1. Systèmes Zéro-dimensionnels à coefficients dans $\mathbb{C}$

On s'intéresse ici aux systèmes d'équations $\{P_1 = 0, ..., P_s = 0\}$ avec $P_i \in \mathbb{C}[X_1, ..., X_n], i = 1...s$ admettant un nombre fini de solutions complexes. Notons $\mathcal{E} = \{P_1, ..., P_s\}$, on impose donc que $\sharp V(\mathcal{E}) < \infty$, $\sharp V(\mathcal{E})$ étant le cardinal de $V(\mathcal{E})$.

1.1. Direction séparante

Un outil qui nous servira plusieurs fois est l'utilisation d'une forme linéaire séparant un ensemble de points.

Définition 1. *Soit $\mathcal{S} \subset \mathbb{C}^n$ un ensemble de points tel que $\sharp\mathcal{S} = d < \infty$ et $U = a_1 X_1 + ... + a_n X_n$, $a_i \in \mathbb{C}$, une forme linéaire. On dit que U sépare $\mathcal{S}$ si $\forall x, y \in S$, $x \neq y \Rightarrow U(x) \neq U(y)$.*

Lemme 2. *$\exists i \in \left\{0...n\,\frac{d\,(d-1)}{2}\right\}$ tel que $U_i = X_1 + i\,X_2 + ... + i^{n-1} X_n$ sépare $\mathcal{S}$*

Démonstration. Pour $x \neq y \in \mathcal{S}$, on considère le polynôme de $\mathbb{C}[i]$ $U_i(x) - U_i(y) = x_1 - y_1 + i\,(x_2 - y_2) + ... + i^{(n-1)}(x_n - y_n)$. Ce polynôme est non identiquement nul puisque $x \neq y$ et admet par conséquent au plus $n-1$ solutions dans $\mathbb{C}$. En prenant n valeurs entières pour i on est sûr d'éviter une de ses racines. On réitère l'opération pour les $\frac{d\,(d-1)}{2}$ couples possibles d'éléments de $\mathcal{S}$ pour conclure. □

1.2. L'anneau quotient $\frac{\mathbb{C}[X_1, ..., X_n]}{I}$

A un idéal I de $\mathbb{C}[X_1, ..., X_n]$ on associe une relation d'équivalence sur $\mathbb{C}[X_1, ..., X_n]$ appelée *congruence modulo I*. On note $a = b$ mod I si et seulement si $a - b \in I$. Il est clair que si $a_1 - b_1 \in I$, $a_2 - b_2 \in I$ alors

$$(a_1 + a_2) - (b_1 + b_2) \in I, \quad a_1\,a_2 - b_1\,b_2 \in I. \tag{1}$$

L'*anneau quotient A/I* est alors l'ensemble des classes d'équivalences avec la structure d'anneau naturelle obtenue en définissant la somme ou le produit de deux classes comme la classe de la somme ou du produit de deux éléments quelconques de ces classes.

Théorème 3. *On se donne un ensemble de polynômes $\mathcal{E} = \{P_1, ..., P_s\} \subset \mathbb{C}[X_1, ..., X_n]$.*
$\#V(\mathcal{E}) < \infty$ ssi $\frac{\mathbb{C}[X_1, ..., X_n]}{I}$ est un $\mathbb{C}$-espace vectoriel de dimension finie.

Démonstration.

- $\#V(\mathcal{E}) < \infty \Rightarrow \forall i = 1 ... n, P_i = \prod_{\alpha \in V(\mathcal{E})} (X_i - \alpha) \in I(V(\mathcal{E}))$. Il existe donc $n_i \in \mathbb{N}^\star$ tel que $P_i^{n_i} \in \langle \mathcal{E} \rangle$. Ainsi $\{X_1^{e_1} ... X_n^{e_n}, e_i < n_i\,\sharp V(\mathcal{E}), i = 1 ... n\}$ engendre $\frac{\mathbb{C}[X_1, ..., X_n]}{I}$ comme $\mathbb{C}$-espace vectoriel;
- Si $\frac{\mathbb{C}[X_1, ..., X_n]}{I}$ est un $\mathbb{C}$-espace vectoriel de dimension finie, alors $\forall i = 1 ... n$, $\exists n_i \in \mathbb{N}$, 1, $X_i ..., X_i^{n_i}$ soient linéairement dépendants. Ainsi, $\forall i = 1 ... n$, $\exists p_i \in \mathbb{C}[X_i]$ t.q. $p_i \in I$ et $V(\mathcal{E}) \subset \{x = (x_1, ..., x_n) \in \mathbb{C}^n, p_i(x_i) = 0\}$ ce qui implique $\#V(\mathcal{E}) < \infty$. □

Un petit résultat qui sera utile à diverses reprises :

Proposition 4. *On se donne un ensemble de polynômes $\mathcal{E} = \{P_1, ..., P_s\} \subset \mathbb{C}[X_1, ..., X_n]$ tel que $\#V(\mathcal{E}) < \infty$. Si $U \in \mathbb{C}[X_1, ..., X_n]$ sépare $V(\mathcal{E})$, alors $1, U, ..., U^{d-1}$ avec $d = \sharp V(\mathcal{E})$ sont linéairement indépendants dans $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$.*

Démonstration. Soit $U \in \mathbb{C}[X_1, ..., X_n]$ séparant et supposons qu'il existe des scalaires $u_0, ..., u_{d-1}$ tels que $P_u = \sum_{i=0}^{d-1} u_i U^i = 0$ dans $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$. Ceci implique en particulier que $P_u \in \langle \mathcal{E} \rangle$ et donc que $P_u \in \sqrt{\langle \mathcal{E} \rangle}$ et donc que $P_u(\alpha) = 0, \forall \alpha \in V(\mathcal{E})$. En outre $P_u(\alpha) - P_u(\beta) = (U(\alpha) - U(\beta))(u_1 + ... + u_{d-1}(U(\alpha) - U(\beta))^{d-2}) = 0, \forall \alpha \neq \beta \in V(\mathcal{E})$ ce qui implique en particulier que $u_1 = 0$ car $U(\alpha) \neq U(\beta)$ par hypothèse. De proche en proche, on montre que $u_1, ..., u_{d-1} = 0$ et donc que $P_u(U) = u_0$ et comme $P(U(\langle \backslash alpha \rangle)) = 0, \forall \alpha \in V(\mathcal{E})$, alors $P_u = 0$.

□

1.3. Anneaux de fractions - Anneau local - Anneau local d'un point

Dans cette partie, le terme anneau indique par défaut un anneau commutatif unitaire.

Anneau de fractions

Si A est un anneau et $S \subset A$ une partie de A stable pour la multiplication, on définit l'anneau de fractions de A associé à S par $S^{-1}A = \{\frac{a}{s} \text{modulo} \sim, a \in A, s \in S\}$ ou $\frac{a}{s} \sim \frac{a'}{s'} \Leftrightarrow \exists t \in S, t(a\,s' - a'\,s) = 0$.

C'est un anneau pour les opérations $\left(\frac{a}{s}\right) + \left(\frac{a'}{s'}\right) = \left(\frac{a\,s' + a'\,s}{s\,s'}\right)$ et $\left(\frac{a}{s}\right) \times \left(\frac{a'}{s'}\right) = \left(\frac{a\,a'}{s\,s'}\right)$

Anneaux locaux

Un anneau local est un anneau possèdant un unique idéal maximal.

Une définition équivalente consiste à dire que A est un anneau local si $\forall a \in A$ soit a soit 1+a est inversible.

Une troisième définition équivalente est de dire que l'ensemble des éléments non inversibles de A est un idéal (maximal).

Anneau local d'un point

Soit $\alpha \in \mathbb{C}^n$, on pose $S_\alpha = \{P \in \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}, P(\alpha) \neq 0\}$ et on définit le localisé de $\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$ en α par $\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha = S_\alpha^{-1}\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$. C'est un anneau local.

1.4. Décomposition de $\frac{\mathbb{C}[X_1, ..., X_n]}{I}$

Proposition 5. *$\mathcal{E} = \{f_1, ..., f_s\} \subset \mathbb{C}[X_1, ..., X_n]$. Si $V(\mathcal{E}) \subset \mathbb{C}^n$ est fini, alors $\forall x \in V(\mathcal{E})$, $\exists e_x \in \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ tel que*

- $\sum_{x \in V(\mathcal{E})} e_x = 1$ *dans* $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$
- $\forall x \in V(\mathcal{E}), e_x^2 = e_x$ *dans* $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$
- $\forall x \in V(\mathcal{E}), e_x(x) = 1$
- *Dans* $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$, $e_x e_y = 0, \forall x \neq y, x, y \in V(\mathcal{E})$

Démonstration. On prend $U = \sum_{i=1}^n a_i\, X_i$ avec $a_i \in \mathbb{C}$ et tel que U sépare $V(\mathcal{E})$ et on pose $s_x = \frac{\prod_{y \neq x \in V(\mathcal{E})} (U - U(y))}{\prod_{y \neq x \in V(\mathcal{E})} (U(x) - U(y))}$.

$s_x\, s_y$ s'annule sur $V(\mathcal{E})$ donc $\exists n \in \mathbb{N}^\star$ $(s_x\, s_y)^{n_{x,y}} \in \langle \mathcal{E} \rangle$. On pose $t_x = s_x^{n_{x,y}}$ et $t_y = s_y^{n_{x,y}}$ et on a alors $t_x\, t_y = 0$ dans $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ et $t_x(x) = 1$.

On remarque que $V(\mathcal{E} \cup \{t_x, x \in V(\mathcal{E})\}) = \emptyset$ donc $I(V(\mathcal{E} \cup \{t_x, x \in V(\mathcal{E})\})) = 1$ et donc il existe des polynômes $r_x, x \in V(\mathcal{E})$ et $r_1, ..., r_s$ tels que $1 = \sum_{x \in V(\mathcal{E})} r_x\, t_x + \sum_{i=1}^s r_i\, f_i$ ce qui implique que $1 = \sum_{x \in V(\mathcal{E})} r_x\, t_x$ dans $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$.

On pose alors, pour tout $x \in V(\mathcal{E})$, $e_x = r_x\, t_x$. On a alors $\sum_{x \in V(\mathcal{E})} e_x = 1$, $e_y = \sum_{x \in V(\mathcal{E})} e_x\, e_y = e_y^2$.

Comme e_x est multiple de t_x alors $e_x e_y$ est multiple de $t_x t_y$ et donc $e_x e_y = 0$ dans $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$.

□

Lemme 6. $\forall \alpha \in V(\mathcal{E}), \left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha \simeq e_\alpha\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$

Démonstration.

Supposons que pour tout q, $q(\alpha) \neq 0$, $e_\alpha q$ soit inversible dans $e_\alpha\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$ et définissons les morphismes d'anneaux

$\Phi : e_\alpha\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right) \to \left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha$ tel que $\Phi(e_\alpha p) = \frac{p}{1}$

et

$\Psi : \left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha \to e_\alpha\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$ tel que $\Psi\left(\frac{p}{q}\right) = (e_\alpha\, p)\,(e_\alpha q)^{-1}$

Alors $\Phi\left(\Psi\left(\frac{p}{q}\right)\right) = \Phi((e_\alpha\ p)\ (e_\alpha q)^{-1}) = \frac{e_\alpha p}{e_\alpha q} = \frac{p}{q}$ et $\Psi(\Phi(e_\alpha p)) = \Psi\left(\frac{p}{1}\right) = (e_\alpha p)(e_\alpha)^{-1} = (e_\alpha^2 p)(e_\alpha)^{-1} = e_\alpha p$ dans $e_\alpha\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$.

Soit $q \in \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ tel que $q(\alpha) \neq 0$: c'est en particulier un inversible de $\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha$.

Montrons que $e_\alpha q$ est alors inversible dans $e_\alpha\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$.

Comme $q(\alpha) \neq 0$ alors $q = q(\alpha)(1 + v)$ avec $v(\alpha) = 0$.

En outre, $\forall y \in V(\mathcal{E}), (e_\alpha\, v)(y) = 0$ puisque $e_\alpha(y) = 0$ si $y \neq \alpha$ et $v(\alpha) = 0$.

Ainsi $\exists n \in \mathbb{N}^\star, (e_\alpha\, v)^n = e_\alpha v^n \in \langle \mathcal{E} \rangle$ et donc $e_\alpha v^n = 0$ dans $\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$.

Ainsi $\frac{1}{e_\alpha q} = \frac{1}{e_\alpha q(\alpha)(1+v)} = \frac{1}{e_\alpha^2 q(\alpha)} e_\alpha\,(1 - v + v^2 - ... + (-1)^{n-1} v^{n-1})$ dans $\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$ que l'on ré-écrit $\frac{1}{e_\alpha q} = \frac{1}{e_\alpha q(\alpha)} e_\alpha^2\,(1 - v + v^2 - ... + (-1)^{n-1} v^{n-1}) = \frac{1}{q(\alpha)} e_\alpha\,(1 - v + v^2 - ... + (-1)^{n-1} v^{n-1}) \in e_\alpha\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$.

□

Ce lemme nous permet, entre autres, de voir $\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha$ comme un $\mathbb{C}$-espace vectoriel dès lors que $\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$ en est un.

Définition 7. *$\forall \alpha \in V(\mathcal{E})$, la multiplicité $\mu(\alpha)$ de $\alpha \in V(\mathcal{E})$ est la dimension de $\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha$ comme $\mathbb{C}-$*espace *vectoriel.*

Théorème 8. $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle} \cong \oplus_{\alpha \in V(\mathcal{E})}\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha$. *En particulier* $\dim\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right) = \sum_{\alpha \in V(\mathcal{E})} \mu(\alpha)$.

Démonstration. En fait on ne fait qu'écrire que si $f \in \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$, comme $\sum_{\alpha \in V(\mathcal{E})} e_\alpha = 1$, f s'exprime alors comme $f = \sum_{\alpha \in V(\mathcal{E})} e_\alpha f$ ou les $e_\alpha\, f$ sont des éléments de $e_\alpha\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$ qui est isomorphe à $\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha$. □

Corollaire 9. $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle f_1, ..., f_s \rangle}$ *est un $\mathbb{C}$-espace vectoriel dont la dimension est le nombre de zéros de $\langle f_1, ..., f_s \rangle$ comptés avec multiplicités, soit* $\dim_{\mathbb{C}}\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle f_1, ..., f_s \rangle}\right) = \sum_{\alpha \in V(f_1, ..., f_s)} \mu(\alpha)$.

1.5. Zéros de polynômes comme valeurs propres

Théorème 10. *Soient $f \in \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ et $M_f : \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle} \to \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ t.q. $M_f(g) = f\,g$.*

Alors, pour tout $\alpha \in V(\mathcal{E})$:

- $M_f\left(\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha\right) \subset \left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha$

- *M_f restreint à $\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)_\alpha$ a comme unique valeur propre $f(\alpha)$*

Démonstration. (Voir TD) □

Une application directe de ce théorème est le calcul effectif de toutes les premières coordonnées des zéros d'un système à coefficients rationnels. En effet, en calculant une base de Gröbner G de $\langle \mathcal{E} \rangle$ pour un ordre monomial $>$ arbitraire, on peut calculer explicitement

- une base de monômes $\mathcal{B} = \{w_1, ..., w_D\}$ de $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$: on calcule tous les monômes m tels que $\text{Reduction}_>(m, G) = m$) de sorte à pouvoir exprimer toute classe d'élément $\overline{p} \in \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ comme un vecteur dans cette base que l'on notera $\vec{p}^{\mathcal{B}}$.
- la matrice de M_{X_1}: $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle} \to \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ exprimée dans la base $\mathcal{B}$ qui est constituée des vecteurs colonnes $\overrightarrow{X_1 w_i}^{\mathcal{B}}$. Remarquons au passage que si $\mathcal{E} \subset \mathbb{Q}[X_1, ..., X_n]$ alors M_{X_1} est à coefficients rationnels.
- calculer les valeurs propres de M_{X_i} ou alors son polynôme caractéristique (à coefficients rationnels lui aussi si $\mathcal{E} \subset \mathbb{Q}[X_1, ..., X_n]$) puis en isoler les zéros par exemple.

Corollaire 11. *Soient $f \in \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ et M_f: $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle} \to \frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ t.q. $M_f(g) = fg$. Alors*

- $\text{Trace}(M_f) = \sum_{\alpha \in V(\mathcal{E})} \mu(\alpha) f(\alpha)$ *et en particulier*
  $\text{Trace}(M_1) = \sum_{\alpha \in V(\mathcal{E})} \mu(\alpha) = \dim_{\mathbb{C}}\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$
- $\text{Det}(M_f) = \prod_{\alpha \in V(\mathcal{E})} f(\alpha)^{\mu(\alpha)}$ *et en particulier vaut* 0 *si et seulement si* $\exists \alpha \in V(\mathcal{E}), f(\alpha) = 0$
- $\text{Polchar}(M_f) = \prod_{\alpha \in V(\mathcal{E})} (T - f(\alpha))^{\mu(\alpha)}$ *et en particulier* $\text{Polchar}(M_{X_1})$ *a pour racines toutes les premières coordonnées de tous les zéros de* $\mathcal{E} = 0$.

1.6. Compter le nombre de zéros

Théorème 12. *On définit la forme quadratique q_1: $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle} \to \mathbb{C}$ telle que $q_1(f) = \text{Trace}(M_{f^2})$. Alors* $\text{rang}(q_1) = \sharp V(\mathcal{E})$.

Démonstration. (Voir TD) □

Remarque 13. Si $I \subset \mathbb{Q}[X_1, ..., X_n]$, on peut définir q_1: $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle} \to \mathbb{C}$ telle que $q_1(f) = \text{Trace}(M_{f^2})$ et on aura alors $\text{rang}(q_1) = \sharp V_{\mathbb{C}}(\mathcal{E})$ avec $V_{\mathbb{C}}(I) = \{\alpha \in \mathbb{C}^n, f(\alpha) = 0, \forall f \in \langle \mathcal{E} \rangle\}$

1.7. Paramétrisations rationnelles

L'objectif ici est de représenter les zéros d'un système zéro-dimensionnel au moyen de polyômes en une seule variable, sans perdre d'information.

On aimerait par exemple trouver des polynômes $h_0, h_1, ..., h_n \in \mathbb{C}[U]$ tels que $h_0(U) = 0$, $X_1 = h_1(U), ..., X_n = h_n(U)$.

C'est parfois possible par de simples manipulations algébriques.

Par exemple si tous les éléments de $V(\mathcal{E})$ sont de multiplicité 1, on peut se donner une forme séparante U auquel cas $1, ..., U^{d-1}$ sera une famille libre de $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ et donc une base de $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ puisque dans ce cas $d = \sum_{\alpha \in V(\mathcal{E})} = \sum_{\alpha \in V(\mathcal{E})} \mu(\alpha) = \dim_{\mathbb{C}}\left(\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}\right)$. Il ne reste plus qu'à exprimer la classe de X_1 puis $X_2, ..., X_n$ dans $\frac{\mathbb{C}[X_1, ..., X_n]}{\langle \mathcal{E} \rangle}$ en utilisant cette base pour trouver les polynômes $h_0, ..., h_n$ désirés.

C'est généralement toutefois impossible par de simples manipulations algébriques qui préserveraient $\frac{\mathbb{C}[X_1,...,X_n]}{\langle\mathcal{E}\rangle}$. En effet, il n'existe en général pas de polynôme permettant de trouver un isomorphisme de $\frac{\mathbb{C}[X_1,...,X_n]}{\langle\mathcal{E}\rangle} \to \frac{\mathbb{C}[U]}{\langle h_0\rangle}$.

Par exemple posons $n=2$ et $\mathcal{E}=\{f_1=X_1^2,\ f_2=X_1\ X_2,\ f_3=X_2^2\}$. On peut voir que $V(\mathcal{E})=\{(0,0)\}$.

On remarque que les éléments de $\frac{\mathbb{C}[X_1,...,X_n]}{\langle\mathcal{E}\rangle}$ s'écrivent sous la forme $a\,X_1+b\,X_2+c$ avec $a,b,c\in\mathbb{C}$, $\frac{\mathbb{C}[X_1,...,X_n]}{\langle\mathcal{E}\rangle}$ est un espace vectoriel de dimension 3 sur $\mathbb{C}$, donc $\{(0)\}$ est de multiplicité 3.

En particulier, si h_0 existe, il est forcément de degré 3 pour que $\frac{\mathbb{C}[U]}{\langle h_0\rangle}$ soit de dimension 3.

Supposons qu'il existe un isomorphisme $\phi\colon \frac{\mathbb{C}[X_1,...,X_n]}{\langle\mathcal{E}\rangle} \to \frac{\mathbb{C}[U]}{\langle h_0\rangle}$ et soit $a\,X_1+b\,X_2+c$ l'antécédent de U par ϕ. On a alors $\phi(a\,X_1+b\,X_2+c)=U$ et $\phi((a\,X_1+b\,X_2+c)^2)=U^2=2\,c\,\phi(a\,X_1+b\,X_2+c)-c^2=2\,c\,U-c^2$ ce qui implique que $U^2-2\,c\,U-c^2=0$ et contredit donc le fait que ϕ est surjective.

Définition 14. *Soient $I\subset\mathbb{Q}[X_1,...,X_n]$ supposé zéro-dimensionnel et $t\in\mathbb{Q}[X_1,...,X_n]$. On note $V_{\mathbb{C}}(I)=\{\alpha\in\mathbb{C}^n, f(\alpha)=0, \forall f\in I\}$ et on pose :*

- $f_t(T):=\prod_{\alpha\in V_{\mathbb{C}}(I)}(T-t(\alpha))^{\mu(\alpha)}$
- *pour tout $v\in\mathbb{Q}[X_1,...,X_n]$* $g_{t,v}(T)=\sum_{\alpha\in V_{\mathbb{C}}(I)}\mu(\alpha)v(\alpha)\prod_{y\neq t(\alpha),\,y\in\mathbb{V}_{\mathbb{C}}(I)}(T-t(y))$

Théorème 15. *Avec les notations de la définition précédente:*

i. Le polynôme f_t est à coefficients rationnels et on note $H_d=\sum_{i=0}^{d}a_i\,T^{d-i}=\prod_{\alpha\in V_{\mathbb{C}}(I)}(T-t(\alpha))$ sa partie sans facteurs carrés.

ii. $g_{t,v}(T)=\sum_{i=0}^{d-1}\mathrm{Trace}(M_{vt^i})\,H_{d-i-1}(T)$ avec $H_j(T)=\sum_{i=0}^{j}a_i\,T^{j-i}$, ce qui implique que $g_{t,v}(T)\in\mathbb{Q}[T]$

iii. Si de plus t sépare $V(I)$,

$$\begin{array}{rccc} \phi\colon & V_{\mathbb{C}}(I) & \to & V_{\mathbb{C}}(f_t) \\ & (\alpha_1,...,\alpha_n) & \hookrightarrow & t(\alpha_1,...,\alpha_n) \\ & \left(\frac{g_{t,X_1(T)}}{g_{t,1}(T)},...,\frac{g_{t,X_n(T)}}{g_{t,1}(T)}\right) & \hookleftarrow & \beta \end{array}$$

est une bijection préservant les multiplicités et les zéros à coordonnées réelles.

Démonstration.

i. On remarque simplement que f_t est le polynôme caractéristique de M_t qui est à coefficients rationnels.

ii. $\frac{g_{t,v}(T)}{H_d(T)}=\sum_{\alpha\in V_{\mathbb{C}}(I)}\frac{\mu(\alpha)\,v(\alpha)}{T-t(\alpha)}=\sum_{I\geqslant 0}\frac{\sum_{\alpha\in V_{\mathbb{C}}(I)}\mu(\alpha)\,v(\alpha)\,t^i(\alpha)}{T^{i+1}}=\sum_{I\geqslant 0}\frac{\mathrm{Trace}(M_{vt^i})}{T^{i+1}}$.

Ainsi, $g_{t,v}(T)=\left(\sum_{I\geqslant 0}\frac{\mathrm{Trace}(M_{vt^i})}{T^{i+1}}\right)(\sum_{i=0}^{d}a_i\,T^{d-i})=\sum_{i=0}^{d-1}\mathrm{Trace}(M_{vt^i})\,H_{d-i-1}(T)$, en tenant compte du fait que les termes de droite et de gauche sont des polynômes de degré au plus $d-1$.

iii. $\frac{g_{t,v}(t(\alpha))}{g_{t,v}(t(\alpha))}=\frac{\left(\sum_{\beta\in V_{\mathbb{C}}(I),t(\beta)=t(\alpha)}\mu(\beta)\,v(\beta)\right)\left(\prod_{y\in t(V_{\mathbb{C}}(I))\setminus t(\alpha)}(t(\alpha)-y)\right)}{\left(\sum_{\beta\in V_{\mathbb{C}}(I),t(\beta)=t(\alpha)}\mu(\beta)\right)\left(\prod_{y\in t(V_{\mathbb{C}}(I))\setminus t(\alpha)}(t(\alpha)-y)\right)}=\frac{\sum_{\beta\in V_{\mathbb{C}}(I),t(\beta)=t(\alpha)}\mu(\beta)\,v(\beta)}{\sum_{\beta\in V_{\mathbb{C}}(I),t(\beta)=t(\alpha)}\mu(\beta)}$

En particulier, si t sépare $V_{\mathbb{C}}(I)$, $\frac{g_{t,v}(t(\alpha))}{g_{t,v}(t(\alpha))}=v(\alpha)$. Ceci montre le bijection et le point i) montre la préservation des multiplicités. La préservation du caractère réel des racines est conséquence directe du fait que tous les polynômes sont à coefficients rationnels. □