CHAPITRE 4

ALGÈBRES DE DIMENSION 0

Sommaire

Nous développerons dans ce chapitre l'idée suivante : la résolution d'un système d'équations polynomiales qui engendre un idéal I de $\mathbb{K}[\mathbf{x}]$, se déduit de l'étude de l'algèbre quotient $\mathbb{K}[\mathbf{x}]/I$. L'étude de cette algèbre permet de trouver la géométrie des solutions : compter le nombre de racines du système, les déterminer, analyser leurs multiplicités, ...

4.1. Cas d'une seule variable

En une variable, l'idéal I est engendré par un seul polynôme $f = f_d\, x^d + \cdots + f_0$ de degré d. L'espace vectoriel $\mathcal{A} = \mathbb{K}[x]/(f)$ est de dimension d et de base $(1, x, \ldots, x^{d-1})$. Nous allons supposer que le corps $\mathbb{K}$ est algébriquement clos et que les racines de f sont simples.

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

$$\begin{array}{rccc} M_x : \mathcal{A} & \to & \mathcal{A} \\ a & \mapsto & a\, x. \end{array}$$

Sa matrice dans la base $(1, x, \ldots, x^{d-1})$ 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 aux coordonnées du reste de la la division euclidienne de x^d par f dans la base $(1, x, \ldots, x^{d-1})$. Le polynôme caractéristique de $\mathtt{M}_x$ est $(-1)^d f$. Donc les valeurs propres de M_x sont les racines $\zeta_1, \ldots, \zeta_d$ de f. Ces valeurs propres sont supposées distinctes, la matrice $\mathtt{M}_x$ est alors diagonalisable sur $\mathbb{K}$.

Si p est un élément de $\mathbb{K}[x]$, les valeurs propres de la multiplication par p dans $\mathcal{A}$ sont $p(\zeta_1), \ldots, p(\zeta_d)$ (car la matrice de l'endomorphisme M_p dans la base $(1, x, \ldots, x^{d-1})$ est $\mathtt{M}_p = p(\mathtt{M}_x)$). Les matrices $\mathtt{M}_p, p \in \mathbb{K}[x]$, commutent deux à deux, donc elles sont diagonalisables dans une même base, puisque $\mathtt{M}_x$ est diagonalisable. Nous allons décrire une telle base. Soit

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

le $i^{\text{ème}}$ *polynôme d'interpolation de Lagrange* de f. Les éléments $\mathbf{e}_i(\mathbf{e}_i - 1)$, $(x - \zeta_i)\, \mathbf{e}_i$, $\mathbf{e}_i\, \mathbf{e}_j$ si $j \neq i$, s'annulent aux différentes racines de f. Ils sont donc divisibles par f, et nous avons dans $\mathcal{A}$

$$\mathbf{e}_i^2 \equiv \mathbf{e}_i \quad , \quad x\, \mathbf{e}_i \equiv \zeta_i \mathbf{e}_i \quad , \quad \mathbf{e}_i \mathbf{e}_j \equiv 0 \ \text{ si } \ i \neq j.$$

Comme $\mathbf{e}_1+\cdots+\mathbf{e}_d = 1$ et $x\mathbf{e}_i \equiv \zeta_i\mathbf{e}_i$, $\mathcal{A} \equiv \mathbb{K}\,\mathbf{e}_1 \oplus \cdots \oplus \mathbb{K}\,\mathbf{e}_d$ (en effet, pour tout $p \in \mathbb{K}[\mathbf{x}], p \equiv p(\zeta_1)\mathbf{e}_1 + \cdots + p(\zeta_d)\mathbf{e}_d$). La famille $\mathbf{e} = (\mathbf{e}_1, \ldots, \mathbf{e}_d)$ est une base de $\mathcal{A}$, formée *d'idempotents orthogonaux* (i.e. $\mathbf{e}_i^2 \equiv \mathbf{e}_i,\ \mathbf{e}_i\mathbf{e}_j \equiv 0$ si $i \neq j$). De plus, $\mathbf{e}_i$ est un vecteur propre de M_x associé à la valeur propre ζ_i. La matrice de multiplication par p dans la base $\mathbf{e}$ de $\mathcal{A}$ est

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

La structure de l'algèbre $\mathcal{A} = \mathbb{K}[x]/(f)$, dans le cas d'un polynôme f de degré d n'ayant que des racines simples, se décrit complètement en terme des idempotents $\mathbf{e}_1, \ldots, \mathbf{e}_d$, qui sont en correspondance avec les racines de f.

***Proposition* 4.1.** *Soit $f \in \mathbb{K}[x]$ n'ayant que des racines simples $\zeta_1, \ldots, \zeta_d$. Si $\mathbf{e}_i(x) = \prod_{j=1, j\neq i}^{d} \left(\frac{x-\zeta_j}{\zeta_i-\zeta_j}\right), i = 1, \ldots, d$, alors $\mathbf{e} = (e_1, \ldots, e_d)$ est une base (d'idempotents orthogonaux) de l'espace vectoriel $\mathcal{A} = \mathbb{K}[x]/(f)$. Et pour tout $p \in \mathbb{K}[x]$, l'endomorphisme de multiplication par p dans $\mathcal{A}$ dans la base $\mathbf{e}$ est diagonale et ses valeurs propres sont $p(\zeta_1), \ldots, p(\zeta_d)$.*

Maintenant nous allons nous intéresser au dual $\widehat{\mathcal{A}}$ de $\mathcal{A}$ (i.e. l'espace vectoriel des formes linéaires sur $\mathcal{A}$). C'est un espace vectoriel de dimension d. La base de $\widehat{\mathcal{A}}$ duale de la base $(1, x, \ldots, x^{d-1})$ de $\mathcal{A}$ sera notée $\delta = (\delta^0, \ldots, \delta^{d-1})$. Tout élément Λ de $\widehat{\mathcal{A}}$ se décompose dans cette base sous la forme

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

Si $g \in \mathbb{K}[x]$ et $r = r_0 + \cdots + r_{d-1}\,x^{d-1}$ est le reste de la division euclidienne de g par f, alors

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

Parmi les formes linéaires sur $\mathcal{A}$, les *évaluations* $\mathbf{1}_\zeta : p \mapsto p(\zeta)$ aux différentes racines ζ de f vont jouer un rôle particulier.

Considérons l'application linéaire transposée de M_x

$$\begin{array}{rccc} \widehat{M_x} : & \widehat{\mathcal{A}} & \to & \widehat{\mathcal{A}} \\ & \Lambda & \mapsto & \Lambda \circ M_x. \end{array}$$

La matrice de $\widehat{M_x}$ dans la base δ est la transposée de la matrice de M_x dans la base $(1, x, \ldots, x^{d-1})$ de $\mathcal{A}$.

Comme tout polynôme r de degré au plus $d-1$ s'écrit dans $\mathbf{e}$ sous la forme

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

la base de $\widehat{\mathcal{A}}$ duale de la base $\mathbf{e}$ de $\mathcal{A}$ est $\widehat{\mathbf{e}} = (\mathbf{1}_{\zeta_1}, \ldots, \mathbf{1}_{\zeta_d})$.

De plus, $\mathbf{1}_{\zeta_i}$ est un vecteur propre de $\widehat{M_x}$ associé à la valeur propre ζ_i. En effet, pour tout $a \in \mathcal{A}$,

$$\big(\widehat{M_x}(\mathbf{1}_{\zeta_i})\big)(a) = \mathbf{1}_{\zeta_i}(x\,a) = (\zeta_i \mathbf{1}_{\zeta_i})(a).$$

$\mathbf{1}_{\zeta_i}$ est également un vecteur propre de tous les endomorphismes $\widehat{M_p}$, $p \in \mathcal{A}$, associé à la valeur propre $p(\zeta_i)$.

***Proposition* 4.2.** *Soit $f \in \mathbb{K}[x]$ n'ayant que des racines simples $\zeta_1, \ldots, \zeta_d$. Pour tout $p \in \mathbb{K}[x]$, les valeurs propres du transposé de l'endomorphisme de multiplication par p dans $\mathbb{K}[x]/(f)$ sont $p(\zeta_1), \ldots, p(\zeta_d)$ et elles sont associées respectivement aux vecteurs propres $\mathbf{1}_{\zeta_1}, \ldots, \mathbf{1}_{\zeta_d}$.*

Nous avons ainsi une description complète des opérateurs de multiplication de $\mathcal{A}$ et de leurs transposés. Nous allons voir dans les sections suivantes que cette description se généralise au cas multivariable et avec multiplicité.

4.2. Idéaux 0-dimensionnels de $\mathbb{K}[\mathbf{x}]$

Rappelons qu'un idéal I de $\mathbb{K}[\mathbf{x}]$ définit une variété algébrique affine $\mathcal{Z}(I) = \{a \in \overline{\mathbb{K}}^n : f(a) = 0, \forall f \in I\}$ de dimension 0, si cette variété est un ensemble fini et non vide. Par abus de langage, nous dirons que l'idéal I est de dimension 0 ou 0-*dimensionnel*.

***Théorème* 4.3.** *Les conditions suivantes sont équivalentes pour un idéal propre I (i.e. $I \neq \mathbb{K}[\mathbf{x}]$) :*

i) L'idéal I est 0-dimensionnel.

ii) Pour tout $i \in \{1, \ldots, n\}$, $\mathbb{K}[x_i] \cap I \neq \{0\}$.

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

Démonstration. i) $\Rightarrow$ ii) Fixons $i \in \{1, \ldots, n\}$ et notons $\xi_1, \ldots, \xi_m$ les $i^{\text{èmes}}$ coordonnées des points de $\mathcal{Z}(I)$. Pour tout $j \in \{1, \ldots, m\}$, il existe $g_j \in \mathbb{K}[x_i]$ non nul tel que $g_j(\xi_j) = 0$. Le polynôme $g = g_1 \ldots g_m \in \mathbb{K}[x_i]$ est non nul et s'annule sur $\mathcal{Z}(I)$. D'après le théorème des zéros de Hilbert, il existe $N \in \mathbb{N}$ tel que $g^N \in I \cap \mathbb{K}[x_i]$.

ii) $\Rightarrow$ iii) Pour chaque $i \in \{1, \ldots, n\}$, soit $p_i \in I \cap \mathbb{K}[x_i] \setminus \{0\}$. Il est facile de vérifier que l'espace vectoriel $\mathcal{A}$ est engendré par les monômes $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, avec $0 \leq \alpha_i < \deg p_i$. Ainsi, la dimension de $\mathcal{A}$ est finie.

iii) $\Rightarrow$ i) Posons $D = \dim_{\mathbb{K}} \mathcal{A}$. Pour tout $i \in \{1, \ldots, n\}$, $\{1, x_i, \ldots, {x_i}^D\}$ est une famille liée de $\mathcal{A}$. Il existe alors des scalaires $c_0, \ldots, c_D$ non tous nuls tels que $q_i(x_i) = c_0 + c_1 x_i + \cdots + c_D x_i^D \in I$. Pour chaque $i \in \{1, \ldots, n\}$, les $i^{èmes}$ coordonnées des points de $\mathcal{Z}(I)$ sont solutions de $q_i(x_i)$, donc leur nombre est fini. Par conséquent, la variété $\mathcal{Z}(I)$ est un ensemble fini. □

***Remarque* 4.4.** D'après la proposition 2.24, l'espave vectoriel $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ admet une base monomiale (i.e. constituée de classes modulo I de monômes de $\mathbb{K}[\mathbf{x}]$).

Dorénavant, dans ce chapitre, I désignera un idéal 0-dimensionnel de $\mathbb{K}[\mathbf{x}]$, $\mathcal{A}$ le $\mathbb{K}$-espace vectoriel $\mathbb{K}[\mathbf{x}]/I$, D sa dimension, $(\mathbf{x}^\alpha)_{\alpha\in E}$ (où E est un sous-ensemble de $\mathbb{N}^n$ de cardinal D) une base monomiale de $\mathcal{A}$, $\mathcal{Z}(I)$ la variété algébrique $\{\zeta_1, \ldots, \zeta_d\}$ définie par I. Pour chaque $i \in \{1, \ldots, d\}, \zeta_i = (\zeta_{i,1}, \ldots, \zeta_{i,n}) \in \overline{\mathbb{K}}^n$.

Les monômes de $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$ sont en bijection avec les éléments de $\mathbb{N}^n$. Chaque $\mathbf{x}^\alpha$ est associé au multi-indice α. Pour $n = 2$, la figure suivante représente un exemple de base $(\mathbf{x}^\alpha)_{\alpha\in E}$. Les monômes situés au dessus des points noirs se réduisent, modulo l'idéal I, à des combinaisons linéaires des $\mathbf{x}^\alpha, \alpha \in E$.

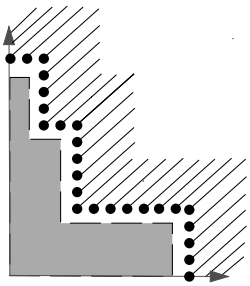

FIGURE 4.1. Base monomiale d'une algèbre quotient.

***Exemple* 4.5.** *Soient $f_1(x_1, x_2) = 13x_1^2 + 8x_1x_2 + 4x_2^2 - 8x_1 - 8x_2 + 2$ et $f_2(x_1, x_2) = x_1^2 + x_1x_2 - x_1 - 1/6$. L'idéal $I = (f_1, f_2)$ est 0-dimensionnel car il est facile de vérifier que l'espace vectoriel $\mathcal{A} = \mathbb{K}[x_1, x_2]/I$ est de dimension 4 et de base $(1, x_1, x_2, x_1x_2)$.*

Nous pouvons vérifier algorithmiquement si un idéal est 0-dimensionnel.

***Proposition* 4.6.** *Soit G une base de Gröbner d'un idéal I pour un ordre monomial quelconque. L'idéal I est 0-dimensionnel si, et seulement si, pour tout $i \in \{1, \ldots, n\}$, il existe $(g_i, m_i) \in G \times \mathbb{N}^*$ tel que $\mathtt{m}(g_i) = x_i^{m_i}$.*

Démonstration. D'après le *iii*) du théorème 4.3 et la proposition 2.24, I est 0-dimensionnel si, et seulement si, $\mathtt{m}(G) = \{\mathtt{m}(g) : g \in G\}$ contient une puissance de chaque variable. □

Le résultat précédent est plus précis pour l'ordre lexicographique.

***Corollaire* 4.7.** *Soit I un idéal 0-dimensionnel. Si G est une base de Gröbner de I pour l'ordre lexicographique $x_1 < \cdots < x_n$, alors il existe des polynômes $g_1, \ldots, g_t$ dans G tels que $g_1 \in \mathbb{K}[x_1], g_2 \in \mathbb{K}[x_1, x_2]$ et $\mathtt{m}(g_2)$ soit une puissance de $x_2, \ldots, g_n \in \mathbb{K}[x_1, \ldots, x_n]$ et $\mathtt{m}(g_n)$ soit une puissance de x_n.*

Démonstration. D'après la proposition 4.6, pour tout $i \in \{1, \ldots, n\}$, il existe $(g_i, m_i) \in G \times \mathbb{N}^*$ tel que $\mathtt{m}(g_i) = x_i^{m_i}$. Comme l'ordre choisi est l'ordre lexicographique $x_1 < \cdots < x_n$, $g_i \in \mathbb{K}[x_1, \ldots, x_i]$. □

***Remarque* 4.8.** Ce corollaire ramène (en théorie) la résolution d'un système d'équations polynomiales ayant un nombre fini de solutions à celle d'un système triangulaire, c'est-à-dire dont certaines équations ne dépendent que de la variable x_1, d'autres que des variables $x_1, x_2, \ldots$ La résolution d'un tel système se fait en résolvant des polynômes d'une variable. Cette approche présente au moins deux inconvénients. Premièrement, le calcul de bases de Gröbner lexicographiques est, en général, coûteux (voir exercice 4.1) et donc peu utilisé en pratique. Pour remédier à ceci dans le cas 0-dimensionnel, on calcul une base de Gröbner pour un ordre moins coûteux et on utilise un procédé de conversion pour avoir une base de Gröbner lexicographique (consulter [**FGLM93**] pour plus de détails). Deuxièmement, la résolution d'un système triangulaire se fait de la manière suivante : on commence par résoudre numériquement $g_1(x_1) = 0$, puis on remplace dans $g_2(x_1, x_2)$ la variable x_1 par les zéros approchés de $g_1(x_1)$ pour obtenir un polynôme d'une variable $\tilde{g}_2(x_2)$ que l'on résout numériquement. Et ainsi de suite. L'accumulation des erreurs dans ce procédé peut fausser complétement le résultat (voir exercice 4.2). Nous verrons, dans les prochaines sections, comment on peut transformer le problème de la résolution polynomiale de manière plus économique, en un problème d'algèbre linéaire : à savoir le calcul de *valeurs et vecteurs propres*.

4.3. Dual de l'algèbre $\mathcal{A}$

Un ingrédient important de l'approche matricielle, qui sera développée dans les sections suivantes, pour la résolution algébrique est la dualité au sens classique. Supposons que le corps $\mathbb{K}$ est algébriquement clos, et rappelons que l'espace vectoriel $\mathcal{A}$ est de dimension finie D et de base $(\mathbf{x}^\alpha)_{\alpha \in E}$. L'espace vectoriel des formes linéaires sur $\mathbb{K}[\mathbf{x}]$ (resp. $\mathcal{A}$) est noté $\widehat{\mathbb{K}[\mathbf{x}]}$ (resp. $\widehat{\mathcal{A}}$). La base de $\widehat{\mathcal{A}}$ duale de la base $(\mathbf{x}^\alpha)_{\alpha \in E}$ de $\mathcal{A}$ est désignée par $(\delta^\alpha)_{\alpha \in E}$. Toute forme linéaire Λ sur $\mathcal{A}$ s'écrit donc sous la forme

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

Le dual $\widehat{\mathcal{A}}$ s'identifie (naturellement) à l'ensemble des éléments de $\widehat{\mathbb{K}[\mathbf{x}]}$ qui s'annulent sur l'idéal I. Pour cela, $\widehat{\mathcal{A}}$ est parfois noté $I^\perp$.

Si $p \in \mathbb{K}[\mathbf{x}]$ et $\alpha \in E$, $\mathbf{d}^\alpha(p)$ est le coefficient du monôme $\mathbf{x}^\alpha$ de la base de $\mathcal{A}$ dans p. Dans le cas où cette base est obtenue à partir d'une base de Gröbner G de I, $\mathbf{d}^\alpha(p)$ est le coefficient de $\mathbf{x}^\alpha$ dans le reste de la division de p par G.

L'espace vectoriel $\widehat{\mathcal{A}}$ peut être muni d'une structure de $\mathcal{A}$-module de la façon suivante : si $(a, \Lambda) \in \mathcal{A} \times \widehat{\mathcal{A}}$,

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

Pour $\zeta \in \mathbb{K}^n$, la forme linéaire

$$\begin{array}{rcl} \mathbf{1}_\zeta : \mathbb{K}[\mathbf{x}] & \to & \mathbb{K} \\ a & \mapsto & a(\zeta) \end{array}$$

est appelée *l'évaluation en* ζ. Si $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathcal{Z}(I)$, $\mathbf{1}_\zeta$ s'annule sur I et définit donc un élément de $\widehat{\mathcal{A}} = I^\perp$. Il s'écrit dans la base $(\mathbf{d}^\alpha)_{\alpha \in E}$ sous la forme

$$\mathbf{1}_\zeta = \sum_{\alpha=(\alpha_1,\ldots,\alpha_n)\in E} \zeta_1^{\alpha_1} \ldots \zeta_n^{\alpha_n}\ \mathbf{d}^\alpha. \tag{4.1}$$

Nous accorderons un intérêt particulier à ces évaluations.

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

Comme I est 0-dimensionnel, d'après l'exercice 4.4, la décomposition primaire minimale de $I = Q_1 \cap \ldots \cap Q_d$, où Q_i est $\mathfrak{m}_{\zeta_i}$-primaire (i.e. Q_i est un idéal primaire et $\sqrt{Q_i} = \mathfrak{m}_{\zeta_i} = (x_1 - \zeta_{i,1}, \ldots, x_n - \zeta_{i,n})\big)$. Désignons par $\mathcal{A}_i$ le *transporteur* de l'idéal Q_i/I dans l'idéal nul $\mathbf{0}$ de $\mathcal{A}$ (i.e. $\mathcal{A}_i = (\mathbf{0} : Q_i/I) = \{a \in \mathcal{A} : qa \equiv 0, \forall q \in Q_i/I\}$). Les idéaux $\mathcal{A}_i$ sont des sous-algèbres de l'algèbre $\mathcal{A}$.

***Théorème* 4.9.** *L'algèbre $\mathcal{A}$ est une somme directe des sous-algèbres $\mathcal{A}_1, \ldots, \mathcal{A}_d$ (i.e. $\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2 \oplus \cdots \oplus \mathcal{A}_d$).*

Nous avons besoin du lemme suivant pour démontrer ce théorème.

***Lemme* 4.10.** *Si J_1, J_2, J sont des idéaux d'un anneau commutatif et unitaire A, alors*

i) $(J : J_1) \cap (J : J_2) = (J : J_1 + J_2)$.

ii) Si de plus J_1 et J_2 sont deux idéaux étrangers (i.e. $J_1 + J_2 = A$), alors $(J : J_1) + (J : J_2) = (J : J_1 \cap J_2)$.

Démonstration. i) Cette égalité est évidente.
ii) Soit $(p_1, p_2) \in J_1 \times J_2$ tel que $1 = p_1 + p_2$. Pour tout $a \in (J : J_1 \cap J_2)$, $a\,p_1 \in (J : J_2)$, $a\,p_2 \in (J : J_1)$. Ainsi, $a = ap_1 + ap_2 \in (J : J_1) + (J : J_2)$, et

$(J : J_1 \cap J_2) \subset (J : J_1) + (J : J_2)$. L'inclusion inverse est immédiate. □

Démonstration. (preuve du théorème 4.9) Si $d = 1, I = Q_1$ est primaire et $\mathcal{A} = \mathcal{A}_1$. Supposons que $d \geq 2$. Pour tout $i \in \{1, \ldots, d\}$ et $L \subset \{1, \ldots, d\} \setminus \{i\}$, $Q_i + \cap_{j \in L} Q_j = \mathbb{K}[\mathbf{x}]$. D'après le lemme 4.10,

$$\mathcal{A}_1 + \cdots + \mathcal{A}_d = (\mathbf{0} : Q_1/I) + \cdots + (\mathbf{0} : Q_d/I) = (\mathbf{0} : Q_1 \cap \ldots \cap Q_d/I) = \mathcal{A}.$$

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

$$\begin{aligned}(\mathcal{A}_1 + \cdots + \mathcal{A}_i) \cap \mathcal{A}_{i+1} &= \big((\mathbf{0} : Q_1/I) + \cdots + (\mathbf{0} : Q_i/I)\big) \cap (\mathbf{0} : Q_{i+1}/I) \\ &= \big(\mathbf{0} : ((Q_1 \cap \ldots \cap Q_i) + Q_{i+1})/I\big) = (\mathbf{0} : \mathcal{A}) = \mathbf{0}.\end{aligned}$$

□

***Remarque* 4.11.** Dans le cas d'une variable, $I = (f) = \big(\prod_{i=1}^{d} (x - \zeta_i)^{\mu_i}\big)$, le théorème 4.9 est une conséquence du théorème des restes chinois :

$$\mathcal{A} = \bigoplus_{i=1}^{d} \mathbb{K}[x]/\big((x - \zeta_i)^{\mu_i}\big).$$

***Définition* 4.12.** *La* multiplicité *de la racine $\zeta_i \in \mathcal{Z}(I)$ est la dimension du sous-espace vectoriel $\mathcal{A}_i$ de $\mathcal{A}$. Elle est notée μ_{ζ_i}(ou μ_i). La racine ζ_i est dite* simple *si $\mu_i = 1$, et* multiple *si $\mu_i > 1$.*

***Théorème* 4.13.** *La dimension de $\mathcal{A}$ est le nombre de racines (chaque racine est comptée autant de fois que sa multiplicité) de I.*

Démonstration. D'après le théorème 4.9, $\dim_{\mathbb{K}} \mathcal{A} = \sum_{i=1}^{d} \mu_i$. □

***Remarque* 4.14.** Le nombre d de racines distinctes de I est inférieur à la dimension D de $\mathcal{A}$. Si toutes ces racines sont simples, $d = D$. Ceci est le cas si, et seulement si, l'idéal I est radical (voir l'exercice 4.7).

4.5. Idempotents de l'algèbre $\mathcal{A}$

D'après le théorème 4.9, il existe un unique $(\mathbf{e}_1, \ldots, \mathbf{e}_d) \in \mathcal{A}_1 \times \cdots \times \mathcal{A}_d$ tel que $1 \equiv \mathbf{e}_1 + \cdots + \mathbf{e}_d$ dans $\mathcal{A}$. Nous avons

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

Comme les $\mathcal{A}_i$ sont des sous-algèbres de $\mathcal{A}$ et $\mathcal{A}_i \cap \mathcal{A}_j = \mathbf{0}$ pour $i \neq j$, nous déduisons que $\mathbf{e}_i^2 \equiv \mathbf{e}_i$ et $\mathbf{e}_i\, \mathbf{e}_j \equiv 0$ pour $i \neq j$. Les $\mathbf{e}_i$ sont donc des *idempotents orthogonaux.*

***Proposition* 4.15.** *La sous-algèbre $\mathcal{A}_i$ de $\mathcal{A}$ coïncide avec $\mathcal{A}\mathbf{e}_i$, et $\mathbf{e}_i$ est son élément neutre.*

Démonstration. Soit $a \in \mathcal{A}_i$. Puisque $\mathcal{A}_i \cap \mathcal{A}_j = \mathbf{0}$ si $i \neq j$, $a \equiv a\,\mathbf{e}_1 + \cdots + a\,\mathbf{e}_d \equiv a\,e_i$. Réciproquement, si $a \in \mathcal{A}$, $a\,\mathbf{e}_i \in \mathcal{A}_i$ (car $\mathcal{A}_i$ est un idéal de $\mathcal{A}$). □

Si $\zeta_j \in \mathcal{Z}(I)$, $\mathbf{e}_i(\zeta_j)$ est défini sans ambiguïté, en posant $\mathbf{e}_i(\zeta_j) = e_i(\zeta_j)$, où e_i est un représentant dans $\mathbb{K}[\mathbf{x}]$ de $\mathbf{e}_i \in \mathcal{A}$.

***Proposition* 4.16.** *Les idempotents $\mathbf{e}_1, \ldots, \mathbf{e}_d$ de $\mathcal{A}$ vérifient*

$$\mathbf{e}_i(\zeta_j) = \begin{cases} 1 & \text{si} \quad i = j \\ 0 & \text{si} \quad i \neq j. \end{cases}$$

Démonstration. Soit $i \in \{1, \ldots, d\}$. Si $d = 1, \mathbf{e}_1 = 1$ et $\mathbf{e}_1(\zeta_1) = 1$. Supposons que $d \geq 2$. Pour chaque $j \neq i$, il existe $q \in Q_i$ tel que $q(\zeta_j) \neq 0$ $\big(\text{car } \mathcal{Z}(Q_i) = \{\zeta_i\} \neq \{\zeta_j\} = \mathcal{Z}(Q_j)\big)$. Comme $\mathbf{e}_i \in \mathcal{A}_i = (\mathbf{0} : Q_i/I), q\,\mathbf{e}_i \equiv 0$, et $\mathbf{e}_i(\zeta_j) = 0$. Ainsi, $1 = \mathbf{e}_1(\zeta_i) + \cdots + \mathbf{e}_d(\zeta_i) = \mathbf{e}_i(\zeta_i)$. □

***Remarque* 4.17.** Si les points de $\mathcal{Z}(I)$ sont simples, alors pour tout $f \in \mathbb{K}[\mathbf{x}]$,

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

Les idempotents $\mathbf{e}_i$ jouent donc un rôle dual des évaluations $\mathbf{1}_{\zeta_i}$, c'est-à-dire celui d'une base pour les polynômes d'interpolations aux racines $\zeta_1, \ldots, \zeta_d$ de l'idéal I.

Nous avons vu, dans la section 4.1, que dans le cas d'une variable et si toutes les racines de I sont simples, les idempotents sont les polynômes d'interpolation de Lagrange.

4.6. Description des sous-algèbres $\mathcal{A}_i$ de $\mathcal{A}$

Considérons l'application linéaire surjective

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

Son noyau permet de calculer la composante $\mathfrak{m}_{\zeta_i}$-primaire Q_i de l'idéal I.

***Proposition* 4.18.** *Le noyau de $M_{\mathbf{e}_i}$ est* $\ker(M_{\mathbf{e}_i}) = Q_i/I$.

Démonstration. L'application $M_{\mathbf{e}_i}$ est la projection de $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_d$ sur $\mathcal{A}_i$, donc

$$\ker(M_{\mathbf{e}_i}) = \oplus_{j \neq i} \mathcal{A}_j = (I : \cap_{j \neq i} Q_j)/I = Q_i/I.$$

□

Il en résulte que $\mathcal{A}_i$ s'identifie à $\mathcal{A}/\ker(M_{\mathbf{e}_i}) = \mathbb{K}[\mathbf{x}]/Q_i$.

***Corollaire* 4.19.** *L'application linéaire*

$$\begin{aligned} \phi_i : \mathbb{K}[\mathbf{x}]/Q_i &\rightarrow \mathcal{A}_i \\ a &\mapsto a\,\mathbf{e}_i \end{aligned}$$

est un isomorphisme d'algèbres.

Nous déduisons de la proposition 4.18, l'algorithme suivant pour construire la composante primaire Q_i de I associée à la racine ζ_i.

***Algorithme* 4.20.** COMPOSANTES PRIMAIRES D'UN IDÉAL 0-DIMENSIONNEL.

ENTRÉE : `Une base de` $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ `et les tables de multiplications.`

1. `Trouver les idempotents` $\mathbf{e}_1, \ldots, \mathbf{e}_d$.
2. `Pour chaque` $i \in \{1, \ldots, d\}$, `déterminer`
   - i) `La matrice de l'application linéaire` $M_{\mathbf{e}_i}$.
   - ii) `Une base` $(p_{i,1}, \ldots, p_{i,D-\mu_i})$ `de` $\ker(M_{\mathbf{e}_i})$.

SORTIE : `L'idéal` $I + (p_{i,1}, \ldots, p_{i,D-\mu_i})$ `est la composante primaire` Q_i `de` I.

Cet algorithme s'appuie sur la connaissance des idempotents. Nous allons voir par la suite comment les obtenir.

***Proposition* 4.21.** *$\mathcal{A}_i$ est un anneau local d'idéal maximal $(\mathfrak{m}_{\zeta_i}/I)\mathbf{e}_i$.*

Démonstration. D'après le corollaire 4.19, il suffit de vérifier que $\mathbb{K}[\mathbf{x}]/Q_i$ est un anneau local d'idéal maximal $\mathfrak{m}_{\zeta_i}/Q_i$. Soit $\mathfrak{m}/Q_i$ un idéal maximal de $\mathbb{K}[\mathbf{x}]/Q_i$. Comme $Q_i \subset \mathfrak{m}$ et $\mathfrak{m}$ est maximal, $\sqrt{Q_i} = \mathfrak{m}_{\zeta_i} \subset \mathfrak{m}$, et donc $\mathfrak{m}_{\zeta_i} = \mathfrak{m}$. □

***Corollaire* 4.22.** *Si $a \in \mathcal{A}$, alors $\big(a - a(\zeta_i)\big)\mathbf{e}_i$ est nilpotent.*

Démonstration. Puisque $a - a(\zeta_i) \in \mathfrak{m}_{\zeta_i}/I$, il existe alors un entier N tel que $\big(a - a(\zeta_i)\big)^N \equiv 0$ dans $\mathbb{K}[\mathbf{x}]/Q_i$. D'après le corollaire 4.19,

$$\phi_i\big(\big(a - a(\zeta_i)\big)^N\big) \equiv \big(a - a(\zeta_i)\big)^N \mathbf{e}_i \equiv \big(\big(a - a(\zeta_i)\big)\mathbf{e}_i\big)^N \equiv 0.$$

□

4.7. Opérateurs de multiplication de $\mathcal{A}$

Soit $a \in \mathcal{A}$. Intéressons-nous à l'opérateur de multiplication par a dans $\mathcal{A}$

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

$\mathtt{M}_a$ désigne sa matrice dans la base $(\mathbf{x}^\alpha)_{\alpha\in E}$. L'endomorphisme transposé de M_a est

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

La matrice de $\widehat{M_a}$ dans la base $(\mathbf{d}^\alpha)_{\alpha\in E}$ est la transposée de $\mathtt{M}_a$. Les opérateurs M_a et $\widehat{M_a}$ ont donc les mêmes valeurs propres.

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

***Théorème* 4.23.** *Soit $\mathcal{Z}(I) = \{\zeta_1, \ldots, \zeta_d\}$ la variété définie par l'idéal I.*

i) Si $a \in \mathbb{K}[\mathbf{x}]$, alors les valeurs propres de M_a (et $\widehat{M_a}$) sont $a(\zeta_1), \ldots, a(\zeta_d)$. En particulier, celles de $M_{x_i}, i = 1, \ldots, n$, sont les $i^{\text{èmes}}$ coordonnées des racines $\zeta_1, \ldots, \zeta_d$.

ii) Si $a \in \mathbb{K}[\mathbf{x}]$, alors les évaluations $\mathbf{1}_{\zeta_1}, \ldots, \mathbf{1}_{\zeta_d}$ sont des vecteurs propres de $\widehat{M_a}$ associés respectivement aux valeurs propres $a(\zeta_1), \ldots, a(\zeta_d)$. De plus, ils sont les seuls (à des scalaires près) vecteurs propres communs à tous les endomorphismes $\widehat{M_a}$, $a \in \mathbb{K}[\mathbf{x}]$.

Démonstration. i) Soit $i \in \{1, \ldots, d\}$. Pour tout $b \in \mathcal{A}$,

$$\big(\widehat{M_a}(\mathbf{1}_{\zeta_i})\big)(b) = \mathbf{1}_{\zeta_i}(a\,b) = \big(a(\zeta_i)\,\mathbf{1}_{\zeta_i}\big)(b).$$

Ceci montre que $a(\zeta_1), \ldots, a(\zeta_d)$ sont des valeurs propres de M_a et $\widehat{M_a}$, les $\mathbf{1}_{\zeta_i}$ sont des vecteurs propres de $\widehat{M_a}$ associés aux valeurs propres $a(\zeta_i)$, et qu'ils sont communs à tous les endomorphismes $\widehat{M_a}$.

Montrons que réciproquement toute valeur propre de M_a est de la forme $a(\zeta_i)$. Pour cela, définissons

$$p(\mathbf{x}) = \prod_{\zeta\in\mathcal{Z}(I)} \big(a(\mathbf{x}) - a(\zeta)\big) \in \mathbb{K}[\mathbf{x}].$$

Ce polynôme s'annule sur $\mathcal{Z}(I)$. D'après le théorème des zéros de Hilbert, il existe $m \in \mathbb{N}$ tel que $p^m \in I$. Si $\mathbb{I}$ désigne l'identité de $\mathcal{A}$, l'opérateur

$$p^m(M_a) = \prod_{\zeta\in\mathcal{Z}(I)} \big(M_a - a(\zeta)\,\mathbb{I}\big)^m$$

est nul, et le polynôme minimal de M_a divise $\prod_{\zeta\in\mathcal{Z}(I)}\big(T-a(\zeta)\big)^m$. Par suite, les valeurs propres de M_a sont de la forme $a(\zeta)$, $\zeta\in\mathcal{Z}(I)$.

ii) Soit $\Lambda\in\widehat{\mathcal{A}}$ un vecteur propre commun à toutes les applications linéaires $\widehat{M}_a$, $a\in\mathbb{K}[\mathbf{x}]$. Si $\gamma=(\gamma_1,\ldots,\gamma_n)\in\mathbb{K}^n$ vérifie $\widehat{M}_{x_i}(\Lambda)=\gamma_i\,\Lambda$, pour $i=1,\ldots,n$, alors tout monôme $\mathbf{x}^\alpha$ satisfait

$$\big(\widehat{M}_{x_i}(\Lambda)\big)(\mathbf{x}^\alpha)=\Lambda(x_i\,\mathbf{x}^\alpha)=\gamma_i\Lambda(\mathbf{x}^\alpha).$$

Il s'en suit que pour tout $\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n$,

$$\Lambda(\mathbf{x}^\alpha)=\gamma_1^{\alpha_1}\ldots\gamma_n^{\alpha_n}\,\Lambda(1)=\Lambda(1)\,\mathbf{1}_\gamma(\mathbf{x}^\alpha)\ ,$$

c'est-à-dire $\Lambda=\Lambda(1)\,\mathbf{1}_\gamma$. Comme $\Lambda\in\widehat{\mathcal{A}}=I^\perp$, $\Lambda(p)=\Lambda(1)p(\gamma)=0$ pour tout $p\in I$. Puisque $\Lambda(1)\neq 0$, $\gamma\in\mathcal{Z}(I)$ et $\mathbf{1}_\gamma\in\widehat{\mathcal{A}}$. □

***Remarque* 4.24.** Si $a\in\mathbb{K}[\mathbf{x}]$, alors l'ensemble de tous les vecteurs propres de M_a est $\cup_{i=1}^d\big(I:a-a(\zeta_i)\big)/I$.

Le théorème 4.23 et l'identité (4.1) permettent de calculer les racines de I (par un seul calcul) si la base choisie $(\mathbf{x}^\alpha)_{\alpha\in E}$ de $\mathcal{A}$ contient $1,x_1,\ldots,x_n$.

***Algorithme* 4.25.** Calcul des racines d'un idéal radical.

Entrée : `Une base` $(\mathbf{x}^\alpha)_{\alpha\in E}$ `de` $\mathcal{A}$ `qui contient` $1,x_1,\ldots,x_n$ `et les tables de multiplication. Soit` a `un élément de` $\mathbb{K}[\mathbf{x}]$ `qui sépare` $\mathcal{Z}(I)$ `(i.e. l'application` $\zeta\in\mathcal{Z}(I)\mapsto a(\zeta)\in\mathbb{K}$ `est injective).`

1. `Déterminer les vecteurs propres` $\Lambda=(\Lambda_0,\Lambda_1,\ldots,\Lambda_n,\ldots)$ `de` $\widehat{M}_a$ `dans la base` $(\mathbf{d}^\alpha)_{\alpha\in E}$ `de` $\widehat{\mathcal{A}}$.
2. `Pour tout vecteur propre` Λ, `calculer` $\zeta=\big(\frac{\Lambda_1}{\Lambda_0},\ldots,\frac{\Lambda_n}{\Lambda_0}\big)$.

Sortie : `Les points` ζ `ainsi obtenus sont les zéros de` I.

***Remarque* 4.26.** Les vecteurs propres Λ dans cet algorithme peuvent se calculer par des méthodes numériques. Pour un aperçu de ces techniques, consulter [**GVL96**].

Si l'idéal I n'est pas radical, cet algorithme produit les zéros simples de I, mais les racines multiples nécessitent, comme nous allons le voir, une triangularisation simultanée de matrices de multiplication.

***Exemple* 4.27.** *Calculons la matrice de multiplication par x_1 dans $\mathcal{A}$ de l'exemple 4.5,*

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

Les matrices de M_{x_1} et M_{x_2} dans la base $(1, x_1, x_2, x_1x_2)$ sont

$$\mathtt{M}_{x_1} = \begin{pmatrix} 0 & \frac{1}{6} & 0 & \frac{5}{54} \\ 1 & 1 & 0 & \frac{55}{54} \\ 0 & 0 & 0 & \frac{2}{27} \\ 0 & -1 & 1 & -1 \end{pmatrix} \quad , \quad \mathtt{M}_{x_2} = \begin{pmatrix} 0 & 0 & -\frac{25}{24} & -\frac{5}{54} \\ 0 & 0 & -\frac{5}{4} & -\frac{55}{54} \\ 1 & 0 & 2 & \frac{5}{54} \\ 0 & 1 & \frac{5}{4} & 2 \end{pmatrix}.$$

Les valeurs propres de l'endomorphisme $\widehat{M_{x_1}}$ sont $-\frac{1}{3}$ et $\frac{1}{3}$, leur multiplicité est 2, leurs sous-espaces propres respectifs sont les droites vectorielles engendrées par $\Lambda_1 = \big(1, -\frac{1}{3}, \frac{5}{6}, -\frac{5}{18}\big)$, $\Lambda_2 = \big(1, \frac{1}{3}, \frac{7}{6}, \frac{7}{18}\big)$.

D'après le théorème 4.23, il existe deux racines ζ_1, ζ_2 communes à f_1, f_2 telles que $x_1(\zeta_1) = \zeta_{1,1}$ (resp. $x_1(\zeta_2) = \zeta_{2,1}$) est une valeur propre associée au vecteur propre $\mathbf{1}_{\zeta_1}$ (resp. $\mathbf{1}_{\zeta_2}$). Donc $\mathbf{1}_{\zeta_1}$ et Λ_1 (resp. $\mathbf{1}_{\zeta_2}$ et Λ_2) sont liés. Comme la base de $\mathcal{A}$ est $(1, x_1, x_2, x_1x_2)$, les solutions du système $f_1 = f_2 = 0$ sont $\zeta_1 = (-\frac{1}{3}, \frac{5}{6})$ et $\zeta_2 = (\frac{1}{3}, \frac{7}{6})$. Les quatrièmes coordonnées des vecteurs Λ_1 et Λ_2 (correspondent à x_1x_2) sont bien le produit des deuxièmes et troisièmes coordonnées.

***Remarque* 4.28.** Lorsque certains sous-espaces propres de $\widehat{M_a}$ sont de dimensions au moins 2, les évaluations $\mathbf{1}_{\zeta_i}$ sont des combinaisons linéaires des vecteurs propres de ces sous-espaces. Il est donc possible de paramétrer ces ζ_i sans pour autant les expliciter : si la dimension du sous-espace propre associé à une valeur propre $a(\zeta)$ est $m \geq 2$, et $(\Lambda_1, \ldots, \Lambda_m)$ est une base de celui-ci, d'après le théorème 4.23, il existe $(c_1, \ldots, c_m) \in \mathbb{K}^m$ tel que $\mathbf{1}_\zeta = c_1\Lambda_1 + \cdots + c_m\Lambda_m$. Ainsi, $(\zeta^\alpha)_{\alpha\in E} = c_1(\Lambda_{1,\alpha})_{\alpha\in E} + \cdots + c_m(\Lambda_{m,\alpha})_{\alpha\in E}$, où $(\Lambda_{i,\alpha})_{\alpha\in E}$ sont les coordonnées du vecteur propre Λ_i dans la base duale $(\mathbf{d}^\alpha)_{\alpha\in E}$ de la base $(\mathbf{x}^\alpha)_{\alpha\in E}$ de $\mathcal{A}$. Pour expliciter les zéros de I, nous utiliserons le fait que les matrices $\mathtt{M}_{x_1}, \ldots, \mathtt{M}_{x_n}$ commutent.

***Proposition* 4.29.** *Il existe une base de $\mathcal{A}$ dans laquelle les matrices $\mathtt{T}_j$ des opérateurs M_{x_j} sont triangulaires. Et si $t^j_{i,i}$ désigne le $i^{ème}$ élément de la diagonale de $\mathtt{T}_j$, alors $\mathcal{Z}(I) = \{\mathtt{t}_i := (t^1_{i,i}, \ldots, t^n_{i,i}), i = 1, \ldots, D\}$.*

Démonstration. Puisque $M_{x_1}, \ldots, M_{x_n}$ commutent, ils se triangularisent dans une même base en $\mathtt{T}_1, \ldots, \mathtt{T}_n$. Pour tout $p \in I$, la matrice de multiplication

par p dans $\mathcal{A}$ est $\mathtt{M}_p = p(\mathtt{M}_{x_1}, \ldots, \mathtt{M}_{x_n}) = \mathbf{0}$. Donc $p(\mathtt{T}_1, \ldots, \mathtt{T}_n) = \mathbf{0}$, et le $i^{ème}$ élément $p(\mathtt{t}_i)$ de la diagonale de la matrice $p(\mathtt{T}_1, \ldots, \mathtt{T}_n)$ est nul. Par suite $t_i \in \mathcal{Z}(I)$, pour $i = 1, \ldots, D$.

Montrons que réciproquement tout élément de $\mathcal{Z}(I)$ est un point $\mathtt{t}_i$. Soit $l = \sum_{i=1}^n \lambda_i x_i$ une forme linéaire qui sépare $\mathcal{Z}(I)$. Les valeurs propres de M_l sont les termes diagonaux de la matrice $\sum_{j=1}^n \lambda_j \mathtt{T}_j$, c'est-à-dire $l(\mathtt{t}_i)$, $i = 1, \ldots, D$. Soit ζ un zéro de I. D'après le théorème 4.23, il existe $i_0 \in \{1, \ldots, D\}$ tel que $l(\zeta) = l(\mathtt{t}_{i_0})$. Comme $\mathtt{t}_{i_0} \in \mathcal{Z}(I)$ et l sépare $\mathcal{Z}(I)$, $\zeta = \mathtt{t}_{i_0}$. □

La proposition 4.29 permet de résoudre les systèmes polynomiaux.

***Algorithme* 4.30.** CALCUL DES RACINES PAR TRIANGULATION SIMULTANÉE.

ENTRÉE : Les matrices $\mathtt{M}_{x_i}$ des opérateurs de multiplication par les variables x_i pour $i = 1, \ldots, n$ dans une base de $\mathcal{A}$.

1. Déterminer une décomposition de Schur de $\mathtt{M}_{x_1}$ (i.e. trouver une matrice unitaire P telle que $\mathtt{T}_1 = \mathtt{P}\mathtt{M}_{x_1}\mathtt{P}^{-1}$ soit triangulaire).
2. Calculer les matrices triangulaires $\mathtt{T}_i = \mathtt{P}\mathtt{M}_{x_i}\mathtt{P}^{-1}$, $i = 2, \ldots, n$.

SORTIE : Si $t_{i,i}^j$ désigne le $i^{ème}$ élément de la diagonale de $\mathtt{T}_j$, alors

$$\mathcal{Z}(I) = \{(t_{i,i}^1, \ldots, t_{i,i}^n), i = 1, \ldots, D\}.$$

4.8. Décomposition des opérateurs de multiplication de $\mathcal{A}$

Comme les sous-algèbres $\mathcal{A}_i$ de $\mathcal{A}$ sont stables par multiplication par les éléments de $\mathcal{A}$, et $\mathcal{A}_i\mathcal{A}_j \equiv 0$ si $i \neq j$, les matrices des opérateurs M_a, $a \in \mathcal{A}$, se décomposent en blocs dans une base de $\mathcal{A}$ adaptée à la décomposition $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_d$.

***Théorème* 4.31.** *Il existe une base de $\mathcal{A}$ dans laquelle tout endomorphisme M_a se décompose sous la forme*

$$\begin{pmatrix} \mathtt{N}_a^1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \mathtt{N}_a^d \end{pmatrix}, \quad \text{avec} \quad \mathtt{N}_a^i = \begin{pmatrix} a(\zeta_i) & \ldots & \star \\ & \ddots & \vdots \\ \mathbf{0} & & a(\zeta_i) \end{pmatrix}, \ i = 1, \ldots, d.$$

Le bloc $\mathtt{N}_a^i$ correspond à la sous-algèbre $\mathcal{A}_i$.

Démonstration. Pour chaque $i \in \{1, \ldots, d\}$, les opérateurs de multiplication dans $\mathcal{A}_i$ par les éléments de $\mathcal{A}$ commutent. Donc il est possible de choisir une

base de $\mathcal{A}_i$ pour que les matrices de multiplication $\mathtt{N}_a^i$ par $a \in \mathcal{A}$, dans $\mathcal{A}_i$, dans cette base soient triangulaires supérieures. D'après le corollaire 4.19 et le théorème 4.23, la seule valeur propre de $\mathtt{N}_a^i$ est $a(\zeta_i)$. □

Nous déduisons le résultat suivant :

***Corollaire* 4.32.** *Si μ_ζ est la multiplicité de la racine $\zeta \in \mathcal{Z}(I)$, alors pour tout $a \in \mathcal{A}$, nous avons*

i) la trace de l'endomorphisme M_a est $\mathrm{tr}(M_a) = \sum_{\zeta\in\mathcal{Z}(I)} \mu_\zeta a(\zeta)$,

ii) le déterminant de l'endomorphisme M_a est $\det(M_a) = \prod_{\zeta\in\mathcal{Z}(I)} a(\zeta)^{\mu_\zeta}$.

***Remarque* 4.33.** Sur la diagonale de $\mathtt{N}_a^i$ du théorème 4.31, $a(\zeta_i)$ apparaît autant de fois que la multiplicité de ζ_i. Cependant si $a(\zeta_i) = a(\zeta_j)$ pour $i \neq j$, la multiplicité de la valeur propre $a(\zeta_i)$ de la multiplication par a dans $\mathcal{A}$ est plus grande que μ_{ζ_i}.

4.9. Forme de Chow de l'idéal I

Le théorème de structure 4.31 permet de définir la *forme de Chow* de I.

***Définition* 4.34.** *La* forme de Chow *de l'idéal I est le polynôme homogène de $\mathbb{K}[\mathbf{u}] = \mathbb{K}[u_0, \ldots, u_n]$ défini par*

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

μ_ζ désigne la multiplicité de $\zeta = (\zeta_1, \ldots, \zeta_n)$.

***Proposition* 4.35.** *La forme de Chow de I est le déterminant de la matrice $u_0\mathbb{I} + u_1\mathtt{M}_{x_1} + \cdots + u_n\mathtt{M}_{x_n}$, où $\mathbb{I}$ désigne la matrice identité et $\mathtt{M}_{x_i}$ la matrice de multiplication par x_i dans $\mathcal{A}$ (dans une base quelconque de $\mathcal{A}$).*

Démonstration. D'après le théorème 4.31, pour tout $(u_0, \ldots, u_n) \in \mathbb{K}^{n+1}$,

$$\begin{aligned} \det(u_0\mathbb{I} + u_1\mathtt{M}_{x_1} + \cdots + u_n\mathtt{M}_{x_n}) &= \det(\mathtt{M}_{u_0+u_1 x_1+\cdots+u_n x_n}) \\ &= \prod_{\zeta\in\mathcal{Z}(I)} (u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n)^{\mu_\zeta}. \end{aligned}$$

□

***Remarque* 4.36.** Il est donc possible de déterminer la forme de Chow en calculant les matrices des opérateurs $M_{x_1}, \ldots, M_{x_n}$, à l'aide par exemple d'une base de Gröbner de I. Et si nous utilisons un algorithme de factorisation pour décomposer le polynôme $\det(u_0\mathbb{I} + u_1\mathtt{M}_{x_1} + \cdots + u_n\mathtt{M}_{x_n}) \in \mathbb{K}[\mathbf{u}]$ en facteurs linéaires (voir [**CM93, CG05**]), les coefficients de ces facteurs permettent de déterminer les racines de I.

La partie sans facteur carré de $\mathcal{C}_I(\mathbf{u})$ est

$$\tilde{\mathcal{C}}_I(\mathbf{u}) = \frac{\mathcal{C}_I(\mathbf{u})}{\operatorname{pgcd}\big(\mathcal{C}_I(\mathbf{u}), \frac{\partial \mathcal{C}_I}{\partial u_0}(\mathbf{u})\big)} = \prod_{\zeta \in \mathcal{Z}(I)} (u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n) \in \mathbb{K}[\mathbf{u}].$$

Elle est appelée *la forme de Chow réduite* de I.

4.10. Représentation univariée rationnelle

La représentation univariée rationnelle est la description des solutions d'un système polynomial multivariable et 0-dimensionnel $f_1 = \cdots = f_m = 0$ à l'aide des zéros d'un polynôme en une variable et d'une application rationnelle. Nous utiliserons, pour cela, la forme de Chow de $I = (f_1, \ldots, f_m)$.

***Théorème* 4.37.** *Soit $\Delta(\mathbf{u})$ un multiple de la forme de Chow réduite $\tilde{\mathcal{C}}_I(\mathbf{u})$. Pour $t = (t_1, \ldots, t_n) \in \mathbb{K}^n$ générique, nous écrivons*

$$\frac{\Delta}{\operatorname{pgcd}\big(\Delta, \frac{\partial \Delta}{\partial u_0}\big)}\big((0, t) + \mathbf{u}\big) = d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0) + r(\mathbf{u}),$$

avec $d_0(u_0), \ldots, d_n(u_0) \in \mathbb{K}[u_0]$, $\operatorname{pgcd}\big(d_0(u_0), {d_0}'(u_0)\big) = 1$, et le polynôme $r(\mathbf{u})$ appartient à l'idéal $(u_1, \ldots, u_n)^2$ de $\mathbb{K}[\mathbf{u}] = \mathbb{K}[u_0, \ldots, u_n]$. Alors pour tout $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathcal{Z}(I)$, il existe une racine ζ_0 de $d_0(u_0)$ telle que

$${d_0}'(\zeta_0)\ \zeta_i - d_i(\zeta_0) = 0\ , \quad i = 1, \ldots, n.$$

***Remarque* 4.38.** La proposition 4.35 donne un moyen pour calculer la forme de Chow en utilisant les opérateurs de multiplication. Nous verrons, dans les sections 6.4 et 10.3, comment obtenir un multiple de la forme de Chow en utilisant les matrices des résultants ou les bézoutiens.

Le théorème 4.37 décrit les éléments de $\mathcal{Z}(I)$, comme les valeurs des points $\big(\frac{d_1(u_0)}{{d_0}'(u_0)}, \ldots, \frac{d_n(u_0)}{{d_0}'(u_0)}\big)$ en certaines racines de $d_0(u_0)$. Cette approche remonte à Macaulay, qui l'a utilisée pour déterminer une décomposition primaire d'un idéal (voir la note en bas de la page 88 de [**Mac16**]). Elle a été utilisé par la suite par plusieurs auteurs (voir [**ABRW96, Rou96, Rou99**]). Sur l'extension de cette méthode au cas non 0-dimensionnel, voir sous-secion 10.3.4 ou consulter [**EM99a**].

Pour montrer le théorème 4.37, nous avons besoin du lemme suivant :

***Lemme* 4.39.** *Soient $A(\mathbf{u})$ et $B(\mathbf{u})$ deux polynômes de $\mathbb{K}[\mathbf{u}]$ premiers entre eux. Pour $t = (t_1, \ldots, t_n) \in \mathbb{K}^n$ générique, $A_0(u_0) = A(u_0, t_1, \ldots, t_n)$ et $B_0(u_0) = B(u_0, t_1, \ldots, t_n)$ sont premiers entre eux dans $\mathbb{K}[u_0]$.*

Démonstration. Si l'un des deux polynômes ne dépend pas de u_0, alors le lemme est vrai pour tout $t \in \mathbb{K}^n$. Sinon $A(\mathbf{u})$ et $B(\mathbf{u})$ sont premiers entre eux dans $(\mathbb{K}[u_1, \ldots, u_n])[u_0]$. Il existe alors $\delta \in \mathbb{K}[u_1, \ldots, u_n]$ non nul, $F \in$

$\mathbb{K}[\mathbf{u}]$, $G \in \mathbb{K}[\mathbf{u}]$ tels que $F(\mathbf{u})A(\mathbf{u}) + G(\mathbf{u})B(\mathbf{u}) = \delta(u_1, \ldots, u_n)$. Pour tout $t \in \mathbb{K}^n$ vérifiant $\delta(t_1, \ldots, t_n) \neq 0, A_0(u_0)$ et $B_0(u_0)$ sont premiers entre eux. □

Démonstration. (preuve du théorème 4.37) Décomposons $\Delta(\mathbf{u})$ sous la forme

$$\Delta(\mathbf{u}) = \Big(\prod_{\zeta=(\zeta_1,\ldots,\zeta_n)\in\mathcal{Z}(I)} (u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n)^{n_\zeta} \Big) H(\mathbf{u}) \ ,$$

avec $n_\zeta \in \mathbb{N}^*, \prod_{\zeta\in\mathcal{Z}(I)}(u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n)^{n_\zeta}$ et $H(\mathbf{u})$ premiers entre eux. Posons

$$d(\mathbf{u}) = \frac{\Delta(\mathbf{u})}{\operatorname{pgcd}\big(\Delta(\mathbf{u}), \frac{\partial\Delta}{\partial u_0}(\mathbf{u})\big)} = \Big(\prod_{\zeta\in\mathcal{Z}(I)} (u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n) \Big) h(\mathbf{u}) \ ,$$

où $\prod_{\zeta\in\mathcal{Z}(I)}(u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n)$ et $h(\mathbf{u})$ sont premiers entre eux. Soit $t = (t_1, \ldots, t_n) \in \mathbb{K}^n$, et notons $\mathtt{t} = (0, t_1, \ldots, t_n) \in \mathbb{K}^{n+1}$. Nous avons

$$\begin{aligned} d(\mathtt{t} + \mathbf{u}) &= \Big(\prod_{\zeta\in\mathcal{Z}(I)} \big(\langle t, \zeta\rangle + u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n\big) \Big) h(\mathtt{t} + \mathbf{u}) \\ &= d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0) + r(\mathbf{u}) \ , \end{aligned}$$

avec $\langle t, \zeta\rangle = t_1\zeta_1 + \cdots + t_n\zeta_n$, $d_0, \ldots, d_n \in \mathbb{K}[u_0]$, et $r(\mathbf{u}) \in (u_1, \ldots, u_n)^2$. Développons $h(\mathtt{t} + \mathbf{u})$ sous la forme

$$h(\mathtt{t} + \mathbf{u}) = h_0(u_0) + u_1 h_1(u_0) + \cdots + u_n h_n(u_0) + s(\mathbf{u}) \ ,$$

où $h_0, \ldots, h_n \in \mathbb{K}[u_0]$ et $s(\mathbf{u}) \in (u_1, \ldots, u_n)^2$. Par identification

$$\begin{aligned} d_0(u_0) &= \Big(\prod_{\zeta\in\mathcal{Z}(I)} \big(\langle t, \zeta\rangle + u_0\big) \Big) h_0(u_0) \quad , \quad \text{et pour } i = 1, \ldots, n \ , \\ d_i(u_0) &= \Big(\sum_{\zeta\in\mathcal{Z}(I)} \zeta_i \prod_{\xi\neq\zeta} \big(\langle t, \xi\rangle + u_0\big) \Big) h_0(u_0) + \Big(\prod_{\zeta\in\mathcal{Z}(I)} \big(\langle t, \zeta\rangle + u_0\big) \Big) h_i(u_0). \end{aligned}$$

Ainsi,

$$d_0{}'(u_0) = \Big(\sum_{\zeta\in\mathcal{Z}(I)} \prod_{\xi\neq\zeta} \big(\langle t, \xi\rangle + u_0\big) \Big) h_0(u_0) + \Big(\prod_{\zeta\in\mathcal{Z}(I)} \big(\langle t, \zeta\rangle + u_0\big) \Big) h_0{}'(u_0).$$

D'après le lemme 4.39, si $t \in \mathbb{K}^n$ est générique, les polynômes $h_0(u_0)$ et $\prod_{\zeta\in\mathcal{Z}(I)} \big(\langle t, \zeta\rangle + u_0\big)$ sont premiers entre eux. Si $\zeta_0 = -\langle t, \zeta\rangle$ est une racine de

$d_0(u_0)$, alors $h_0(\zeta_0) \neq 0$, et

$$\begin{aligned} d_0{}'(\zeta_0) &= \Big(\prod_{\xi\neq\zeta}\big(\langle t,\xi\rangle - \langle t,\zeta\rangle\big)\Big)h_0(\zeta_0)\ , \\ d_i(\zeta_0) &= \zeta_i\Big(\prod_{\xi\neq\zeta}\big(\langle t,\xi\rangle - \langle t,\zeta\rangle\big)\Big)h_0(\zeta_0)\ , \text{ pour } \ i=1,\ldots,n. \end{aligned}$$

Supposons, de plus, que le vecteur générique t sépare $\mathcal{Z}(I)$. Alors

$$\zeta_i = \frac{d_i(\zeta_0)}{d_0{}'(\zeta_0)} \ \text{ pour } i=1,\ldots,n.$$

□

La représentation de $\mathcal{Z}(I)$ donnée par le théorème 4.37 n'est pas minimale, car les racines de $d_0(u_0)$ ne définissent pas toutes nécessairement des zéros de I. Nous venons de démontrer que la variété $\mathcal{Z}(I)$ est décrite seulement par les racines de $d_0(u_0)$ qui n'annulent pas $h_0(u_0)$.

Nous déduisons de ce qui précede l'algorithme suivant :

***Algorithme* 4.40.** Représentation univariée rationnelle (minimale) des racines de l'idéal 0-dimensionnel $I=(f_1,\ldots,f_m)$.

Entrée : `Un mutltiple de la forme de Chow réduite` $\Delta(\mathbf{u})$ `de` I.

1. `Calculer` $d(\mathbf{u}) = \frac{\Delta(\mathbf{u})}{\operatorname{pgcd}\left(\Delta(\mathbf{u}),\frac{\partial\Delta}{\partial u_0}(\mathbf{u})\right)}$.
2. `Choisir` $t \in \mathbb{K}^n$ `générique (i.e. tel que le polynôme` $d_0(u_0)$ `ci-dessus soit sans facteur carré) et développer` $d(\mathtt{t}+\mathbf{u})$ `sous la forme`
$$d(\mathtt{t}+\mathbf{u}) = d_0(u_0) + u_1 d_1(u_0) + \cdots + u_n d_n(u_0) + \cdots$$
3. `Décomposer` $d_0(u_0)$`, puis garder ses facteurs irréductibles` $p_1,\ldots,p_s$ `qui divisent les numérateurs des fractions rationnelles`
$$f_i\left(\frac{d_1(u_0)}{d_0{}'(u_0)},\ldots,\frac{d_n(u_0)}{d_0{}'(u_0)}\right)\ ,\ i=1,\ldots,m.$$

Sortie : `La représentation minimale de` $\mathcal{Z}(I)$ `est donnée par`

$$(p_1\ldots p_s)(u_0)=0 \quad , \quad \left(\frac{d_1(u_0)}{d_0{}'(u_0)}\ ,\ldots\ ,\ \frac{d_n(u_0)}{d_0{}'(u_0)}\right).$$

Dans le cas où le polynôme $\Delta(\mathbf{u})$ est exactement la forme de Chow $\mathcal{C}_I(\mathbf{u})$, nous avons la proposition suivante :

***Proposition* 4.41.** *Avec les notations du théorème 4.37, si $\Delta(\mathbf{u}) = \mathcal{C}_I(\mathbf{u})$ et t sépare $\mathcal{Z}(I)$, alors il y a une bijection entre les racines de $d_0(u_0)$ et $\mathcal{Z}(I)$.*

Démonstration. Voir l'exercice 4.13. □

***Remarque* 4.42.** L'algorithme précédent fournit une autre méthode pour résoudre le système $f_1 = \cdots = f_m = 0$, en résolvant une équation d'une variable, puis en reportant ses solutions dans des fractions rationnelles. Cette approche se prête bien à des calculs exacts et sur des nombres algébriques. Elle peut être utilisée dès que l'on dispose d'une base de $\mathcal{A}$, par exemple via une base de Gröbner. Il suffit alors de calculer les matrices de multiplication $\mathtt{M}_{x_i}$, pour $i = 1, \ldots, n$, puis les premiers termes du développement de la partie sans facteur carré de $\mathcal{C}_I(\mathtt{t} + \mathbf{u})$. Une alternative aux bases de Gröbner pour déterminer un multiple de la forme de Chow de I est l'utilisation des résultants ou des bézoutiens (voir sections 6.4 et 10.3).

Une base de Gröbner lexicographique fournit également une représentation rationnelle de la variété $\mathcal{Z}(f_1, \ldots, f_m)$ (voir exercice 4.15). Cette approche se prête également à une arithmétique exacte ou avec des nombres algébriques, mais se révèle souvent plus coûteuse que la méthode précédente. Pour avoir plus de détails sur ces deux représentations, consulter [**Rou96**].

Nous avons vu comment résoudre le système $f_1 = \ldots = f_m = 0$ en calculant les vecteurs propres des matrices $\mathtt{M}_{x_i}$. Comparée à la représentation rationnelle qui nécessite le calcul d'un déterminant, la méthode des vecteurs propres est plus avantageuse (numériquement) si les coefficients des $\mathtt{M}_{x_i}$ ne sont connus qu'avec une certaine incertitude.

***Exemple* 4.43.** *Reprenons l'exemple 4.5. La forme de Chow de (f_1, f_2) est*

$$\begin{aligned} C &= \det(u_0\mathbb{I} + u_1\mathtt{M}_1 + u_2\mathtt{M}_2) \\ &= -\frac{2}{9}u_0^2u_2u_1 + u_0^4 + \frac{1}{81}u_1^4 + \frac{1225}{1296}u_2^4 + \frac{35}{9}u_0u_2^3 + \frac{2}{81}u_2u_1^3 - \frac{11}{54}u_1^2u_2^2 \\ &\quad -\frac{35}{162}u_1u_2^3 - \frac{4}{9}u_0u_2u_1^2 - \frac{4}{9}u_0u_1u_2^2 + 4u_0^3u_2 + \frac{107}{18}u_0^2u_2^2 - \frac{2}{9}u_0^2u_1^2. \end{aligned}$$

la factoriLe polynôme d est

$$d(u_0, u_1, u_2) = \frac{1225}{1296}u_2^2 + \frac{35}{18}u_0u_2 + \frac{35}{36}u_0^2 - \frac{35}{324}u_2u_1 - \frac{35}{324}u_1^2.$$

Pour $t = (0, 1)$ (qui est ici générique), $d\big((0, 0, 1) + (u_0, u_1, u_2)\big) =$

$$\frac{35}{48} + \frac{35}{18}u_0 + \frac{35}{36}u_0^2 - \frac{35}{108}u_1 + \left(\frac{385}{216} + \frac{35}{18}u_0\right)u_2 - \frac{35}{324}u_1u_2 - \frac{35}{324}u_1^2 + \frac{1225}{1296}u_2^2.$$

Ainsi,

$$\begin{aligned} d_0(u_0) &= \frac{35}{48} + \frac{35}{18}u_0 + \frac{35}{36}u_0^2 = \frac{35}{36}\Big(u_0 + \frac{1}{2}\Big)\Big(u_0 + \frac{3}{2}\Big), \\ d_1(u_0) &= -\frac{35}{108}, \\ d_2(u_0) &= \frac{385}{216} + \frac{35}{18}u_0. \end{aligned}$$

D'après la proposition 4.41, la représentation rationnelle minimale de $\mathcal{Z}(f_1, f_2)$ est donnée par

$$\Big(u_0 + \frac{1}{2}\Big)\Big(u_0 + \frac{3}{2}\Big) = 0, \quad \Big(-\frac{1}{6\,(1+u_0)}\,, \frac{11 + 12\,u_0}{12\,(1+u_0)}\Big).$$

Donc les solutions du système $f_1 = f_2 = 0$ sont $(-\frac{1}{3}, \frac{5}{6}), (\frac{1}{3}, \frac{7}{6})$.

4.11. Nombre de racines réelles

Dans des domaines, tels que la robotique, la vision, la chimie, la biologie, les statistiques ... la modélisation de certains problèmes conduit à des systèmes polynomiaux à coefficients réels. Pour ces questions, seules les solutions réelles ont une interprétation physique. C'est pour cela que nous allons nous intéresser à la résolution algébrique réelle.

Soient $f_1, \ldots, f_m$ des éléments de $\mathbb{R}[\mathbf{x}]$. Supposons que la variété complexe $\mathcal{Z}_\mathbb{C} = \{\zeta \in \mathbb{C}^n : f_1(\zeta) = \cdots = f_m(\zeta) = 0\} = \{\zeta_1, \ldots, \zeta_d\}$ soit finie. Le but de cette section est l'étude de la structure de l'algèbre réelle $\mathcal{A}_\mathbb{R} = \mathbb{R}[\mathbf{x}]/I$, où I (resp. J) désigne l'idéal de $\mathbb{R}[\mathbf{x}]$ (resp. $\mathbb{C}[\mathbf{x}]$) engendré par $f_1, \ldots, f_m$.

L'algèbre complexe $\mathcal{A}_\mathbb{C} = \mathbb{C}[\mathbf{x}]/J = \mathcal{A}_\mathbb{R} \otimes_\mathbb{R} \mathbb{C}$ est munie (naturellement) d'une conjugaison, qui fixe les variables $x_1, \ldots, x_n$ et conjugue les coefficients complexes des polynômes. Ainsi, $\mathcal{A}_\mathbb{R}$ devient l'ensemble des éléments fixes de $\mathcal{A}_\mathbb{C}$ par cette conjugaison. Le conjugué d'un élément $a \in \mathcal{A}$ est noté $\overline{a}$.

Soient $\zeta_1, \overline{\zeta}_1, \ldots, \zeta_s, \overline{\zeta}_s$ les racines complexes non réelles de $f_1 = \cdots = f_m = 0$, et $\zeta_{2s+1}, \ldots, \zeta_d$ ses racines réelles.

***Lemme* 4.44.** *Si $\zeta \in \mathcal{Z}_\mathbb{C}$ et $\mathbf{e}_\zeta$ désigne l'idempotent associé à ζ, alors $\overline{\mathbf{e}}_\zeta = \mathbf{e}_{\overline{\zeta}}$.*

Démonstration. Il est facile de vérifier que $\overline{\mathcal{A}}_\zeta = \mathcal{A}_{\overline{\zeta}}$, et par suite $\overline{\mathbf{e}}_\zeta \in \mathcal{A}_{\overline{\zeta}}$. D'après le théorème 4.9, la décomposition $1 = \mathbf{e}_{\zeta_1} + \cdots + \mathbf{e}_{\zeta_d}$, avec $\mathbf{e}_{\zeta_i} \in \mathcal{A}_{\zeta_i}$, est unique, donc $\overline{\mathbf{e}}_\zeta = \mathbf{e}_{\overline{\zeta}}$. □

Soit $\zeta \in \mathcal{Z}_\mathbb{C}$. Introduisons les notations suivantes :

$$\mathbf{e}_{\zeta,\Re} = \mathbf{e}_\zeta + \mathbf{e}_{\overline{\zeta}} \;\;,\;\; \mathbf{e}_{\zeta,\Im} = \frac{1}{\mathbf{i}}(\mathbf{e}_\zeta - \mathbf{e}_{\overline{\zeta}}) \;\;,\;\; \mathcal{A}_{\zeta,\mathbb{R}} = \mathbf{e}_{\zeta,\Re}\,\mathcal{A}_\mathbb{R}\ .$$

Si $\zeta \in \mathcal{Z}_\mathbb{C} \cap \mathbb{R}^n$, $\mathcal{A}_{\zeta,\mathbb{R}} = \mathbf{e}_\zeta \mathcal{A}_\mathbb{R}$. Si $\zeta \in \mathcal{Z}_\mathbb{C} \setminus \mathbb{R}^n$, $\mathbf{e}_{\zeta,\Im}^2 \equiv -\mathbf{e}_{\zeta,\Re}$.

***Lemme* 4.45.** *Si $\zeta \in \mathcal{Z}_{\mathbb{C}}$, alors la sous-algèbre $\mathcal{A}_{\zeta,\mathbb{R}}$ de $\mathcal{A}_{\mathbb{R}}$ contient $\mathbf{e}_{\zeta,\Re}$ et $\mathbf{e}_{\zeta,\Im}$. Et de plus, $\mathbf{e}_{\zeta,\Re}$ est son élément neutre.*

Démonstration. Les éléments $\mathbf{e}_{\zeta,\Re}$ et $\mathbf{e}_{\zeta,\Im}$ de $\mathcal{A}_{\mathbb{C}}$ sont fixes par conjugaison complexe, ils appartiennent donc à $\mathcal{A}_{\mathbb{R}}$. Par suite $\mathcal{A}_{\zeta,\mathbb{R}} \subset \mathcal{A}_{\mathbb{R}}$. Puisque $\mathbf{e}_{\zeta,\Im} \in \mathcal{A}_{\mathbb{R}}$ et $\mathbf{e}_{\zeta,\Re}\,\mathbf{e}_{\zeta,\Im} \equiv \mathbf{e}_{\zeta,\Im}$, nous déduisons que $\mathbf{e}_{\zeta,\Im} \in \mathcal{A}_{\zeta,\mathbb{R}}$. De plus, pour tout $a \in \mathcal{A}_{\zeta,\mathbb{R}}$, $\mathbf{e}_{\zeta,\Re}\,a \equiv a$ (car $\mathbf{e}^2_{\zeta,\Re} \equiv \mathbf{e}_{\zeta,\Re}$). □

Notons $\mathcal{W}$ un sous-ensemble de $\mathcal{Z}_{\mathbb{C}}$ qui contient un seul représentant par classe de conjugaison des racines de I (i.e. $\mathcal{W} = \{\xi_1, \ldots, \xi_s, \zeta_{2s+1}, \ldots, \zeta_d\}$, avec $\xi_i \in \{\zeta_i, \overline{\zeta}_i\}$ pour $i = 1, \ldots, s$).

***Proposition* 4.46.** *L'algèbre réelle $\mathcal{A}_{\mathbb{R}}$ se décompose en $\mathcal{A}_{\mathbb{R}} = \oplus_{\zeta\in\mathcal{W}}\, \mathcal{A}_{\zeta,\mathbb{R}}$.*

Démonstration. D'après le théorème 4.9, $\mathcal{A}_{\mathbb{C}} = \oplus_{\zeta\in\mathcal{W}}(\mathbf{e}_{\zeta} + \mathbf{e}_{\overline{\zeta}})\,\mathcal{A}_{\mathbb{C}}$. Comme l'ensemble des éléments de $\mathcal{A}_{\mathbb{C}}$ fixes par conjugaison est $\mathcal{A}_{\mathbb{R}}$, nous déduisons la décomposition souhaitée pour $\mathcal{A}_{\mathbb{R}}$.

□

Considérons maintenant la forme linéaire

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

où $tr(M_a)$ désigne la trace de l'opérateur de multiplication par a dans $\mathcal{A}_{\mathbb{C}}$.

***Lemme* 4.47.** *Si $g \in \mathbb{C}[\mathbf{x}]$ et $\zeta \in \mathcal{Z}_{\mathbb{C}}$, alors $Tr(g\,\mathbf{e}_{\zeta}) = \mu_{\zeta}\, g(\zeta)$. En particulier si $h \in \mathbb{C}[\mathbf{x}]$ et $\alpha \in \mathbb{N}^n \setminus \{0\}$, alors $Tr\big((\mathbf{x}-\zeta)^{\alpha} h \mathbf{e}_{\zeta}\big) = 0$.*

Démonstration. D'après le corollaire 4.22, $\big(g - g(\zeta)\big)\mathbf{e}_{\zeta}$ est nilpotent, donc

$$Tr\big((g - g(\zeta))\mathbf{e}_{\zeta}\big) = Tr(g\mathbf{e}_{\zeta}) - g(\zeta)Tr(\mathbf{e}_{\zeta}) = 0.$$

Puisque $\mathcal{A}_{\mathbb{C}} = \oplus_{\zeta\in\mathcal{Z}_{\mathbb{C}}}\mathcal{A}_{\zeta}, \mathbf{e}_{\zeta}$ est l'unité de la sous-algèbre $\mathcal{A}_{\zeta}$ de $\mathcal{A}_{\mathbb{C}}$ et $\mathbf{e}_{\zeta}\mathcal{A}_{\xi} = 0$ pour tout $\xi \in \mathcal{Z}_{\mathbb{C}} \setminus \{\zeta\}$, $Tr(\mathbf{e}_{\zeta}) = \dim_{\mathbb{C}}(\mathcal{A}_{\zeta}) = \mu_{\zeta}$. Ainsi, $Tr(g\mathbf{e}_{\zeta}) = g(\zeta)\,\mu_{\zeta}$. □

Pour tout $h \in \mathbb{R}[\mathbf{x}]$, définissons la forme bilinéaire

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

où $Tr(hab)$ désigne la trace de l'opérateur de multiplication pas hab dans $\mathcal{A}_{\mathbb{R}}$. La matrice de S_h est réelle symétrique, donc elle est diagonalisable sur $\mathbb{R}$.

Les racines réelles de $f_1, \ldots, f_m$ vont être décrites à l'aide de la forme quadratique Q_h associée à S_h. Le cas d'une variable a été étudié par Hermite, Jacobi au dix-neuvième siècle (voir [**Kli72**]). Le cas multivariable a été notamment étudié dans [**PRS93, Ped96, BPR03**].

Nous rappelons que la *signature* d'une forme quadratique Q sur $\mathcal{A}_{\mathbb{R}}$ est la différence entre le nombre de valeurs propres positives et le nombre de valeurs propres négatives de la matrice de Q dans une base quelconque de $\mathcal{A}_{\mathbb{R}}$. Le *rang* de Q est le nombre de valeurs propres non nulles de la matrice de Q.

***Théorème* 4.48.** *Soit $h \in \mathbb{R}[\mathbf{x}]$.*

i) Le nombre de racines complexes distinctes ζ de $f_1, \ldots, f_m$ telles que $h(\zeta) \neq 0$ est égal au rang de la forme quadratique Q_h.

ii) La différence entre le nombre de racines réelles distinctes ζ de $f_1, \ldots, f_m$ telles que $h(\zeta) > 0$ et le nombre de racines réelles distinctes ξ de $f_1, \ldots, f_m$ telles que $h(\xi) < 0$ est égale à la signature de Q_h.

Démonstration. Si $\mathcal{A}_{\zeta,\mathbb{R}} \neq \mathcal{A}_{\xi,\mathbb{R}}$, alors $\mathcal{A}_{\zeta,\mathbb{R}} \cdot \mathcal{A}_{\xi,\mathbb{R}} \equiv 0$. Par conséquent, la matrice de Q_h dans une base de $\mathcal{A}_{\mathbb{R}}$ formée d'éléments des sous-algèbres $\mathcal{A}_{\zeta,\mathbb{R}}$ est diagonale par blocs. Pour prouver le théorème 4.48, il suffit donc de le faire pour la restriction de Q_h à $\mathcal{A}_{\zeta,\mathbb{R}}$. Le rang (resp. la signature) de Q_h sera la somme des rangs (resp. signatures) de ces restrictions. La restriction de Q_h à $\mathcal{A}_{\zeta,\mathbb{R}}$ sera aussi notée Q_h.

D'après la proposition 4.15, le $\mathbb{C}$-espace vectoriel $\mathcal{A}_\zeta$ a une base de la forme $\big\{(\mathbf{x}-\zeta)^{\alpha_i}\mathbf{e}_\zeta, i = 0, \ldots, \mu_\zeta - 1\big\}$, avec $\alpha_i \in \mathbb{N}^n$ et $\alpha_0 = 0$.

Si $\zeta = \overline{\zeta}$, cette base est réelle et c'est aussi une base du $\mathbb{R}$-espace vectoriel $\mathcal{A}_{\zeta,\mathbb{R}}$. D'après le lemme 4.47, la matrice de Q_h dans cette base est

$$\big(Tr(\,(\mathbf{x}-\zeta)^{\alpha_i+\alpha_j}\, h\mathbf{e}_\zeta)\big)_{i,j=0,\ldots,\mu_\zeta-1} = \begin{pmatrix} \mu_\zeta\, h(\zeta) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

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

Si $\zeta \neq \overline{\zeta}$, nous déduisons la base réelle suivante de $\mathcal{A}_\zeta \oplus \mathcal{A}_{\overline{\zeta}} = (\mathbf{e}_\zeta + \mathbf{e}_{\overline{\zeta}})\mathcal{A}$, de celles de $\mathcal{A}_\zeta$ et $\mathcal{A}_{\overline{\zeta}}$,

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

Cette famille est aussi une base du $\mathbb{R}$-espace vectoriel $\mathcal{A}_{\zeta,\mathbb{R}}$. D'après le lemme 4.47, la matrice de Q_h dans cette base est

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

Le rang de Q_h est donc 2 si $h(\zeta) \neq 0$ et 0 sinon. Pour étudier sa signature, posons $a = \Re\big(h(\zeta)\big)$ et $b = \Im\big(h(\zeta)\big)$ (la partie réelle et la partie imaginaire de

$h(\zeta)\big)$. Si $ab = 0$, la signature de Q_h est nulle. Si $ab \neq 0$, la signature Q_h est la signature de la forme quadratique

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

qui est encore nulle.

Par conséquent, le rang de Q_h (comme forme quadratique sur $\mathcal{A}$) compte le nombre de racines complexes distinctes $\zeta \in \mathcal{Z}_{\mathbb{C}}$ telles que $h(\zeta) \neq 0$, et sa signature, la différence entre le nombre de racines réelles ζ telles que $h(\zeta) > 0$ et le nombre de racines réelles ξ telles que $h(\xi) < 0$. □

Le théorème 4.48 permet de compter le nombre de racines dans une région donnée (voir exercices 4.18, 4.19, 4.20). Ce qui est utile pour la localisation des zéros d'un système polynomial avant de les déterminer numériquement.

***Corollaire* 4.49.** *Soient $f_1, \ldots, f_m \in \mathbb{R}[\mathbf{x}]$.*

i) Le nombre de racines complexes distinctes du système $f_1 = \cdots = f_m = 0$ est égal au rang de la forme quadratique Q_1.

ii) Le nombre de racines réelles distinctes de $f_1 = \cdots = f_m = 0$ est égal à la signature de Q_1.

***Algorithme* 4.50.** Nombre de racines réelles d'un système polynomial.

Entrée : `Des polynômes` $f_1, \ldots, f_m \in \mathbb{R}[\mathbf{x}]$ `définissant une variété de dimension` 0.

1. `Déterminer une base` $(\mathbf{x}^\alpha)_{\alpha \in E}$ `de` $\mathbb{R}[\mathbf{x}]/(f_1, \ldots, f_m)$.
2. `Calculer la matrice symétrique` $\big(Tr(\mathbf{x}^{\alpha+\beta})\big)_{\alpha,\beta \in E}$`, sa signature` s `et son rang` r.

Sortie : `Retourner`

$r = \mathrm{card}\{\zeta \in \mathbb{C}^n : f_1(\zeta) = \cdots = f_m(\zeta) = 0\}$,

$s = \mathrm{card}\{\xi \in \mathbb{R}^n : f_1(\xi) = \cdots = f_m(\xi) = 0\}$.

***Exemple* 4.51.** *Reprenons l'exemple 4.5 et calculons les matrices $\mathtt{Q}_1$ de Q_1 et $\mathtt{Q}_{x_1}$ de Q_{x_1}. Par exemple*

$$\mathtt{Q}_{x_1} = \begin{pmatrix} Tr(x_1) & Tr(x_1^2) & Tr(x_1x_2) & Tr(x_1^2x_2) \\ Tr(x_1^2) & Tr(x_1^3) & Tr(x_1^2x_2) & Tr(x_1^3x_2) \\ Tr(x_1x_2) & Tr(x_1^2x_2) & Tr(x_1x_2^2) & Tr(x_1^2x_2^2) \\ Tr(x_1^2x_2) & Tr(x_1^3x_2) & Tr(x_1^2x_2^2) & Tr(x_1^3x_2^2) \end{pmatrix}.$$

En utilisant les matrices $\mathtt{M}_{x_1}$ *et* $\mathtt{M}_{x_2}$ *calculées dans l'exemple 4.27,* $Tr(1) = 4, Tr(x_1) = tr(\mathtt{M}_{x_1}) = 0, Tr(x_2) = tr(\mathtt{M}_{x_2}) = 4, Tr(x_1x_2) = Tr(\mathtt{M}_{x_1}\mathtt{M}_{x_2}) = \frac{2}{9}$. *La forme linéaire* Tr *a pour coordonnées* $(4, 0, 4, \frac{2}{9})$ *dans la base duale de la base* $(1, x_1, x_2, x_1\,x_2)$ *de* $\mathcal{A}$. *Les coordonnées de la forme linéaire* $x_1 \cdot Tr$ *dans la même base sont*

$$ {}^t\big(Tr(x_1), Tr(x_1^2), Tr(x_1x_2), Tr(x_1^2\,x_2)\big) = {}^t\mathtt{M}_{x_1}\,{}^t\left(4, 0, 4, \frac{2}{9}\right) = {}^t\left(0, \frac{4}{9}, \frac{2}{9}, \frac{4}{9}\right). $$

Ce vecteur constitue la première colonne de la matrice $\mathtt{Q}_{x_1}$. *Les autres colonnes de* $\mathtt{Q}_{x_1}$ *s'obtiennent par multiplication de ce vecteur par* ${}^t\mathtt{M}_{x_1}$, ${}^t\mathtt{M}_{x_2}$, ${}^t\mathtt{M}_{x_2}\,{}^t\mathtt{M}_{x_1}$ *:*

$$ \mathtt{Q}_1 = \begin{pmatrix} 4 & 0 & 4 & \frac{2}{9} \\ 0 & \frac{4}{9} & \frac{2}{9} & \frac{4}{9} \\ 4 & \frac{2}{9} & \frac{37}{9} & \frac{4}{9} \\ \frac{2}{9} & \frac{4}{9} & \frac{4}{9} & \frac{37}{81} \end{pmatrix} \quad , \quad \mathtt{Q}_{x_1} = \begin{pmatrix} 0 & \frac{4}{9} & \frac{2}{9} & \frac{4}{9} \\ \frac{4}{9} & 0 & \frac{4}{9} & \frac{2}{81} \\ \frac{2}{9} & \frac{4}{9} & \frac{4}{9} & \frac{37}{81} \\ \frac{4}{9} & \frac{2}{81} & \frac{37}{81} & \frac{4}{81} \end{pmatrix}. $$

Le rang des deux formes quadratiques Q_1 *et* Q_{x_1} *est* 2, *leurs signatures respectives sont* 2 *et* 0. *Ceci confirme que le système de l'exemple 4.5 a deux racines réelles distinctes et que leurs premières coordonnées sont de signes opposés (voir exemple 4.27).*

4.12. Exercices

***Exercice* 4.1.** Soient

$$ f_1(x, y, z) = x^5 + y^4 + z^3 - 1 \quad \text{et} \quad f_2(x, y, z) = x^3 + y^3 + z^2 - 1 $$

des éléments de $\mathbb{K}[x, y, z]$. En utilisant un système de calcul formel, calculer :

1. La base de Gröbner réduite de (f_1, f_2) pour l'ordre gradué lexicographique inverse $x > y > z$.
2. La base de Gröbner réduite pour l'ordre lexicographique $x > y > z$.
3. Que constatez-vous ?

***Exercice* 4.2.** Soit $f(x) = (x + 1)(x + 2)\ldots(x + 20)$.

1. En utilisant un système de calcul formel, trouver les racines du polynôme $g(x) = f(x) + 10^{-9}x^{19}$.
2. Comparer les racines de $f(x)$ à celles de $g(x)$.

***Exercice* 4.3.** Soit $\mathcal{Z}$ une partie de $\mathbb{K}^n$ contenant d éléments. Montrer qu'au moins une des formes linéaires $x_1 + ix_2 + \cdots + i^{n-1}x_n, i = 0, \ldots, (n-1)\binom{d}{2}$, sépare $\mathcal{Z}$.

***Exercice* 4.4.** Soient $\mathbb{K}$ un corps algébriquement clos et I un idéal 0-dimensionnel de $\mathbb{K}[\mathbf{x}]$.

1. Montrer que tout idéal premier propre de $\mathbb{K}[\mathbf{x}]$ contenant I est maximal.
2. Si $\mathcal{Z}(I) = \{\zeta_1, \ldots, \zeta_d\}$, montrer que $\sqrt{I} = \mathfrak{m}_{\zeta_1} \cap \ldots \cap \mathfrak{m}_{\zeta_d}$, où $\mathfrak{m}_{\zeta_i}$ désigne l'idéal maximal de $\mathbb{K}[\mathbf{x}]$ défini par la racine ζ_i.

3. En déduire une décomposition primaire de I.
4. Montrer que cette décomposition est unique.

***Exercice* 4.5.** Soit I un idéal 0-dimensionnel de $\mathbb{K}[\mathbf{x}]$ et $Q_1 \cap \ldots \cap Q_r$ sa décomposition primaire. Montrer que l'algèbre $\mathbb{K}[\mathbf{x}]/I$ est isomorphe à $\mathbb{K}[\mathbf{x}]/Q_1 \times \cdots \times \mathbb{K}[\mathbf{x}]/Q_r$.

***Exercice* 4.6.** Un *anneau artinien* est un anneau dans lequel toute suite décroissante d'idéaux est stationnaire. Montrer :

1. Un anneau A est artinien si, et seulement si, tout ensemble non vide d'idéaux de A admet un élément minimal.
2. Dans un anneau artinien, tout idéal premier est maximal.
3. Dans un anneau artinien, il y a seulement un nombre fini d'idéaux maximaux.
4. Si I est un idéal de $\mathbb{K}[\mathbf{x}]$ tel que le $\mathbb{K}$-espace vectoriel $\mathbb{K}[\mathbf{x}]/I$ est de dimension finie, alors $\mathbb{K}[\mathbf{x}]/I$ est artinien.

***Exercice* 4.7. Radical d'un idéal 0-dimensionnel**
Soit I un idéal 0-dimensionnel de $\mathbb{K}[\mathbf{x}]$.

1. Montrer que le nombre de racines distinctes de I est $\dim_{\mathbb{K}}\big(\mathbb{K}[\mathbf{x}]/\sqrt{I}\big)$.
2. Si f est un polynôme en une variable, $\tilde{f} = \dfrac{f}{\mathrm{pgcd}(f, f')}$ est sa partie sans facteur carré. Montrer que $\sqrt{I} = I + \big(\tilde{f}_1(x_1), \ldots, \tilde{f}_n(x_n)\big)$, où $\big(f_i(x_i)\big) = I \cap \mathbb{K}[x_i]$, pour $i = 1, \ldots, n$.

***Exercice* 4.8.** Le but de cet exercice est de donner une autre construction des idempotents (voir [**GVRR97**] pour plus de détails).

Soit I un idéal de $\mathbb{K}[\mathbf{x}]$ tel que le $\mathbb{K}$-espace vectoriel $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ soit de dimension finie. Notons $\mathcal{Z}(I) = \{\zeta_1, \ldots, \zeta_d\}$.

1. En utilisant les polynômes d'interpolation de Lagrange, montrer qu'il existe des éléments p_i de $\mathbb{K}[\mathbf{x}]$ tels que $p_i(\zeta_i) = 1$ et $p_i(\zeta_j) = 0$ si $i \neq j$.
2. Montrer qu'il existe des entiers positifs n_i tels que $p_i^{n_i}\, p_j^{n_j} \in I$ si $i \neq j$.
3. Prouver qu'il existe des polynômes a_i tels que $\sum_{i=1}^{d} a_i p_i^{n_i} - 1 \in I$.
4. En déduire l'existence d'éléments $\mathbf{e}_1, \ldots, \mathbf{e}_d$ de $\mathbb{K}[\mathbf{x}]$ qui vérifient

$$\sum_{i=1}^{d} \mathbf{e}_i \equiv 1 \ , \ \mathbf{e}_i\, \mathbf{e}_j \equiv 0 \text{ si } i \neq j \ , \ \mathbf{e}_i^2 \equiv \mathbf{e}_i \ , \ \mathbf{e}_i(\zeta_i) = 1.$$

***Exercice* 4.9. Radical d'un idéal.**
Soit I un idéal 0-dimensionnel de $\mathbb{K}[\mathbf{x}]$. Notons $\mathbf{e}_1, \ldots, \mathbf{e}_d$ (resp. $\mathfrak{m}_{\zeta_1}, \ldots, \mathfrak{m}_{\zeta_d}$) les idempotents (resp. idéaux maximaux) associés à $\mathcal{Z}(I) = \{\zeta_1, \ldots, \zeta_d\}$.

1. Si $\mathcal{B}_\zeta = \mathcal{A}_\zeta / \mathbf{e}_\zeta\, \mathfrak{m}_\zeta$ et $\mathcal{B} = \oplus_{\zeta \in \mathcal{Z}(I)} \mathcal{B}_\zeta$, montrer que $\mathcal{B} = \mathbb{K}\mathbf{e}_1 \oplus \cdots \oplus \mathbb{K}\mathbf{e}_d$. Puis décomposer $a \in \mathbb{K}[\mathbf{x}]$ selon cette somme directe.
2. Prouver que $\sqrt{I} = I + \sum_{\zeta \in \mathcal{Z}(I)} \mathbf{e}_\zeta\, \mathfrak{m}_\zeta$.
3. Si $a \in \mathcal{A}_\zeta$, montrer que la forme linéaire $a.Tr$ sur $\mathcal{A}$ est nulle si, et seulement si, $a \in \mathbf{e}_\zeta\, \mathfrak{m}_\zeta$.

4. En déduire que $\sqrt{I} = I + \mathcal{E}$, où $\mathcal{E}$ désigne l'espace vectoriel engendré par $\{a \in \mathbb{K}[\mathbf{x}]/I : a.Tr = 0\}$.
5. Donner un algorithme pour construire le radical de I.

***Exercice* 4.10.** Donner un système $f_1 = f_2 = 0$ de $\mathbb{K}[x, y]$ tel que $\mathcal{Z}(f_1, f_2)$ soit finie et pour tout $a \in \mathcal{A} = \mathbb{K}[x, y]/(f_1, f_2)$, les sous-espaces propres de l'endomorphisme transposé de la multiplication par a dans $\mathcal{A}$ soient de dimensions au moins 2.

***Exercice* 4.11.** Soient $f_1 = x^3 - 3x^2 + 2x, f_2 = y - x^2 + 1$ des éléments de $\mathbb{K}[x, y]$.

1. Déterminer une base de l'espace vectoriel $\mathcal{A} = \mathbb{K}[x, y]/(f_1, f_2)$.
2. Calculer les valeurs propres de la multiplication par x dans $\mathcal{A}$ et leurs sous-espaces propres.
3. Calculer les valeurs propres de la multiplication par y dans $\mathcal{A}$ et leurs sous-espaces propres.
4. En déduire les solutions du système $f_1 = f_2 = 0$.
5. Trouver les sous-algèbres locales $\mathcal{A}_i$ de $\mathcal{A}$.

***Exercice* 4.12.** Soient $f_1 = x^2 - xy + y, f_2 = x^2y - x^2 - y^2 + y$ des polynômes de $\mathbb{K}[x, y]$.

1. Déterminer une base de l'espace vectoriel $\mathcal{A} = \mathbb{K}[x, y]/(f_1, f_2)$.
2. Quel est le nombre de racines réelles, puis complexes, communes aux équations $f_1 = 0, f_2 = 0$?
3. Calculer les valeurs propres des endomorphismes de multiplication par $x, y, 2x + 3y$ dans $\mathcal{A}$ et leurs sous-espaces propres.
4. Déterminer $\mathcal{Z}(f_1, f_2)$.

***Exercice* 4.13.** Montrer la proposition 4.41.

***Exercice* 4.14.** Soit I l'idéal de $\mathbb{C}[x_1, x_2, x_3, x_4]$ engendré par les 4 polynômes

$$f_1 = 2x_1^2 + 2{x_2}^2 + 2{x_3}^2 + {x_4}^2 - x_4 \ , \ f_2 = 2x_1x_2 + 2x_2x_3 + 2x_3x_4 - x_3 \ ,$$
$$f_3 = 2x_1x_3 + x_3^2 + 2x_2x_4 - x_2 \ , \ f_4 = 2x_1 + 2x_2 + 2x_3 + x_4 - 1.$$

Utiliser un système de calcul formel pour :

1. Calculer la base de Gröbner réduite lexicographique avec $x_1 < x_2 < x_3 < x_4$.
2. Déterminer le nombre de racines complexes (en tenant compte des multiplicités) communes à f_1, f_2, f_3, f_4, le nombre de racines complexes distinctes communes à f_1, f_2, f_3, f_4, et le nombre de racines réelles distinctes communes à f_1, f_2, f_3, f_4.
3. Calculer les matrices des opérateurs de multiplication $M_{x_1}, M_{x_2}, M_{x_3}, M_{x_4}$.
4. Résoudre $f_1 = f_2 = f_3 = f_4 = 0$ par la méthode des vecteurs propres, puis par triangulation simultanée.
5. Déterminer la forme de Chow de l'idéal I.
6. Trouver une représentation univariée rationnelle des zéros de I.
7. Comparer cette représentation avec la base de Gröbner lexicographique déjà calculée.

***Exercice* 4.15.** Soit I un idéal 0-dimensionnel et radical de $\mathbb{K}[\mathbf{x}]$. Supposons que x_n sépare $\mathcal{Z}(I)$.

1. Montrer que la base de Gröbner réduite pour l'ordre lexicographique $x_1 < \cdots < x_n$ est $\{x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\}$, où les g_i sont des polynômes de la variable x_n.
2. En déduire que la $\mathbb{K}$-algèbre $\mathbb{K}[\mathbf{x}]/I$ est isomorphe à $\mathbb{K}[x_n]/\big(g_n(x_n)\big)$.
3. Si J est un idéal 0-dimensionnel de $\mathbb{K}[\mathbf{x}]$, est-ce que l'on peut toujours trouver un polynôme d'une variable g tel que $\mathbb{K}[\mathbf{x}]/J$ soit isomorphe à $\mathbb{K}[x_n]/\big(g(x_n)\big)$?

***Exercice* 4.16.** Soient $I = (f_1, \ldots, f_m)$ un idéal radical et 0-dimensionnel, et a un élément de $\mathbb{K}[\mathbf{x}]$ qui sépare $\mathcal{Z}(I)$.

1. Si $P(T)$ est le polynôme caractéristique de l'endomorphisme M_a de multiplication par a dans $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$, montrer que l'application
$$\begin{array}{rcl} \mathbb{K}[T] & \to & \mathcal{A} \\ g(T) & \mapsto & g(a) \end{array}$$
induit un isomorphisme entre $\mathbb{K}[T]/\big(P(T)\big)$ et $\mathcal{A}$.
2. Soient $g_1, \ldots, g_n$ des polynômes de $\mathbb{K}[T]$ tels que $g_i(a) = x_i$ dans $\mathcal{A}$. Montrer que $\mathcal{Z}(f_1, \ldots, f_m) = \{\big(g_1(\lambda), \ldots, g_n(\lambda)\big) : \lambda \text{ est valeur propre de } M_a\}$.

***Exercice* 4.17. Calcul d'une représentation univariée rationnelle à partir des traces.**
Soient I un idéal 0-dimensionnel de $\mathbb{K}[\mathbf{x}]$, $\mathcal{C}(\mathbf{u})$ sa forme de Chow et $t = (t_0, \ldots, t_n)$ un vecteur générique de $\mathbb{K}^{n+1}$.

1. Montrer que
$$d_0(u_0) := \mathcal{C}(t_0 + u_0, t_1, \ldots, t_n) = \prod_{\zeta \in \mathcal{Z}(I)} \big(t(\zeta) + u_0\big)^{\mu_\zeta},$$
$$\begin{aligned} d_0(u_0 + \epsilon) &= d_0(u_0) + \epsilon \sum_{\zeta \in \mathcal{Z}(I)} \mu_\zeta \big(t(\zeta) + u_0\big)^{\mu_\zeta - 1} \prod_{\xi \neq \zeta} \big(t(\xi) + u_0\big)^{\mu_\xi} + \mathcal{O}(\epsilon^2), \\ \tilde{d_0}(u_0; \epsilon\, x_i) &= \mathcal{C}(t_0 + u_0, t_1, \ldots, t_i + \epsilon\, x_i, \ldots, t_n) \\ &= d_0(u_0) + \epsilon \sum_{\zeta \in \mathcal{Z}(I)} \mu_\zeta\, \zeta_i \big(t(\zeta) + u_0\big)^{\mu_\zeta - 1} \prod_{\xi \neq \zeta} \big(t(\xi) + u_0\big)^{\mu_\xi} + \mathcal{O}(\epsilon^2), \end{aligned}$$
où $t(\zeta) = t_0 + \zeta_1 t_1 + \cdots + \zeta_n t_n$ si $\zeta = (\zeta_1, \ldots, \zeta_n)$.
2. Quel est le coefficient de ϵ dans $d_0(u_0 + \epsilon)$?
3. Si $d_i(u_0)$ désigne le coefficient de ϵ dans $\tilde{d_0}(u_0; \epsilon x_i)$, montrer que
$$\lim_{u_0 \to -t(\zeta)} \frac{d_i(u_0)}{{d_0}'(u_0)} = \zeta_i.$$
4. Montrer que l'on peut déterminer le polynôme $d_0(u_0)$ en calculant les traces des opérateurs de multiplication par les puissances de $t_0 + t_1 x_1 + \cdots + t_n x_n$ dans $\mathbb{K}[\mathbf{x}]/I$ (en utilisant les relations entre les sommes de Newton et les fonctions symétriques élémentaires des racines).

5. En déduire que les polynômes $d_0{}'(u_0), d_1(u_0), \ldots, d_n(u_0)$ peuvent également se calculer à partir de la forme linéaire Tr.
6. Donner un algorithme qui fournit une représentation univariée rationnelle des solutions d'un idéal 0-dimensionnel à l'aide de la forme linéaire Tr.

***Exercice* 4.18.** Soient $h, f_1, \ldots, f_m \in \mathbb{R}[\mathbf{x}]$. Expliquer comment l'on peut obtenir les nombres suivants :

1. Le nombre de racines réelles de $f_1, \ldots, f_m$ qui n'annulent pas h.
2. Le nombre de racines réelles ξ de $f_1, \ldots, f_m$ telles que $h(\xi) > 0$.
3. Le nombre de racines réelles de $f_1, \ldots, f_m$ dans l'hypersurface $\{h = 0\}$.

***Exercice* 4.19.** Quel est le nombre de solutions réelles d'un système polynomial réel à l'intérieur d'une boule euclidienne ouverte de $\mathbb{R}^n$?

***Exercice* 4.20.** Etant donnés $f_1, \ldots, f_m \in \mathbb{R}[\mathbf{x}]$.

1. Soient $h_1, h_2 \in \mathbb{R}[\mathbf{x}]$. Quel est le nombre de racines réelles ζ de $f_1, \ldots, f_m$ telles que $h_1(\zeta) > 0$ et $h_2(\zeta) > 0$?
2. Supposons $n = 2$. Quel est le nombre de racines réelles ζ de $f_1, \ldots, f_m$ à l'intérieur d'un rectangle de $\mathbb{R}^2$?
3. Soient $h_1, \ldots, h_s \in \mathbb{R}[\mathbf{x}]$. Quel est le nombre de racines réelles ζ de $f_1, \ldots, f_m$ telles que $h_1(\zeta) > 0, \ldots, h_s(\zeta) > 0$?