)\,.$$

nous calculons les premiers termes du développement de $d(u+t)$ où $t = (0,1,1)$:

```
collect(expand(subs(u[1]=1+u[1],u[2]=1+u[2],d),[u[1],u[2]]));
```

$$\frac{3}{4} + 2\,u_0 + {u_0}^2 - \frac{1}{3}\,u_1 + \left(\frac{11}{6} + 2\,u_0\right)u_2 + \frac{35}{36}\,{u_2}^2 - \frac{1}{9}\,u_1u_2 - \frac{1}{9}\,{u_1}^2.$$

Ce qui nous donne

$$\begin{aligned} d_0(u_0) &= \frac{3}{4} + 2\,u_0 + {u_0}^2 = \frac{1}{4}\,(2\,u_0 + 3)\,(2\,u_0 + 1)\,, \\ d_1(u_0) &= -\frac{1}{3}, \\ d_2(u_0) &= (\frac{11}{6} + 2\,u_0). \end{aligned}$$

Comme $d_0'(u_0) = 2\,(u_0 + 1)$ est sans facteur carré, nous obtenons la représentation rationnelle minimale suivante :

$$\xi_1 = -\frac{1}{6\,(1+u_0)},\ \xi_2 = \frac{11 + 12\,u_0}{12\,(1+u_0)},\ \left(u_0 + \frac{3}{2}\right)\left(u_0 + \frac{1}{2}\right) = 0.$$

Nous vérifions que ces fractions rationnelles évaluées aux racines de $d_0(u_0) = 0$ nous donnent bien les coordonnées des racines de $f_1 = f_2 = 0$.

```
subs(u[0]=-1/2, [xi1,xi2]);subs(u[0]=-3/2, [xi1,xi2]);
```

$$[-\frac{1}{3},\frac{5}{6}]\quad[\frac{1}{3},\frac{7}{6}]$$

3.10. Nombre de racines réelles d'un système polynomial

Le but de cette section est d'étudier la structure réelle du quotient de $\mathbb{R}[\mathbf{x}]$ par des polynômes à coefficients réels. Soient $f_1,\ldots,f_m$ des polynômes de $\mathbb{R}[\mathbf{x}]$ tels que $\mathcal{Z}_{\mathbb{C}}(f_1,\ldots,f_m)=\{\mathbf{x}_1,\ldots,\mathbf{x}_d\}$ soit finie.

Nous allons nous intéresser à l'algèbre quotient réelle $\mathcal{A}_{\mathbb{R}}=\mathbb{R}[\mathbf{x}]/I$. Rappelons que $\mathcal{A}_{\mathbb{C}}=\mathbb{C}[\mathbf{x}]/I=\mathcal{A}_{\mathbb{R}}\otimes\mathbb{C}$ s'obtient à partir de $\mathcal{A}_{\mathbb{R}}$ par extension des scalaires. L'algèbre $\mathcal{A}_{\mathbb{C}}$ est naturellement munie d'une conjugaison, qui laisse fixe les variables $x_1,\ldots,x_n$ et qui conjugue les coefficients des polynômes. Ainsi $\mathcal{A}_{\mathbb{R}}$ est l'ensemble des éléments de $\mathcal{A}_{\mathbb{C}}$, fixes par conjugaison.

Lemme 3.10.1. — *Pour toute racine $\zeta\in\mathcal{Z}_{\mathbb{C}}(I)$, on a $\overline{\mathbf{e}_\zeta}=\mathbf{e}_{\overline{\zeta}}$, $\mathbf{e}_\zeta$ étant l'idempotent associé à ζ.*

Démonstration. Nous vérifions directement que $\overline{\mathbf{e}_\zeta}$ est un idempotent, et qu'il est dans

$$(\mathbf{0}:\overline{Q_\zeta})=(\mathbf{0}:Q_{\overline{\zeta}})=\mathcal{A}_{\overline{\zeta}}$$

où Q_ζ est la composante primaire de I associée à ζ. Par unicité des idempotents (théorème 3.5.2), nous en déduisons que $\overline{\mathbf{e}_\zeta}=\mathbf{e}_{\overline{\zeta}}$. □

Définition 3.10.2. — *Posons $\mathbf{e}_{\zeta,\Re}=(\mathbf{e}_\zeta+\mathbf{e}_{\overline{\zeta}})$, $\mathbf{e}_{\zeta,\Im}=\frac{1}{\mathbf{i}}(\mathbf{e}_\zeta-\mathbf{e}_{\overline{\zeta}})$ et $\mathcal{A}_{\zeta,\mathbb{R}}=\mathbf{e}_{\zeta,\Re}\mathcal{A}_{\mathbb{R}}$.*

Si $\zeta\in\mathbb{R}^n$, $\mathcal{A}_{\zeta,\mathbb{R}}=\mathbf{e}_\zeta\mathcal{A}_{\mathbb{R}}$.

Lemme 3.10.3. — *$\mathcal{A}_{\zeta,\mathbb{R}}$ est une sous-algèbre de $\mathcal{A}_{\mathbb{R}}$ contenant $\mathbf{e}_{\zeta,\Re}$ et $\mathbf{e}_{\zeta,\Im}$.*

Démonstration. Les éléments $\mathbf{e}_{\zeta,\Re}$ et $\mathbf{e}_{\zeta,\Im}$ étant stables par conjugaison, sont dans $\mathcal{A}_{\mathbb{R}}$. Ce qui montre que $\mathcal{A}_{\zeta,\mathbb{R}}\subset\mathcal{A}_{\mathbb{R}}$. Comme $\mathbf{e}_{\zeta,\Im}\in\mathcal{A}_{\mathbb{R}}$ et $\mathbf{e}_{\zeta,\Re}\mathbf{e}_{\zeta,\Im}\equiv\mathbf{e}_{\zeta,\Im}$, $\mathbf{e}_{\zeta,\Im}$ est donc un élément de $\mathcal{A}_{\zeta,\mathbb{R}}$. Par ailleurs, $\mathcal{A}_{\zeta,\mathbb{R}}$ est stable par multiplication interne. C'est donc une sous-algèbre de $\mathcal{A}_{\mathbb{R}}$. □

Pour tout $a\in\mathcal{A}_{\zeta,\mathbb{R}}$, on a $\mathbf{e}_{\zeta,\Re}\,a\equiv a$ car $\mathbf{e}_{\zeta,\Re}^2\equiv\mathbf{e}_{\zeta,\Re}$ si $\zeta=\overline{\zeta}$ et $\mathbf{e}_{\zeta,\Im}^2\equiv-\mathbf{e}_{\zeta,\Re}$ si $\zeta\neq\overline{\zeta}$. L'idempotent $\mathbf{e}_{\zeta,\Re}$ est donc un élément neutre de $\mathcal{A}_{\zeta,\mathbb{R}}$ et $\mathbf{e}_{\zeta,\Im}$ est une racine de $-\mathbf{e}_{\zeta,\Re}$.

Nous noterons $W(I)$ un sous-ensemble de $\mathcal{Z}_{\mathbb{C}}(I)$ contenant un et un seul représentant par classe de conjugaison des racines de $\mathcal{Z}_{\mathbb{C}}(I)$. Si $\zeta\in\mathbb{R}^n$, $\zeta\in W(I)$, et sinon, on choisira un des éléments de $\{\zeta,\overline{\zeta}\}$.

Proposition 3.10.4. — *Pour tout $\zeta\in\mathcal{Z}_{\mathbb{C}}(I)$, l'idéal $\mathcal{A}_{\zeta,\mathbb{R}}=(\mathbf{e}_\zeta+\mathbf{e}_{\overline{\zeta}})\,\mathcal{A}_{\mathbb{R}}$, est une sous-algèbre de $\mathcal{A}_{\mathbb{R}}$. Nous avons la décomposition suivante :*

$$\mathcal{A}_{\mathbb{R}}=\oplus_{\zeta\in W(I)}\,\mathcal{A}_{\zeta,\mathbb{R}}.$$

Démonstration. Comme les éléments de $(\mathbf{e}_\zeta+\mathbf{e}_{\overline{\zeta}})\,\mathcal{A}_{\mathbb{C}}$ fixes par conjugaison sont les éléments de $(\mathbf{e}_\zeta+\mathbf{e}_{\overline{\zeta}})\,\mathcal{A}_{\mathbb{R}}$, la décomposition $\mathcal{A}_{\mathbb{C}}=\oplus_{\zeta\in W(I)}(\mathbf{e}_\zeta+\mathbf{e}_{\overline{\zeta}})\,\mathcal{A}_{\mathbb{C}}$ (voir théorème 3.5.2) implique la décomposition en sous-algèbres réelles suivante :

$$\mathcal{A}_{\mathbb{R}}=\oplus_{\zeta\in W(I)}\,\mathcal{A}_{\zeta,\mathbb{R}},$$

car $\mathcal{A}_{\mathbb{R}}$ est l'ensemble des éléments de $\mathcal{A}_{\mathbb{C}}$ fixes par conjugaison. □

Considérons maintenant la forme linéaire

$$\begin{array}{rcl} Tr : \mathcal{A}_{\mathbb{C}} & \rightarrow & \mathbb{C} \\ a & \mapsto & Tr(a) = tr(M_a), \end{array}$$

où $tr(M_a)$ est la trace de la multiplication par a dans le quotient $\mathcal{A}_{\mathbb{R}}$. Sa restriction à $\mathcal{A}_{\mathbb{R}}$ est une $\mathbb{R}$-forme linéaire à valeur dans $\mathbb{R}$.

Lemme 3.10.5. — *Pour tout $g \in \mathbb{C}[\mathbf{x}]$, $\zeta \in \mathcal{Z}_{\mathbb{C}}(I)$, $Tr(g(\mathbf{x})\,\mathbf{e}_\zeta) = \mu_\zeta\, g(\zeta)$.*

Démonstration. D'après le corollaire 3.7.4, l'élément $(g(x) - g(\zeta))\mathbf{e}_\zeta$ étant nilpotent, on a $Tr((g(x) - g(\zeta))\mathbf{e}_\zeta) = 0$. Par ailleurs, comme $\mathbf{e}_\zeta$ est l'élément unité de l'algèbre $\mathcal{A}_\zeta$, on a $Tr(\mathbf{e}_\zeta) = \dim_{\mathbb{C}}(\mathcal{A}_\zeta) = \mu_\zeta$ où μ_ζ est la multiplicité de ζ. On en déduit donc que

$$Tr(g(x)\mathbf{e}_\zeta) = g(\zeta)Tr(\mathbf{e}_\zeta) + Tr((g(x) - g(\zeta))\mathbf{e}_\zeta) = g(\zeta)\,\mu_\zeta.$$

□

Remarque 3.10.6. — *On a donc en particulier, pour tout $h \in \mathbb{C}[\mathbf{x}]$ et $\alpha \in \mathbb{N}^n$, $Tr(h(x)\,(x-\zeta)^\alpha \mathbf{e}_\zeta) = 0$ si $\alpha \neq 0$ et $Tr(h(x)\,\mathbf{e}_\zeta) = \mu_\zeta\, h(\zeta)$ sinon.*

Pour tout $h \in \mathbb{R}[\mathbf{x}]$, on définit la forme quadratique

$$\begin{array}{rcl} Q_h : \mathcal{A}_{\mathbb{R}} \times \mathcal{A}_{\mathbb{R}} & \rightarrow & \mathbb{R} \\ (a,b) & \mapsto & Tr(hab). \end{array}$$

Nous allons décrire les racines réelles en fonction de cette forme quadratique. Dans le cas d'une variable, ce problème a été étudié par Hermite, Jacobi ([**7**]). Pour le cas de plusieurs variables, voir [**10**], [**5**].

Théorème 3.10.7. — (Hermite) *Soit $h \in \mathbb{R}[\mathbf{x}]$. Le rang de la forme quadratique Q_h est égal au nombre de racines complexes $\mathbf{x}$ telles que $h(\mathbf{x}) \neq 0$.*

La signature de Q_h est le nombre de racines réelles $\mathbf{x}$ telles que $h(\mathbf{x}) > 0$ moins le nombre de racines réelles ξ telles que $h(\xi) < 0$.

Démonstration. Remarquons tout d'abord que si $\mathcal{A}_{\zeta,\mathbb{R}} \neq \mathcal{A}_{\zeta',\mathbb{R}}$, $\mathcal{A}_{\zeta,\mathbb{R}} \cdot \mathcal{A}_{\zeta',\mathbb{R}} \equiv 0$. Ce qui implique que Q_h a une matrice diagonale par blocs, dans une base de $\mathcal{A}_{\mathbb{R}}$ formée d'éléments des sous-algèbres $\mathcal{A}_{\zeta,\mathbb{R}}$. Pour démontrer le théorème, il suffit donc de le faire pour la restriction de Q_h à $\mathcal{A}_{\zeta,\mathbb{R}} \times \mathcal{A}_{\zeta,\mathbb{R}}$. Le rang (resp. la signature) de Q_h sera la somme des rangs (resp. signatures) de ses restrictions.

Pour tout $\zeta \in \mathcal{Z}_{\mathbb{C}}(I)$, il existe une base de $\mathcal{A}_{\zeta,\mathbb{C}}$ de la forme $(x-\zeta)^{\alpha_i}\mathbf{e}_\zeta$, $\alpha_i \in \mathbb{N}^n$, $i = 0, \ldots, \mu_\zeta - 1$ et $\alpha_0 = \mathbf{0}$, (voir la propriété 3.6.1).

Si $\zeta = \overline{\zeta}$, cette base est réelle et est donc aussi une base du $\mathbb{R}$-espace vectoriel $\mathcal{A}_{\zeta,\mathbb{R}}$. D'après le lemme 3.10.5, la matrice de Q_h dans cette base (à savoir $(Tr(h(x)\,(x-\zeta)^{\alpha_i+\alpha_j}\,\mathbf{e}_\zeta))_{0\leq i,j\leq \mu_\zeta - 1}$) est de la forme

$$\begin{pmatrix} \mu_\zeta\, h(\zeta) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

Son rang est donc 1 si $h(\zeta) \neq 0$ et 0 sinon. Sa signature est 1 si $h(\zeta) > 0$, 0 si $h(\zeta) = 0$ et -1 si $h(\zeta) < 0$.

Si $\zeta \neq \overline{\zeta}$, nous déduisons de la base de $\mathcal{A}_{\zeta,\mathbb{C}}$ et de sa conjuguée, la base réelle de $\mathcal{A}_{\zeta,\mathbb{C}} \oplus \mathcal{A}_{\overline{\zeta},\mathbb{C}} = (\mathbf{e}_\zeta + \mathbf{e}_{\overline{\zeta}}\mathcal{A}_{\mathbb{C}}$ suivante :

$$(x-\zeta)^{\alpha_i}\mathbf{e}_\zeta + (x-\overline{\zeta})^{\alpha_i}\mathbf{e}_{\overline{\zeta}},\ \frac{1}{\mathbf{i}}((x-\zeta)^{\alpha_i}\mathbf{e}_\zeta - (x-\overline{\zeta})^{\alpha_i})\mathbf{e}_{\overline{\zeta}},\ i = 0, \ldots, \mu_\zeta - 1.$$

C'est aussi une base du $\mathbb{R}$-espace vectoriel $\mathcal{A}_{\zeta,\mathbb{R}}$. D'après le lemme 3.10.5, la matrice de Q_h dans cette base, est de la forme

$$\begin{pmatrix} \mu_\zeta(h(\zeta)+h(\overline{\zeta})) & \mu_\zeta \frac{1}{\mathbf{i}}(h(\zeta)-h(\overline{\zeta})) & 0 & \cdots & 0 \\ \mu_\zeta \frac{1}{\mathbf{i}}(h(\zeta)-h(\overline{\zeta})) & -\mu_\zeta(h(\zeta)+h(\overline{\zeta})) & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Le rang de Q_h est donc 2 si $h(\zeta) \neq 0$ et 0 sinon. C'est le nombre de racines complexes $\zeta, \overline{\zeta}$ telles que $h(\zeta) \neq 0, h(\overline{\zeta}) \neq 0$. Posons $a = \Re(h(\zeta)), b = \Im(h(\zeta))$. Si $a = 0$ ou $b = 0$, nous vérifions directement que la signature de Q_h est nulle. Sinon, c'est la signature de la forme quadratique

$$a\,x^2 + 2\,b\,x\,y - a\,y^2 = a\,(x + \frac{b}{a}\,y)^2 - \frac{1}{a}(a^2+b^2)\,y^2,$$

c'est-à-dire encore 0.

Ceci nous montre donc que dans $\mathcal{A}$, le rang de Q_h compte le nombre de racines complexes distinctes ζ de $\mathcal{Z}_{\mathbb{C}}(I)$ telles que $h(\zeta) \neq 0$ et que sa signature compte le nombre de racines réelles ζ telles que $h(\zeta) > 0$ moins le nombre de racines réelles ζ telles que $h(\zeta) < 0$. □
En particulier, nous avons le corollaire suivant :

Corollaire 3.10.8. — *Le nombre de racines complexes distinctes est égal au rang de la forme quadratique Q_1. Le nombre de racines réelles est égal à la signature de Q_1.*

Exemple 3.10.9. — *Nous reprenons les données de l'exemple 3.2.2 et calculons les matrices de Q_1 et de*

$$Q_{x_1} = \begin{pmatrix} Tr(x_1) & Tr(x_1^2) & Tr(x_1x_2) & Tr(x_1^2x_2) \\ Tr(x_1^2) & Tr(x_1^3) & Tr(x_1^2x_2) & Tr(x_1^3x_2) \\ Tr(x_1x_2) & Tr(x_1^2x_2) & Tr(x_1x_2^2) & Tr(x_1^2x_2^2) \\ Tr(x_1^2x_2) & Tr(x_1^3x_2) & Tr(x_1^2x_2^2) & Tr(x_1^3x_2^2) \end{pmatrix}$$

Nous allons utiliser directement les matrices de multiplication $\mathtt{M}_{x_1}$ et $\mathtt{M}_{x_2}$ calculées à l'exemple 3.4.4 de la maniére suivante. Comme $Tr(1) = 4$, $Tr(x_1) = tr(\mathtt{M}_{x_1}) = 0$, $Tr(x_2) = tr(\mathtt{M}_{x_2}) = 4, Tr(x_1x_2) = Tr(\mathtt{M}_{x_1}\mathtt{M}_{x_2}) = \frac{2}{9}$, la forme linéaire Tr a pour coordonnées $[4, 0, 4, \frac{2}{9}]$, dans la base duale de la base monomiale $(1, x_1, x_2, x_1\,x_2)$ de $\mathcal{A}$. Les coordonnées de la forme linéaire $x_1 \cdot Tr$, c'est-à-dire $[Tr(x_1), Tr(x_1^2), Tr(x_1x_2), Tr(x_1^2\,x_2)]$, sont donc $\mathtt{M}_{x_1}^t.[4, 0, 4, \frac{2}{9}] = [0, \frac{4}{9}, \frac{2}{9}, \frac{4}{9}]$. Ce vecteur est la première colonne de Q_{x_1}. Nous obtenons de même les autres colonnes de Q_{x_1}, par multiplication d'un tel vecteur par la matrice $\mathtt{M}_{x_1}^t$ ou $\mathtt{M}_{x_2}^t$:

```
T0  := evalm([4,0,4,2/9]):
T1  := evalm(transpose(M1)&*T0):  T2:= evalm(transpose(M2)&*T0):
T11 := evalm(transpose(M1)&*T1): T12:= evalm(transpose(M2)&*T1):
T112:= evalm(transpose(M2)&*T11):
Q1  := matrix(4,4,[T0,T1,T2,T12]);
Qx1 := matrix(4,4,[T1,T11,T12,T112]);
```

$$Q_1 = \begin{pmatrix} 4 & 0 & 4 & \frac{2}{9} \\ 0 & \frac{4}{9} & \frac{2}{9} & \frac{4}{9} \\ 4 & \frac{2}{9} & \frac{37}{9} & \frac{4}{9} \\ \frac{2}{9} & \frac{4}{9} & \frac{4}{9} & \frac{37}{81} \end{pmatrix}, \quad Q_{x_1} = \begin{pmatrix} 0 & \frac{4}{9} & \frac{2}{9} & \frac{4}{9} \\ \frac{4}{9} & 0 & \frac{4}{9} & \frac{2}{81} \\ \frac{2}{9} & \frac{4}{9} & \frac{4}{9} & \frac{37}{81} \\ \frac{4}{9} & \frac{2}{81} & \frac{37}{81} & \frac{4}{81} \end{pmatrix}$$

Le rang et la signature des formes quadratiques Q_1, Q_{x_1} sont

```
rank(Q1), signature(Q1), rank(Qx1), signature(Qx1);
```

$$2, \quad [2,0], \quad 2, \quad [1,1]$$

ce qui confirme qu'il y a deux racines réelles distinctes telles que pour l'une, $x_1 < 0$ *et pour l'autre* $x_1 > 0$.

BIBLIOGRAPHIE

[1] V. Arnold, A. Varchenko, and Goussein-Zadé. *Singularités des applications différentiables.* Edition Mir, Moscou, 1986.

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

[3] T. Becker, V. Weipfenning, and H. Kredel. *Gröbner Bases. A Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics.* Springer-Verlag, Berlin, 1993.

[4] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics. Springer, New York, 1992.

[5] M. Demazure. Charles Hermite, déjà .... Notes informelles de calcul formel 8, Centre de Math., Ecole Polytechnique (France), 1987.

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

[7] C. Hermite. *Sur l'extension du Théorème de M. Sturm à un Système d'Equations Simultanées*, volume 3 of *Oeuvres de C. Hermite.* 1880.

[8] F.S. Macaulay. *The Algebraic Theory of Modular Systems.* Cambridge Univ. Press, 1916.

[9] B. Mourrain. Computing isolated polynomial roots by matrix methods. *J. of Symbolic Computation, Special Issue on Symbolic-Numeric Algebra for Polynomials*, 26(6):715–738, Dec. 1998.

[10] P. S. Pedersen, M.-F. Roy, and A. Szpirglas. Counting Real Zeros in the multivariate Case. In A. Galligo and F. Eyssette, editors, *Effective Methods in Algebraic Geometry (MEGA'92)*, Progress in Math., pages 203–223, Nice (France), 1993. Birkhäuser.

[11] H. J. Stetter. Eigenproblems are at the Heart of Polynomial System Solving. *SIGSAM Bulletin*, 30(4):22–25, 1996.