# Thèse

présentée à

L'Université de la Méditerranée
Faculté des sciences de Luminy

Ecole doctorale Mathématiques et Informatique de Marseille

pour obtenir le titre de

**DOCTEUR**

Spécialité : Mathématiques-Informatique

# Dualité algébrique, structures et applications

par Olivier Ruatta

Soutenue le Lundi 23 septembre 2002 devant le jury composé de :

| | | | |
|---|---|---|---|
| Mme. Alicia | Dickenstein | Professeur | Rapporteur |
| Mr. Laureano | Gonzalez-Vega | Professeur | Rapporteur |
| Mr. Roger | Marlin | Professeur | Président |
| Mr. Bernard | Mourrain | Chargé de recherches | Directeur |
| Mr Robert | Rolland | Maître de Conférences | |
| Mr. Bruno | Salvy | Directeur de recherches | |
| Mr. Jean-Claude | Yakoubsohn | Professeur | |

# Remerciements

Tout d'abord, je voudrais remercier Bernard Mourrain. Il a su me guider et je l'espère m'insuffler sa grande ouverture d'esprit et son insatiable curiosité intellectuelle. De plus, il a été mon principal interlocuteur et collaborateur. Il a su me consacrer du temps malgré des situations parfois difficiles. J'ai largement profité de son dynamisme, mais aussi de celui de toute l'équipe GALAAD. Je tiens particulièrement à remercier Ioannis Emiris, auprès de qui j'ai trouvé des conseils avisés et une présence très rassérénante. J'ai scientifiquement beaucoup profité de lui, mais aussi de Mohamed Elkadi à qui je dois la plupart des choses que j'ai comprise sur cet encore mystérieux et omniprésent résidu algébrique. Merci aussi à André Galligo pour ses conseils.

Au cours d'un séjour d'un mois en Argentine, j'ai largement vampirisé l'attention et les connaissances de Alicia Dickenstein, qui me fait de plus le très grand honneur d'être rapporteur de cette thèse. Je lui suis redevable d'un nombre incalculable de corrections au texte initial. Je suis également très honoré que Loreano Gonzalez-Vega ait accepté d'être rapporteur de cette thèse, lui qui a beaucoup contribué aux sujets auxquels je me suis intéressé dans le texte.

Jean-Claude Yakoubsohn aura suivi mes travaux pratiquement depuis le début. C'est par lui que sont venues certaines idées comme celle de prendre un "système par les racines" ou l'utilisation d'algorithmes de suivi de racines utilisant l'itération de Weierstrass comme opérateur de correction. Pour cela, ses remarques toujours constructives et sa présence dans le jury : merci ! Merci aussi à Bruno Salvy, sa présence dans ce jury est importante à mes yeux. Bien que je n'aie jamais discuté directement avec lui, j'ai eu vent de ces idées par "des petits jeunes" qui ont confirmé l'impression que j'eue en lisant certains de ses travaux qu'il est un "algorithmiste" très complet. Enfin merci à Roger Marlin de présider ce jury, j'en suis très honoré à plus d'un titre.

Je dois encore remercier un ensemble de scientifiques qui n'ont beaucoup

apporté : l'équipe de calcul formel de Limoges et en particulier Anne Bellido (ce nom reviendra souvent dans le texte) qui a consacré du temps à mes questions bien qu'elle ait beaucoup d'obligations par ailleurs. Merci aussi à Marc Guisti, Eric Schost et Grégoire Lecerf pour leur invitation et nos discussions. J'espère qu'elles continueront car j'ai déjà beaucoup appris auprès d'eux. Je tiens à faire un clin d'œil à Alin Bostan qui nous a rendu visite et qui m'a fait découvrir quelques travaux autour de l'interpolation rationnelle. Je lui souhaite toute la réussite possible sur son sujet de thèse, mais sur d'autres également. Je remercie Marie-Françoise Roy, pour plusieurs raisons, mais principalement pour son soutien afin que je participe au cours "niveau 2" organisé à Ouessant donné par Alain Lascoux. Que ce dernier me permette de le remercier pour la bonne raison que j'ai beaucoup appris en l'écoutant. J'ai également abusé de la patience de Fernando Cukierman, Jorge Vitorio Peirera, Jaques-Arthur Weil, Evelyne Hubert, Manuel Bronstein, Emmanuel Briand. Un grand merci à Victor Pan ; il est inutile de souligner son influence sur mon travail... Merci aussi à Mark Van Barel et Raf Vandebril de qui j'ai appris l'algorithme de Bultheel-Van Barel.

Merci à Monique et à Aurélie. Je remercie aussi mes petits camarades de thèse : Didier Bondyfalat, l'inimitable Philippe Trébuchet, Laurent Busé et les p'tits nouveaux : Guillaume, Jean-Pascal et Jean-Pierre. Leurs conversations sont toujours enrichissantes (ou presque toujours). Merci aussi à Sebastien pour les moult discussions après saturation de boulot.

J'ai le plaisir de remercier Jean-Luc Villevieille et Gérard Chauvel pour la chance qu'ils m'ont donnée de faire des stages au sein de Texas-Instruments au cours de mes études. J'ai beaucoup appris au cours de ces stages.

Merci à mes parents et grands-parents pour leur affection et leur soutien. Je ne pourrais jamais les remercier comme je m'imagine devoir le faire. Je dois aussi beaucoup à Michèle et Alain, je leur exprime ici toute ma reconnaissance et mon amitié.

Je dois aussi de fières chandelles à mes vieux amis : la bella Béa, Cathy, Yan, Nono et à Nausica et Vincent dont j'espère qu'ils continuerons tous à cultiver le seul grain qui vaille.

Je ne pourrais pas non plus remercier Karine comme je l'aimerais pour sa patience, son affection et surtout pour tout le bonheur qu'elle m'offre.

# Table des matières


**1 Introduction 9**

**2 Algèbre de dimension 0 et dualité 13**

2.1 Introduction . . . 13
2.2 Algèbre quotient . . . 14
2.3 Orthogonalité et dualité . . . 17
2.3.1 Opérateurs différentiels et dualité . . . 17
2.3.2 Orthogonalité . . . 19
2.4 Représentation et interpolation . . . 23
2.4.1 Introduction . . . 23
2.4.2 Cas des racines simples . . . 25
2.4.3 Cas de racines multiples . . . 28
2.4.4 Polynômes de relation . . . 31
2.4.5 Relations entre racines et coefficients . . . 33
2.4.6 Application des polynômes de relation à l'interpolation 34
2.5 Deux autres problèmes d'interpolation . . . 35
2.5.1 Restriction d'idéaux . . . 35
2.5.2 Configurations de points et restrictions d'idéaux . . . 37
2.6 Conclusion . . . 40

**3 Approximation simultanée 41**

3.1 Introduction . . . 41
3.2 Méthodes univariées . . . 43
3.2.1 La méthode de Weierstrass univariée . . . 43
3.2.2 L'approche de Frommer-Bellido . . . 45
3.3 Méthodes multivariées . . . 47
3.3.1 Méthode de Weierstrass . . . 47
3.3.2 Méthode de Aberth . . . 51
3.4 Fonction d'itération de Gauss-Weierstrass . . . 54

3.4.1 Calcul de la fonction d'itération . . . . . . . . . . . . . 54
3.5 Méthode de Weierstrass modifiée . . . . . . . . . . . . . . . . 58
3.5.1 Cas univarié . . . . . . . . . . . . . . . . . . . . . . . . 58
3.5.2 Cas multivarié . . . . . . . . . . . . . . . . . . . . . . . 64
3.5.3 Méthode de Gauss-Weierstrass modifiée . . . . . . . . 66
3.6 Expérimentations . . . . . . . . . . . . . . . . . . . . . . . . . 70
3.6.1 Implémentation . . . . . . . . . . . . . . . . . . . . . . 70
3.6.2 Expériences numériques . . . . . . . . . . . . . . . . . 71
3.6.3 Conclusions . . . . . . . . . . . . . . . . . . . . . . . . 73
3.7 Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . 73

**4 Bézoutiens et résidus 75**
4.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . 75
4.2 Algèbres de Gorenstein . . . . . . . . . . . . . . . . . . . . . . 75
4.2.1 Retour sur la dualité locale . . . . . . . . . . . . . . . 75
4.2.2 Algèbres de Gorenstein . . . . . . . . . . . . . . . . . . 77
4.2.3 Représentation des algèbres de Gorenstein . . . . . . . 79
4.2.4 Lien avec les systèmes inverses à la Macaulay . . . . . 82
4.2.5 Suites régulières, quasi-régulières et théorème de Wiebe 83
4.3 Bézoutiens . . . . . . . . . . . . . . . . . . . . . . . . . . . . 84
4.3.1 Les bézoutiens : introduction . . . . . . . . . . . . . . 84
4.3.2 Cas des polynômes d'une variable . . . . . . . . . . . . 85
4.3.3 Bézoutiens : cas multivarié . . . . . . . . . . . . . . . . 86
4.4 Résidus algébriques . . . . . . . . . . . . . . . . . . . . . . . 92
4.4.1 Lois de transformation . . . . . . . . . . . . . . . . . . 98
4.4.2 Résidu et résolution . . . . . . . . . . . . . . . . . . . 99
4.4.3 Bézoutiens, systèmes inverses, résidus et formes normales 102
4.5 Calcul des résidus . . . . . . . . . . . . . . . . . . . . . . . . 104
4.5.1 Algorithme de calcul des résidus dans un cas simple . 104
4.5.2 Algorithme de calcul des résidus multivariés . . . . . . 105
4.5.3 Application à l'implicitisation . . . . . . . . . . . . . . 107
4.6 Bézoutien et implicitisation . . . . . . . . . . . . . . . . . . . 115

**5 Matrices structurées et dualité 119**
5.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . 119
5.2 Matrices structurées usuelles . . . . . . . . . . . . . . . . . . 122
5.2.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . 122
5.2.2 Structures classiques . . . . . . . . . . . . . . . . . . . 122
5.2.3 Liens entre les structures Hankel et bézoutienne . . . . 127
5.3 Matrices structurées et polynômes . . . . . . . . . . . . . . . 128

5.3.1 Matrices quasi-Toeplitz et quasi-Hankel . . . . . . . . . 129
5.3.2 Arithmétique dans une algèbre quotient . . . . . . . . . 131
5.3.3 Bases duales pour $\tau$ . . . . . . . . . . . . . . . . . . . . 134
5.3.4 Produit dans $\mathcal{A}$ . . . . . . . . . . . . . . . . . . . . . . . 135
5.3.5 Inversion dans $\mathcal{A}$ . . . . . . . . . . . . . . . . . . . . . . 135
5.3.6 Méthodes itératives . . . . . . . . . . . . . . . . . . . . . 136
5.3.7 Compter et approximer les racines réelles et complexes 140

**6 Conclusion** **143**

**Bibliographie** **144**

# Chapitre 1

# Introduction

Cette thèse est consacrée aux outils de dualité algébrique ainsi qu'à leurs applications en géométrie algébrique effective (par ce dernier terme on entend le traitement algorithmique d'objets de la géométrie algébrique). Les deux types d'objets qui seront au cœur de cette thèse sont les quotients des algèbres de polynômes et les ensembles algébriques, plus particulièrement ceux de dimension zéro. Théoriquement ce sont les ensembles algébriques les plus simples. Mais ils constituent un contexte très riche auquel on se ramène systématiquement. Pratiquement, ces ensembles apparaissent dans un nombre considérable d'applications puisque les polynômes sont des outils de modélisation courants. On peut citer les domaines d'applications suivants : la conception assistée par ordinateur, la robotique, le traitement du signal, la cryptologie, la chimie moléculaire et bien d'autres encore. Le calcul avec des ensembles algébriques de dimension zéro est un problème très étudié et connu pour être un problème informatique difficile.

Nous distinguons deux approches pour résoudre ce problème : le calcul formel (ou symbolique) et l'analyse numérique. Dans ces deux branches, des travaux très avancés existent. Il est impossible de résumer ces deux approches en quelques lignes. On peut néanmoins essayer de les caractériser grossièrement :

- Le calcul formel traite les polynômes (ou des objets plus complexes) comme des expressions. On traduit alors informatiquement les opérations que les mathématiciens utilisent sur ces objets sous forme d'algorithmes. Au sein de cette branche, plusieurs méthodes différentes co-existent. Elles ne traitent pas exactement les mêmes problèmes en fait, ce qui rend la comparaison difficile. Toutes ces méthodes ont en commun de ne considérer que des opérations exactes sur les objets traités. Ceci implique, par exemple, que le système qu'on traite est connu de manière exacte. Trois approches principales se détachent : le traitement par réécriture (bases de Gröbner [20, 42, 43], formes normales [74, 81], ... ) , les méthodes basées sur les résultants ([93, 66, 23, 40]) et le traitement des polynômes comme des fonctions (résolution géométrique [50, 51, 52]). Généralement les méthodes issues de ces approches se décomposent en deux parties distinctes. Dans un premier temps on cherche à donner une représentation exacte (comme une base de Gröbner ou une représentation géométrique) plus riche que le système de départ, puis on cherche à exploiter l'information calculée pour donner une représentation des solutions du système (comme une représentation univariée rationnelle) permettant de donner des approximations explicites des solutions.

- L'analyse numérique considère les polynômes comme des fonctions. On utilise alors des méthodes numériques, comme la méthode de Newton, pour chercher les zéros de ces fonctions [89, 95, 96, 67, 17]. Ces méthodes sont plus tolérantes aux erreurs sur les coefficients des polynômes donnés au départ. Mais elles ne tiennent en général pas compte de toute l'information due au fait qu'on traite des systèmes algébriques.

Les deux approches ont leurs avantages et leurs inconvénients propres. Mais il demeure que les systèmes algébriques sont des systèmes difficiles à traiter informatiquement dans toute leur généralité. On ne peut en effet pas toujours représenter des nombres réels ou complexes par des mots machines ou des programmes simples permettant de les calculer avec la précision voulue. Autrement dit, certains objets ne peuvent être représentés que par des approximations (pas forcement numériques). Cela entraîne des difficultés pour chacune des approches. Mais même si nous savions calculer avec des nombres réels, nous ne saurions pas si le problème serait plus simple numériquement [17]. Il n'y a donc rien d'étonnant à ce qu'on trouve le problème de la résolution des équations algébriques au sommet de la hiérarchie de complexité de la plupart des modèles de calcul.

Notre point de vue consiste à tirer profit des points forts des deux approches, symbolique et numérique. Notre outil de base est la dualité algébrique, c'est-à-dire l'étude de l'ensemble des formes linéaires sur une algèbre. A travers la structure du dual d'une algèbre, on exploite l'information qu'on peut tirer sur l'algèbre elle-même. Pour les intersections complètes par exemple, une forme linéaire particulière (le résidu algébrique) suffit à obtenir une quantité considérable d'informations sur l'algèbre et par là même sur les solutions d'un système algébrique. On admettra éventuellement qu'on dispose d'informations partielles sur l'algèbre quotient. Cette information peut être obtenue à partir d'un pré-calcul ou de connaissances particulières sur le système qu'on veut résoudre. Des travaux récents étudient les différences et les points communs de certaines approches [28].

Des travaux existent déjà sur l'approche symbolique-numérique ([45, 90, 95, 82, 78, 40, 94, 6, 9, 10, 24, 25, 26, 29, 44, 48, 70] sans pouvoir être exhaustif). Notre approche consiste à utiliser la structure algébrique pour mettre en œuvre des méthodes itératives (comme la méthode de Newton). Cette approche avait déjà été exploitée dans [9, 10, 25, 26, 78]. Ce sont sur ces travaux que nous nous sommes basés.

Dans un premier chapitre, nous nous intéressons aux représentations des algèbres quotients de dimension zéro. Cela nous conduit naturellement à considérer des problèmes d'interpolation que nous traitons complètement. Nous donnons des formules explicites pour les idempotents (qui sont les analogues multivariés des polynômes de Lagrange) d'une algèbre quotient réduite ou non. Ce cadre théorique nouveau nous permet d'exprimer les relations entre coefficients et racines d'un système algébrique. Nous étudions ensuite les conséquences de ces relations pour la génération de systèmes définissant un ensemble algébrique donné (non nécessairement une intersection complète). D'un point de vue pratique, ces formules jouent un rôle important dans les procédés d'évaluation-interpolation nécessaires aux méthodes itératives du deuxième chapitre. Les résultats de ce chapitre on été partiellement publiés en commun avec Bernard Mourrain dans [80].

Dans un deuxième chapitre, nous utilisons les outils développés au premier chapitre pour construire des méthodes itératives pour le calcul simultané de toutes les solutions d'un système algébrique. Nous étendons ainsi les travaux de Anne Bellido sur la méthode de Weierstrass (aussi appelée méthode de Durand-Kerner ou de Dochev). Nous obtenons une formule close pour les systèmes définissant une intersection complète. Nous généralisons cette fonction d'itération pour le cas surcontraint sans toutefois avoir de formule close dans ce cas. On obtient ainsi des méthodes itératives dont la convergence locale est quadratique. On utilise alors ces fonctions d'itération comme opérateurs de correction dans des procédés de suivi de chemins afin d'obtenir des méthodes globales. Nous proposons des expérimentations numériques illustrant l'effectivité de ces méthodes. Ces travaux sont partiellement publiés dans [85] et [80].

Le troisième chapitre est consacré aux algèbres de Gorenstein et à leurs représentations. On y introduit les notions de bézoutien et de résidu algébrique. On décrit ensuite l'algorithme de Mohamed Elkadi et Bernard Mourrain pour calculer le résidu algébrique d'une intersection complète. On expose alors une application, développée en commun avec ces deux auteurs, au calcul de l'équation implicite d'une surface rationnelle donnée sous forme paramétrique. Cette approche suit les travaux de Laureano González-Vega et Guadalupe Trujillo dans [55], [54] et [56], qui reprenaient les travaux de Alexander Kytmanov, L. A. Aizenberg [1] et Tsikh [91].

Dans le quatrième chapitre, nous exposerons un travail commun avec Victor Pan et Bernard Mourrain sur l'utilisation des outils de dualité et ses liens avec les matrices structurées pour concevoir des algorithmes itératifs pour compter ou approximer des racines d'un système algébrique. Ces travaux font suite à l'article de Victor Pan et Bernard Mourrain [78] et améliorent la complexité des méthodes itératives décrites. Ces travaux sont publiés dans [83].

# Chapitre 2

# Algèbre de dimension 0 et dualité

## 2.1 Introduction

Ce chapitre concerne la représentation des algèbres des coordonnées des ensembles algébriques de dimension zéro sur le corps des nombres complexes, c'est-à-dire des ensembles algébriques finis. Par extension nous dirons que ces algèbres sont de dimension zéro. Notre approche trouve ses sources dans le travail de Macaulay au début du vingtième siècle. On utilisera beaucoup de notions déjà présentes dans le travail de cet auteur comme les systèmes inverses. Le travail initié par Macaulay a été développé par différents auteurs au cours du temps, mais il a suscité un regain d'intérêt avec le développement de l'algorithmique des mathématiques comme en témoigne l'intérêt renouvelé pour les méthodes de calcul des résultants par exemple. La théorie des systèmes inverses a été reprise par J. Emsalem [41] et plus récemment par B. Mourrain [73]. Elle nous fournit un cadre efficace pour l'étude de la dualité des algèbres de dimension zéro. Elle permet par exemple de prendre en compte de manière synthétique des informations comme la multiplicité d'un point d'une variété. Notre contribution essentielle est l'application de ce formalisme pour la représentation permettant de concevoir des méthodes d'interpolation. Nous généralisons ainsi l'interpolation de Lagrange et de Hermite sous un angle algébrique. Notre approche complète les travaux d'auteurs comme De Boor [33, 69, 65, 64] qui se sont beaucoup intéressés à l'interpolation algébrique. Notre approche est cependant plus algébrique. Notre point de vue apporte ainsi des résultats nouveaux dans ce domaine. Le lien entre la représentation s'appuyant sur la dualité et l'interpolation vient du fait que souvent la dualité consiste à supposer les points de la variété connus, les évaluations aux points de la variété étant des formes linéaires très particulières.

Les représentations des algèbres de dimension zéro que nous développons permettent d'obtenir beaucoup d'informations. Ainsi nous donnons les relations entre les coefficients d'un système algébrique définissant une variété de dimension zéro et les coordonnées des solutions de ce système. Ces relations généralisent directement les relations connues entre les racines d'un polynôme et ses coefficients en termes de fonctions symétriques élémentaires.

La plupart des résultats exposés dans ce chapitre ont fait l'objet d'une partie d'une publication en collaboration avec Bernard Mourrain [80] et dans [85].

Le chapitre est organisé comme suit : dans une première section nous rappelons des résultats algébriques sur la décomposition des idéaux et celle des algèbres quotients. Nous introduisons ensuite les notions d'orthogonalité et de dualité. Dans une troisième section nous utilisons les résultats des deux sections précédentes pour donner des résultats sur la représentation des algèbres de dimension zéro en mettant l'accent sur les liens qu'entretient cette théorie avec l'interpolation. Nous nous intéressons enfin à de nouveaux problèmes d'interpolation qui nous seront utiles par la suite avant de conclure.

## 2.2 Algèbre quotient

Dans cette section nous introduisons le matériel algébrique qui nous sera nécessaire par la suite. C'est aussi l'occasion de fixer un certain nombre de notations. Les résultats de ce chapitre ne sont pas nouveaux, mais leur usage est important pour le développement du formalisme que nous utilisons. Il s'agit essentiellement de résultats de décomposition des algèbres de dimension zéro.

Dans toute la suite, $\mathbb{K}$ représente un corps de caractérisque nulle et $\overline{\mathbb{K}}$ sera sa clôture algébrique. Certains des résultats que nous donnons restent valables en dehors de ce cadre, mais pour la simplicité de l'exposé, nous nous limiterons à ce cadre. Globalement, nous pensons à $\mathbb{R}$ ou $\mathbb{C}$ pour le corps $\mathbb{K}$ bien que nous utilisions toujours $\mathbb{Q}$ ou une de ses extensions finies en pratique (ce sont les corps pour lesquels on sait représenter les éléments et faire des opérations effectives). On pensera à $\mathbb{C}$ pour $\overline{\mathbb{K}}$ bien qu'on ne sache bien sûr traiter effectivement que des extensions finies de $\mathbb{Q}$. On note $\mathbb{K}[x]$ (resp. $\overline{\mathbb{K}}[x]$) l'anneau des polynômes de la variable $x$ à coefficients dans $\mathbb{K}$ (resp. $\overline{\mathbb{K}}$) et $\mathbb{K}[x_1,\ldots,x_n]$ (resp. $\overline{\mathbb{K}}[x_1,\ldots,x_n]$) celui des polynômes des variables $x_1, \dots, x_n$ à coefficients dans $\mathbb{K}$ (resp. $\overline{\mathbb{K}}$).

Soient $f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n]$, on note $\mathcal{I}$ l'idéal qu'ils engendrent. On note $\mathcal{A} = \mathbb{K}[x_1, \dots, x_n]/\mathcal{I}$ l'anneau quotient de $\mathbb{K}[x_1, \dots, x_n]$ par l'idéal $\mathcal{I}$. On note $\mathcal{Z}_{\overline{\mathbb{K}}}(\mathcal{I}) = \left\{\mathbf{z} \in \overline{\mathbb{K}}^n \mid g(\mathbf{z}) = 0\,,\, \forall g \in \mathcal{I}\right\} = \left\{\mathbf{z} \in \overline{\mathbb{K}}^n \mid f_i(\mathbf{z}) = 0,\ \forall i \in \{1, \dots, m\}\right\} = \mathcal{Z}(\mathcal{I})$. On dit que $\mathcal{A}$ est l'anneau des coordonnées de $\mathcal{Z}(\mathcal{I})$. Dans toute la suite de ce chapitre, nous admettrons l'hypothèse suivante :

**Hypothèse 2.2.1** *On suppose que $\mathcal{Z}(\mathcal{I})$ est un ensemble fini $\{\zeta_1, \dots, \zeta_d\}$.*

**Proposition 2.2.2** *Sous l'hypothèse 2.2.1, l'idéal $\mathcal{I}$ est dit zéro-dimensionnel et il admet la décomposition primaire minimale suivante : $\mathcal{I} = Q_{\zeta_1} \cap \dots \cap Q_{\zeta_d}$ où $Q_{\zeta_i}$ est $\mathbf{m}_{\zeta_i}$ primaire et $\mathbf{m}_{\zeta_i}$ est l'idéal maximal associé à $\zeta_i$.*

*Preuve :* Voir [5] ou [30].♣

**Décomposition de l'anneau quotient**

On note $\mathcal{A}_{\zeta_i} = ((0) : Q_{\zeta_i}/\mathcal{I})$ (i.e. $\mathcal{A}_{\zeta_i} = \{a \in \mathcal{A} \mid aq = 0\,,\, \forall q \in Q_{\zeta_i}\}$). C'est un idéal de $\mathcal{A}$. Du fait que $Q_{\zeta_i}$ est $\mathbf{m}_{\zeta_i}$-primaire, on a la proposition suivante :

**Proposition 2.2.3** *L'algèbre $\mathcal{A}$ est la somme directe des sous-algèbres $\mathcal{A}_{\zeta_1}, \dots, \mathcal{A}_{\zeta_d}$, i.e. $\mathcal{A} = \mathcal{A}_{\zeta_1} \oplus \dots \oplus \mathcal{A}_{\zeta_d}$.*

*Preuve :* On a $\mathcal{A}_{\zeta_1} + \ldots + \mathcal{A}_{\zeta_d} = ((0) : Q_{\zeta_1}/\mathcal{I}) + \dots + ((0) : Q_{\zeta_d}/\mathcal{I}) = ((0) : (Q_{\zeta_1} \cap \dots \cap Q_{\zeta_d})/\mathcal{I}) = \mathcal{A}$. Il ne reste plus qu'à montrer que la somme est directe. Soit alors $i \in \{1, \dots, d\}$, on a :

$$\begin{gathered}\mathcal{A}_{\zeta_{i+1}} \cap (\mathcal{A}_{\zeta_1} + \ldots + \mathcal{A}_{\zeta_i}) \\ = \\ ((0) : Q_{\zeta_{i+1}}/\mathcal{I}) \cap (((0) : Q_{\zeta_1}/\mathcal{I}) + \dots + ((0) : Q_{\zeta_i}/\mathcal{I})) \\ = \\ ((0) : (Q_{\zeta_{i+1}} + (Q_{\zeta_1} \cap \dots \cap Q_{\zeta_i}))/\mathcal{I}) = ((0) : \mathcal{A}) = 0.\end{gathered}$$

Ainsi la somme est directe et la proposition est démontrée. ♣

**Définition 2.2.4** *La multiplicité de $\zeta_i \in \mathcal{Z}(\mathcal{I})$ est la dimension du sous-espace vectoriel $\mathcal{A}_{\zeta_i}$ de $\mathcal{A}$. On note $\mu_i$ cette dimension. Une racine est dite simple si $\mu_i = 1$ et multiple si $\mu_i > 1$.*

Avec les notations de la définition précédente, on a la proposition suivante :

**Proposition 2.2.5** *La dimension de $\mathcal{A}$ comme $\mathbb{K}$-espace vectoriel est le nombre de racines comptées avec multiplicité. C'est-à-dire que* $dim_{\mathbb{K}}\mathcal{A} = \sum_{i=1}^{d} \mu_i$.

La proposition suivante est l'analogue du théorème de partition de l'unité pour les ensembles algébriques de dimension zéro :

**Proposition 2.2.6** *Il existe un unique d-uplet* $(\mathbf{e}_{\zeta_1}, \ldots, \mathbf{e}_{\zeta_d}) \in \mathcal{A}_{\zeta_1} \times \cdots \times \mathcal{A}_{\zeta_d}$ *vérifiant les propriétés suivantes :*

- $\sum_{i=1}^{d} \mathbf{e}_{\zeta_i} = 1 \in \mathcal{A}$
- $\mathbf{e}_{\zeta_i}\mathbf{e}_{\zeta_j} = \delta_{i,j}\mathbf{e}_{\zeta_i} = \delta_{i,j}\mathbf{e}_{\zeta_j}$, *où $\delta_{i,j}$ représente le symbole de Kronecker*

**Définition 2.2.7** *Le d-uplet $(\mathbf{e}_1, \ldots, \mathbf{e}_d)$ vérifiant les propriétés de la proposition précédente est appelé le système fondamental d'idempotents. Les éléments $\mathbf{e}_i$ de ce d-uplet sont appelés des idempotents.*

Comme nous le verrons ultérieurement, la notion d'idempotent généralise celle de polynôme de Lagrange. Une propriété qu'il est facile d'énoncer dès maintenant est donnée par la proposition suivante :

**Proposition 2.2.8** *Les idempotents $\mathbf{e}_{\zeta_1}, \ldots, \mathbf{e}_{\zeta_d}$ de $\mathcal{A}$ vérifient $\mathbf{e}_{\zeta_i}(\zeta_j) = \delta_{i,j}$, pour tous les $i$ et $j \in \{1, \ldots, d\}$.*

*Preuve* : Pour $i$ et $j \in \{1, \ldots, d\}$ avec $i \neq j$, il existe $q \in Q_{\zeta_i}$ tel que $q(\zeta_j) \neq 0$. Sinon, il n'existe pas de tel polynôme et $Q_{\zeta_i} \subset \bigcup_{j \neq i} \mathbf{m}_{\zeta_j}$, ce qui implique que $Q_{\zeta_i} \subset \mathbf{m}_{\zeta_j}$ pour $i \neq j$. C'est en contradiction avec le fait que $Q_{\zeta_i}$ est $\mathbf{m}_{\zeta_i}$-primaire. Maintenant, comme $q\mathbf{e}_{\zeta_i} = 0$ (puisqu'il est inclus dans $Q_{\zeta_i}$), $q(\zeta_j)\mathbf{e}_{\zeta_i}(\zeta_j) = 0$ et donc $\mathbf{e}_{\zeta_i}(\zeta_j) = 0$. D'autre part, $1 = \mathbf{e}_{\zeta_1} + \cdots + \mathbf{e}_{\zeta_d}$ donc $1 = \mathbf{e}_{\zeta_1}(\zeta_i) + \cdots + \mathbf{e}_{\zeta_d}(\zeta_i) = \mathbf{e}_{\zeta_i}(\zeta_i)$, ce qui achève la preuve. ♣

**Proposition 2.2.9** *Pour tout $i \in \{1, \ldots, d\}$, on a $\mathcal{A}_{\zeta_i} = \mathcal{A}\mathbf{e}_{\zeta_i}$ et ainsi $\mathbf{e}_{\zeta_i}$ est l'élément unité de $\mathcal{A}_{\zeta_i}$.*

On sait que si $\mu_i > 1$, alors $\mathcal{A}_{\zeta_i}$ est un espace vectoriel de dimension $> 1$ et comme $\mathcal{A}_{\zeta_i} = \mathcal{A}\mathbf{e}_{\zeta_i}$, c'est un $\mathcal{A}$-module de rang 1. Pour avoir une meilleure compréhension de la structure de $\mathcal{A}_{\zeta_i}$ on considère la projection de $\mathcal{A}$ sur $\mathcal{A}_{\zeta_i}$ :

$$\Pi_{\zeta_i} = \left\{ \begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_{\zeta_i} \\ a & \longmapsto & a\mathbf{e}_{\zeta_i} \end{array} \right.$$

**Proposition 2.2.10** *$Ker(\Pi_{\zeta_i}) = \bigoplus_{j=1, j\neq i}^{d} \mathcal{A}_{\zeta_j} = Q_{\zeta_i}/\mathcal{I}$.*

*Preuve* : Cette proposition découle du fait que :
$\oplus_{j\neq i}^{d} \mathcal{A}_{\zeta_j} = \left( (\mathbf{0}) : \bigcap_{j\neq i} Q_{\zeta_j}/\mathcal{I} \right) = Q_{\zeta_i}/\mathcal{I}$. ♣

On identifie donc $\mathcal{A}_{\zeta_i}$ avec $\mathcal{A}/\mathrm{Ker}\,(\Pi_{\zeta_i})$. Mais comme $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ et $\mathrm{Ker}\,(\Pi_{\zeta_i}) = Q_{\zeta_i}/\mathcal{I}$, on a $\mathcal{A}_{\zeta_i} = \mathbb{K}[x_1, \ldots, x_n]/Q_{\zeta_i}$. Cette dernière égalité permet une bonne représentation de $\mathcal{A}_{\zeta_i}$ par la proposition suivante :

**Proposition 2.2.11** *L'application $\Phi_{\zeta_i} : \left\{ \begin{array}{ccc} \mathbb{K}[x_1, \ldots, x_n] & \longrightarrow & \mathcal{A}_{\zeta_i} \\ a & \longmapsto & a\mathbf{e}_{\zeta_i} \end{array} \right.$ est un isomorphisme de $\mathbb{K}$-algèbres.*

Du fait que $Q_{\zeta_i}$ est $\mathbf{m}_{\zeta_i}$-primaire on déduit du résultat précédent la proposition suivante :

**Proposition 2.2.12** *L'algèbre $\mathcal{A}_{\zeta_i}$ est une algèbre locale d'idéal maximal $(\mathbf{m}_{\zeta_i}/Q_{\zeta_i})\,\mathbf{e}_{\zeta_i}$.*

Pour aller plus avant dans la description de la structure de $\mathcal{A}_{\zeta_i}$ comme $\mathbb{K}$-espace vectoriel, on introduit dans la section suivante la notion de dualité.

## 2.3 Orthogonalité et dualité

**Définition 2.3.1** *Soit $\mathcal{R}$ une $\mathbb{K}$-algèbre, on note $\widehat{\mathcal{R}} = Hom_{\mathbb{K}}(\mathcal{R}, \mathbb{K})$ l'espace dual de $\mathcal{R}$. C'est l'ensemble des formes linéaires définies sur $\mathcal{R}$.*

Dans toute la suite de cette section, $\mathcal{R}$ désigne $\mathbb{K}[x_1, \ldots, x_n]$. Dans la sous-section suivante, on explique comment les opérateurs différentiels peuvent être interprétés comme des formes linéaires sur l'anneau des polynômes.

### 2.3.1 Opérateurs différentiels et dualité

Pour tout $i \in \{1, \ldots, n\}$, on note $\partial_i$ l'opérateur différentiel $\frac{d}{dx_i}$. Soit $\alpha \in \mathbb{N}^n$, on note $|\alpha| = \alpha_1 + \cdots + \alpha_n$, $\alpha! = \alpha_1! \cdots \alpha_n!$ et $\mathbf{d}^\alpha = \frac{1}{\alpha!}\frac{d^{\alpha_1}}{dx_1{}^{\alpha_1}} \cdots \frac{d^{\alpha_n}}{dx_n{}^{\alpha_n}} = \frac{1}{\alpha!}\partial_1 \cdots \partial_n$. On note par $\mathbb{K}[[\partial_1, \ldots, \partial_n]]$ l'anneau des séries formelles des variables $\partial_1, \ldots, \partial_n$ à coefficients dans $\mathbb{K}$.

Soit $\xi \in \mathbb{K}^n$, on définit la forme bilinéaire suivante :

$$\langle .,. \rangle_\xi : \left\{ \begin{array}{ccc} \mathbb{K}[[\partial_1, \ldots, \partial_n]] \times \mathcal{R} & \longrightarrow & \mathbb{K} \\ (\Lambda, f) & \longmapsto & \langle \Lambda, f \rangle_\xi = \Lambda(f)(\xi) \end{array} \right.$$

avec $\Lambda = \sum_{\alpha\in\mathbb{N}^n} \lambda_\alpha \partial^\alpha$ et $\Lambda(f)(\xi) = \sum_{\alpha\in\mathbb{N}^n} \lambda_\alpha (\partial^\alpha f)(\xi)$.

**Proposition 2.3.2** *Soit $\xi \in \mathbb{K}^n$, l'application $\mathbb{K}$-linéaire suivante :*

$$\Theta_\xi : \left\{ \begin{array}{ccc} \mathbb{K}[[\partial_1,\dots,\partial_n]] & \longrightarrow & \widehat{\mathcal{R}} \\ \Lambda & \longmapsto & \langle \Lambda, . \rangle_\zeta \end{array} \right.$$

*est un isomorphisme.*

*Preuve* : On peut exprimer la réciproque de $\Theta_\xi$ de la façon suivante : soit $\tau \in \widehat{\mathcal{R}}$, alors pour tout $f \in R$, on a $f(\mathbf{x}) = \sum_{\alpha\in\mathbb{N}^n} f_\alpha(\xi)(\mathbf{x}-\xi)^\alpha$ en utilisant le développement de Taylor au voisinage de $\xi$. On a donc $\tau(f) = \sum_{\alpha\in\mathbb{N}^n} f_\alpha(\xi)\tau((x-\xi)^\alpha) = \sum_{\alpha\in\mathbb{N}^n} \tau((x-\xi)^\alpha)\langle \mathbf{d}^\alpha, f\rangle_\xi$. On note alors $\tau_\alpha = \tau((x-\xi)^\alpha)$. A tout $\tau \in \widehat{\mathcal{R}}$ on associe $\Lambda = \sum_{\alpha\in\mathbb{N}^n} \tau_\alpha \mathbf{d}^\alpha$. Clairement $\forall f \in \mathcal{R}$, $\langle \Lambda, f\rangle_\xi = \sum_{\alpha\in\mathbb{N}^n} \tau_\alpha \langle \mathbf{d}^\alpha, f\rangle_\xi = \tau(f)$. Par suite $\tau = \Theta_\xi^{-1}(\Lambda)$. ♣

Dans toute la suite de la section, nous identifierons $\widehat{\mathcal{R}}$ et $\mathbb{K}[[\partial_1,\dots,\partial_n]]$. L'espace $\widehat{\mathcal{R}}$ est naturellement muni d'une structure de $\mathcal{R}$-module par : $\forall \Lambda \in \widehat{\mathcal{R}}$ et $\forall f \in \mathcal{R}$ on associe $f\Lambda : g \in \mathcal{R} \mapsto \Lambda(fg) \in \mathbb{K}$.

**Remarque 2.3.3** *Par la correspondance entre $\widehat{\mathcal{R}}$ et $\mathbb{K}[[\partial_1,\dots,\partial_n]]$, la multiplication par $x_i - \xi_i$ agit sur $\mathbb{K}[[\partial_1,\dots,\partial_n]]$ comme $\partial_{\partial_i}$. On a d'ailleurs $\langle \mathbf{d}^\beta, (x-\xi)^\alpha\rangle_\xi = \delta_{\alpha,\beta}$ et ainsi $(\mathbf{d}^\alpha)_{\alpha\in\mathbb{N}^n}$ et $((x-\xi)^\alpha)_{\alpha\in\mathbb{N}^n}$ sont deux familles duales pour $\langle .,. \rangle_\zeta$.*

On note par $e^{\xi,\partial} = \sum_{\alpha\in\mathbb{N}^n} \xi^\alpha \mathbf{d}^\alpha$. On a la proposition suivante :

**Proposition 2.3.4** *Soit $\Lambda \in \widehat{\mathcal{R}}$, on a $\Theta_{\mathbf{0}}^{-1}(\Lambda) = e^{\xi,\partial}\Theta_\xi^{-1}(\Lambda)$.*

*Preuve* : Pour prouver ce résultat, il suffit de le démontrer pour tout $\mathbf{d}^\beta$, $\beta \in \mathbb{N}^n$. Pour tout $p = \sum_{\alpha\in\mathbb{N}^n} p_\alpha \mathbf{x}^\alpha \in \mathcal{R}$ on associe $\partial^\beta p = p_\alpha^{(\beta)}\mathbf{x}^\alpha$. Comme $\mathbf{d}^\beta$,

$\beta \in \mathbb{N}^n$, est tel que $\langle \mathbf{d}^\beta, \mathbf{x}^\alpha \rangle_0 = \delta_{\alpha,\beta}$, on a

$$\begin{aligned}
\langle \partial^\beta, p \rangle_\xi &= \sum_{\alpha \in \mathbb{N}^n} p_\alpha^{(\beta)} \xi^\alpha \\
&= \langle \sum_{\alpha \in \mathbb{N}^n} \xi^\alpha \mathbf{d}^\alpha, \sum_{\alpha \in \mathbb{N}^n} p_\alpha^{(\beta)} \mathbf{x}^\alpha \rangle_0 \\
&= \langle \sum_{\alpha \in \mathbb{N}^n} \xi^\alpha \mathbf{d}^\alpha, \partial^\beta p(\mathbf{x}) \rangle_0 \\
&= \langle \partial^\beta e^{\xi,\alpha}, p(\mathbf{x}) \rangle_0 .
\end{aligned}$$

Ce qui prouve la proposition. ♣

### 2.3.2 Orthogonalité

**Définition 2.3.5**

- *Soit $\mathcal{I}$ un idéal de $\mathcal{R}$, on définit le sous-espace vectoriel $\mathcal{I}^\perp \subset \widehat{\mathcal{R}}$ orthogonal à $\mathcal{I}$ (aussi appelé système inverse de $\mathcal{I}$) de la façon suivante :*

$$\mathcal{I}^\perp = \left\{ \Lambda \in \widehat{\mathcal{R}} \,|\, \Lambda(f) = 0 \,,\, \forall f \in \mathcal{I} \right\}$$

- *Soit $D$ un sous-espace vectoriel de $\widehat{\mathcal{R}}$, on définit le sous-espace vectoriel $D^\perp$ de $\mathcal{R}$ orthogonal à $D$ de la façon suivante :*

$$D^\perp = \{ f \in \mathcal{R} \,|\, \Lambda(f) = 0 \,,\, \forall \Lambda \in D \}$$

**Remarque 2.3.6** *L'orthogonal d'un sous-espace vectoriel de $\widehat{\mathcal{R}}$ n'est pas un idéal de $\mathcal{R}$ en général. De plus, comme nous le verrons plus tard, tous les sous-espaces vectoriels de $\widehat{\mathcal{R}}$ ne sont pas des orthogonaux d'idéaux de $\mathcal{R}$.*

La proposition suivante explique le lien fort qui existe entre l'orthogonal d'un idéal $\mathcal{I}$ et le dual de l'algèbre quotient de $\mathcal{R}$ par $\mathcal{I}$.

**Proposition 2.3.7** *Soit $\mathcal{I}$ un idéal de $\mathcal{R}$ et $\mathcal{A} = \mathcal{R}/\mathcal{I}$, alors la projection $\Pi : \mathcal{R} \to \mathcal{A}$ induit un isomorphisme $\Pi_* : \widehat{\mathcal{A}} \to \mathcal{I}^\perp$.*

*Preuve :* On va d'abord donner explicitement $\Pi_*$. Soit $\tau \in \widehat{\mathcal{A}}$, on définit $\Pi_*(\tau) = \tau \circ \Pi$. On voit facilement que $\Pi_*(\tau) \in \mathcal{I}^\perp$. On considère alors l'application suivante :

$$\Theta : \left\{ \begin{array}{ccc} \mathcal{I}^\perp & \longrightarrow & \widehat{\mathcal{A}} \\ \Lambda & \longmapsto & \Theta(\Lambda) \end{array} \right.$$

Pour tout $\Lambda \in \mathcal{I}^{\perp}$, $\Theta(\Lambda)$ est définie de la façon suivante : pour tout $a \in \mathcal{A}$, il existe $b \in \mathcal{R}$ tel que $\Pi(b) = a$, alors $\Theta(\Lambda)(a) = \Lambda b$. On vérifie facilement que cette définition ne dépend pas de l'élément $b$ choisi. En effet si $c \in \mathcal{R}$ est un autre élément tel que $\Pi(c) = a$, alors $b - c \in \mathcal{I}$ et donc $\Lambda(b) - \Lambda(c) = \Lambda(b - c) = 0$. Ce qui montre que $\Theta$ est bien définie. On montre alors que $\Theta$ et $\Pi_*$ sont réciproques l'une de l'autre. Montrons que $\Theta \circ \Pi_* = Id_{\widehat{\mathcal{A}}}$. Pour tout $a \in \mathcal{A}$, on a $(\Theta \circ \Pi)(\tau)(a) = \Theta(\tau \circ \Pi)(a)$, soit $b \in \mathcal{R}$ tel que $\pi(b) = a$, on a $\Theta(\tau \circ \Pi)(a) = \tau(\Pi(b)) = \tau(a)$. Ainsi $(\Theta \circ \Pi)(\tau) = \tau$. Montrons maintenant que $\Pi_* \circ \Theta = Id_{\mathcal{I}^{\perp}}$. Soit $\Lambda \in \mathcal{I}^{\perp}$, alors pour tout $b \in \mathcal{R}$, on a $(\Pi_* \circ \Theta)(\Lambda)(b) = \Pi_*(\Theta(\Lambda)(b)) = \Theta(\Lambda)(\Pi(b)) = \Lambda(b)$ par définition de $\Theta$. Donc $(\Pi_* \circ \Theta)(\Lambda) = \Lambda$. On a donc bien montré que $\Pi_*$ et $\Theta$ sont deux applications réciproques l'une de l'autre. La vérification de la linéarité de ces applications ne présente aucune difficulté. ♣

Le théorème suivant, dont nous ne donnerons pas de preuve ici, explique quel lien existe entre certains sous-espaces vectoriels de $\mathbb{K}[[\partial_1, \ldots, \partial_n]]$ et les idéaux de $\mathcal{R}$. Mais auparavant, nous donnons une définition nécessaire à l'énoncé du théorème.

**Définition 2.3.8** *Soit $E$ un sous-espace vectoriel de $\mathbb{K}[[\partial_1, \ldots, \partial_n]]$. On dit que $E$ est stable si pour tout $\Lambda(\partial) \in E$, $\partial_{\partial_i}\Lambda(\partial) \in E$.*

**Théorème 2.3.9** *Il y a une bijection ensembliste entre les idéaux de $\mathcal{R}$ et les sous-espaces vectoriels de $\widehat{\mathcal{R}}$ fermés pour la topologie $(\partial_1, \ldots, \partial_n)$-adique et stables.*

*Preuve :* Voir [41]. ♣

On remarque que la condition de stabilité vient de la structure de $\mathbb{K}[x_1, \ldots, x_n]$-module et du fait que la multiplication par une variable agit comme la dérivation par rapport à une variable différentielle (voir remarque 2.3.3).

**Propriétés 2.3.10** *Soient $\mathcal{I}$ un idéal de $\mathcal{R}$ et $D$ un sous-espace vectoriel de $\widehat{\mathcal{R}}$ férmé et stable par dérivation :*

- ${\mathcal{I}^{\perp}}^{\perp} = \mathcal{I}$
- ${D^{\perp}}^{\perp} = D$

**Définition 2.3.11** *Soient $\Lambda_1, \ldots, \Lambda_s \in \mathbb{K}[[\partial_1, \ldots, \partial_n]]$, on note $\langle\langle \Lambda_1, \ldots, \Lambda_s \rangle\rangle$ le sous-espace vectoriel de $\mathbb{K}[[\partial_1, \ldots, \partial_n]]$ engendré par les $\Lambda_1, \ldots, \Lambda_s$ et leurs dérivées.*

Les propriétés qui suivent expliquent comment agit la dualité sur les opérations sur les idéaux et pour l'inclusion.

**Propriétés 2.3.12** *Soient $\mathcal{I}$ et $\mathcal{J}$ deux idéaux de $\mathcal{R}$, alors :*
- $\mathcal{I} \subset \mathcal{J}$ *si et seulement si* $\mathcal{J}^\perp \subset \mathcal{I}^\perp$
- $(\mathcal{I} \cap \mathcal{J})^\perp = \mathcal{I}^\perp + \mathcal{J}^\perp$
- $(\mathcal{I} + \mathcal{J})^\perp = \mathcal{I}^\perp \cap \mathcal{J}^\perp$

La proposition suivante donne un analogue de la décomposition en algèbre locale d'une algèbre quotient pour son dual.

**Proposition 2.3.13** *Soit $\mathcal{I}$ un idéal de $\mathcal{R}$ tel que $\mathcal{Z}(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_d\}$, alors on note $\mathcal{A} = \mathcal{R}/\mathcal{I}$ et on a $\widehat{\mathcal{A}} = D_{\zeta_1} \oplus \cdots \oplus D_{\zeta_d}$ où $D_{\zeta_i} = Q_{\zeta_i}^\perp$, où $Q_{\zeta_i}$ est la composante $\mathbf{m}_{\zeta_i}$-primaire de $\mathcal{I}$.*

*Preuve :* On a $\mathcal{I} = \bigcap_{i=1}^{d} Q_{\zeta_i}$, donc $\mathcal{I}^\perp = (\bigcap_{i=1}^{d} Q_{\zeta_i})^\perp = \sum_{i=1}^{d} Q_{\zeta_i}^\perp$. Si $i \neq j$ alors $Q_{\zeta_i}$ et $Q_{\zeta_j}$ sont des idéaux étrangers, donc $Q_{\zeta_i} + Q_{\zeta_j} = \mathcal{R}$ et par suite $(Q_{\zeta_i} + Q_{\zeta_j})^\perp = \mathcal{R}^\perp = 0$ et la somme est directe. ♣

La proposition suivante et le résultat précédent montrent qu'on peut calculer le système inverse localement pour retrouver la structure globale du dual d'une algèbre quotient.

**Proposition 2.3.14** *Soit $\mathcal{I}$ un idéal de $\mathcal{R}$ tel que $\mathcal{Z}(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_d\}$, on note $\mathcal{A} = \mathcal{R}/\mathcal{I}$ et on a $\mathcal{A} = \mathcal{A}_{\zeta_1} \oplus \ldots \oplus \mathcal{A}_{\zeta_d}$ où $\mathcal{A}_{\zeta_i}$ est l'algèbre locale associée à $\zeta_i$, $\forall i \in \{1, \ldots, d\}$. Alors on a $\widehat{\mathcal{A}}_{\zeta_i} = D_{\zeta_i}$ et par suite $\widehat{\mathcal{A}} = \bigoplus_{i=1}^{d} \widehat{\mathcal{A}}_{\zeta_i}$.*

*Preuve :* On a $\mathcal{A}_{\zeta_i} = \mathcal{R}/Q_{\zeta_i}$ et donc $\widehat{\mathcal{A}}_{\zeta_i} = Q_{\zeta_i}^\perp = D_{\zeta_i}$. Le résultat découle alors de la proposition 2.3.13. ♣

La proposition suivante énonce que les duaux des locaux peuvent être représentés par des polynômes différentiels au lieu de séries comme nous aurions pu le croire.

**Proposition 2.3.15** *Soit $Q_{\zeta_i}$ la composante $\mathbf{m}_{\zeta_i}$-primaire de $\mathcal{I}$, alors $\widehat{\mathcal{A}}_{\zeta_i} = Q_{\zeta_i}^\perp \subset \Theta_{\zeta_i}^{-1}(\mathbb{K}[\partial_1, \ldots, \partial_n])$.*

*Preuve :* On a $\mathcal{A}_{\zeta_i}$ qui est un espace vectoriel de dimension finie et il existe $E \in \mathbb{N}^n$ tel que $((\mathbf{x} - \zeta_i)^\alpha)_{\alpha \in E}$ est une base de $\mathcal{A}$. On remarque alors que $(\mathbf{d}^\alpha)_{\alpha \in E}$ est une base duale de la base $((\mathbf{x} - \zeta_i)^\alpha)_{\alpha \in E}$ pour le produit scalaire $\langle ., . \rangle_{\zeta_i}$. Ainsi, toute forme linéaire peut être représentée par une combinaison linéaire des $\mathbf{d}^\alpha$, donc par un polynôme diffénretiel. ♣

Le théorème suivant précise et reformule le résultat que nous venons de démontrer.

**Théorème 2.3.16** *Soit* $\mathcal{I} = (f_1, \ldots, f_m)$ *tel que* $\mathcal{Z}(f_1, \ldots, f_m) = \{\zeta_1, \ldots, \zeta_d\}$, *alors pour tout* $i \in \{1, \ldots, d\}$ *il existe une famille* $\left(\Lambda_1^{(i)}, \ldots, \Lambda_{\mu_i}^{(i)}\right)$ *telle que pour tout* $\Lambda \in \mathcal{I}^\perp$ *on a* $\Lambda = e^{\zeta_i, \partial} \sum_{i=1}^{d} \sum_{j=1}^{\mu_i} \lambda_{i,j} \Lambda_j^{(i)}$. *De plus si* $f \in \mathcal{A}$, *on a* $\Lambda(f) = \sum_{i=1}^{d} \sum_{j=1}^{\mu_i} \lambda_{i,j} \langle \Lambda_j^{(i)}, f \rangle_{\zeta_i}$.

**Corollaire 2.3.17** *La famille* $\left(\Lambda_j^{(i)} e^{\zeta_i, \partial}\right)_{\substack{1 \le i \le d \\ 1 \le j \le \mu_i}}$ *est une base de* $\widehat{\mathcal{A}} = \mathcal{I}^\perp$ *comme* $\mathbb{K}$*-espace vectoriel.*

Plusieurs algorithmes pour calculer de telles bases existent (comme celui donné dans [73]). La plupart du temps, nous supposerons que nous connaissons les polynômes différentiels $\left(\Lambda_j^{(i)}\right)_{1 \le i \le d, 1 \le j \le \mu_i}$.

Nous avons vu comment interpréter les duaux des algèbres locales $\mathcal{A}_{\zeta_i}$ comme des polynômes différentiels par le biais des produits scalaires $\langle ., . \rangle_{\zeta_i}$. La définition suivante explique comment utiliser la décomposition $\widehat{\mathcal{A}} = \oplus_{i=1}^{d} \widehat{\mathcal{A}}_{\zeta_i}$ pour définir un produit scalaire sur $\mathcal{A}$ qui nous permettra de représenter tous les éléments de $\widehat{\mathcal{A}}$ comme des polynômes différentiels dans la proposition suivante. Comme $\widehat{\mathcal{A}} = \oplus_{i=1}^{d} \widehat{\mathcal{A}}_{\zeta_i}$, toute forme linéaire $\Lambda \in \widehat{\mathcal{A}}$ peut se décomposer sous la forme $(\Lambda_1, \ldots, \Lambda_d)$ où $\Lambda_i \in \widehat{\mathcal{A}}_{\zeta_1}$, $\forall i \in \{1, \ldots, d\}$. On donne alors la définition suivante :

**Définition 2.3.18** *On définit la forme bilinéaire* $\langle ., . \rangle_{\mathcal{Z}(\mathcal{I})} : \widehat{\mathcal{A}} \times \mathcal{A} \to \mathbb{K}$ *qui à* $\Lambda = (\Lambda_1, \ldots, \Lambda_d) \in \widehat{\mathcal{A}}$ *et* $p \in \mathcal{A}$ *associe* $\sum_{i=1}^{d} \langle \Lambda_i, p \rangle_{\zeta_i}$.

Une propriété fondamentale de cette forme bilinéaire est donnée par la proposition suivante :

**Proposition 2.3.19** *La forme bilinéaire* $\langle ., . \rangle_{\mathcal{Z}(\mathcal{I})}$ *est non dégénérée.*

*Preuve :* On considère $\Lambda = (\lambda_1, \ldots, \Lambda_d) \in \widehat{\mathcal{A}} \setminus \{0\}$ tel que $\forall p \in \mathcal{A}$, on ait $\langle \Lambda, p \rangle_{\mathcal{A}(\mathcal{I})}$. Alors $\forall p \in \mathcal{A}_{\zeta_i}$, on a $\langle \Lambda, p \rangle_{\mathcal{Z}(\mathcal{I})} = \langle \Lambda_i, p \rangle_{\zeta_i} = 0$ et par suite $\Lambda_i = 0$, $\forall i \in \{1, \ldots, d\}$, ce qui contredit l'hypothèse que $\Lambda \neq 0$. Soit $p = \sum_{i=1}^{d} p_i \in \mathcal{A} \setminus \{0\}$, où $p_i \in \mathcal{A}_{\zeta_i}$, tel que pour tout $\Lambda \in \widehat{\mathcal{A}}$, on ait $\langle \Lambda, p \rangle_{\mathcal{Z}(\mathcal{I})} = 0$.

Alors, $\forall \Lambda_i \in \widehat{\mathcal{A}}_{\zeta_i}$ on aurait $\langle \Lambda_i, p\rangle_{\mathcal{Z}(\mathcal{I})} = 0$, donc $\langle \Lambda_i, p_i\rangle_{\zeta_i} = 0$ et par suite $p_i = 0$, $\forall i \in \{1, \ldots, d\}$. Cela contredit l'hypothèse que $p \neq 0$. Cela montre que la forme bilinéaire $\langle ., .\rangle_{\mathcal{Z}(\mathcal{I})}$ est non dégénérée. ♣

Ce résultat paraphrase le résultat énonçant que le résidu d'un système algébrique est la somme des résidus locaux.

Nous appliquerons ces résultats pour donner des formules explicites d'objets comme les idempotents dans la section suivante.

## 2.4 Représentation des algèbres de dimension zéro et interpolation

### 2.4.1 Introduction

Dans le cas des polynômes univariés à coefficients complexes, on sait décrire un système de "réécriture" modulo un polynôme $P \in \mathbb{C}[x]$ de degré $d$ grâce à la division euclidienne. Cela revient à choisir $1, \ldots, x^{d-1}$ comme base de $\mathbb{C}[x]/\left(P\right)$ pour la structure d'espace vectoriel. C'est dû au fait que tout polynôme admet un unique reste de degré $d-1$ par la division euclidienne par $P$. Mais ce faisant on ne tient compte que de la structure additive du quotient donnée par l'addition vectorielle. La structure multiplicative est néanmoins elle aussi contenue dans cette description. En effet, si on note $N(f)$ le reste de $f \in \mathbb{C}[x]$ par la division euclidienne par $P$ (c'est la forme normale de $f$ pour le système de réécriture évoqué plus haut), on a, pour tout $f$ et $g \in \mathbb{C}[x]$, $N(fg) = N(N(f)N(g))$. Cela nous permet de "calculer dans $\mathcal{A}$". Nous précisons maintenant ce que nous entendons par représentation dans toute la suite du texte. Dans ce qui précède, on vient de donner un isomorphisme de $\mathbb{C}$-espace vectoriel explicite entre $\mathcal{A}$ et $\mathbb{C}[x]_{d-1}$, où $\mathbb{C}[x]_{d-1}$ est l'espace vectoriel des polynômes de degré inférieur ou égal à $d-1$. Se donner un élément $f \in \mathcal{A}$ peut être vu comme le fait de se donner un élément de $\mathrm{End}\left(\mathbb{C}[x]_{d-1}\right)$. En effet, il suffit de considérer $\mathcal{M}_f : g \in \mathbb{C}[x]_{d-1} \mapsto N(fg) \in \mathbb{C}[x]_{d-1}$. Un fait remarquable est alors donné par le théorème suivant :

**Théorème 2.4.1** *Si* $P\left(x\right) = \prod_{i=1}^{d} (x - \zeta_i)$ *avec* $\zeta_i \neq \zeta_j$ *si* $i \neq j$, $i$ *et* $j \in \{1, \ldots, d\}$, *alors pour tout* $f \in \mathbb{C}[x]_{d-1}$ *les valeurs propres de* $\mathcal{M}_f$ *sont* $\{f\left(\zeta_1\right), \ldots, f\left(\zeta_d\right)\}$.

Un corollaire bien connu est le suivant :

**Corollaire 2.4.2** *Si* $P(x) = \prod_{i=1}^{d}(x-\zeta_i)$ *avec* $\zeta_i \neq \zeta_j$ *si* $i \neq j$, $i$ *et* $j \in \{1,\ldots,d\}$, *alors les valeurs propres de* $\mathcal{M}_x$ *sont* $\{\zeta_1,\ldots,\zeta_d\}$.

La matrice $M_x$ de $\mathcal{M}_x$ dans la base monomiale $\{1, x, \ldots, x^{d-1}\}$ de $\mathbb{C}[x]_{d-1}$ est connue sous le nom de matrice compagnon de $P$. Une méthode envisageable pour calculer les racines d'un polynôme $P$ est de calculer les valeurs propres de la matrice $M_x$ exprimée dans une base convenable par des méthodes d'algèbre linéaire (ou par d'autres méthodes, voir [44]). C'est la base de beaucoup d'algorithmes dits "d'algèbre linéaire pour la résolution d'équations algébriques".

Une autre base bien connue de $\mathbb{C}[x]_{d-1}$ est la base des polynômes de Lagrange $L_i(x) = \dfrac{\prod_{i\neq j}(x-\zeta_j)}{\prod_{i\neq j}(\zeta_i-\zeta_j)}$, $i \in \{1,\ldots,d\}$. La formule de Cauchy nous dit alors que $\forall f \in \mathbb{C}[x]$, $\tilde{f} = \sum_{i=1}^{d} f(\zeta_i) L_i(x) \in \mathbb{C}[x]_{d-1}$. Dans cette base, la matrice $M_f$ de $\mathcal{M}_f$ est particulièrement simple puisque c'est la matrice suivante :

$$\begin{pmatrix} f(\zeta_1) & 0 & \cdots & 0 \\ 0 & f(\zeta_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f(\zeta_d) \end{pmatrix}$$

Cela peut être vu comme le fait que, $\forall g \in \mathbb{C}[x]$, $N(fg) = \sum_{i=1}^{d} f(\zeta_i) L_i(x)$, où $L_i$ est le polynôme de Lagrange associé à $\zeta_i$. Cela donne, en plus d'une preuve du théorème fondamental de l'algèbre à partir du théorème de Cauchy et une formule de produit rapide dans $\mathcal{A}$ par produit de convolution. En effet, si on connaît les racines, on transforme, via les évaluations, l'algèbre quotient en algèbre de convolution. Plus remarquable est le fait qu'on en déduit que les vecteurs propres de $\mathcal{M}_f$ sont les polynômes de Lagrange. Un autre fait remarquable est que ces polynômes sont dans ce cas le système fondamental d'idempotents de $\mathcal{A}$. Il existe bien d'autres représentations (i.e. de bases d'espace vectoriel de $\mathbb{C}[x]_{d-1}$ dans lesquelles on exprime le produit de $\mathcal{A}$). La philosophie que nous dégageons est que pour connaître la structure de $\mathcal{A}$ (et implicitement $\mathcal{Z}(P) = (\zeta_1,\ldots,\zeta_d)$), on se fixe une structure d'espace vectoriel dont on calcule une base dans laquelle on traduit la structure multiplicative en termes d'endomorphisme. C'est une extension des idées de la théorie de la représentation des groupes.

Dans la suite de cette section, nous donnons des généralisations de ces résultats dans le cas multivarié. Certains résultats sont déjà connus [39]. La situation est bien plus difficile du fait qu'on ne dispose pas de division euclidienne. Cela entraîne, entre autres choses, que l'espace vectoriel "de représentation" n'est pas unique, alors que dans le cas univarié le choix de $\mathbb{C}[x]_{d-1}$ s'impose de lui-même. Nous introduirons des résultats nouveaux comme des formules explicites pour les idempotents, ce qui nous permettra de donner une généralisation des relations bien connues entre coefficients et racines dans le cas multivarié.

### 2.4.2 Cas des racines simples

Soient $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$. On note $\mathcal{I} = (f_1, \ldots, f_m)$ l'idéal qu'ils engendrent et par $\mathcal{Z} = \mathcal{Z}(\mathcal{I}) = \left\{\zeta \in \overline{\mathbb{K}}^n \mid f_i(\zeta) = 0\,, \forall i \in \{1, \ldots, m\}\right\}$ l'ensemble algébrique associé. On suppose que $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_d\}$ et que toutes les racines sont simples. On note par $\mathbf{1}_{\zeta_i} : p \in \mathcal{A} \to p(\zeta_i)$ la forme linéaire d'évaluation en $\zeta_i$ et par $\mathbf{e}_{\zeta_i}$ l'idempotent associé à $\zeta_i$ pour $i \in \{1, \ldots, d\}$.

En corollaire des propositions 2.2.3, 2.2.9 et 2.2.8, nous avons la proposition suivante :

**Proposition 2.4.3** *Les idempotents $\mathbf{e}_{\zeta_1}, \ldots, \mathbf{e}_{\zeta_d}$ de $\mathcal{A}$ forment une base de $\mathcal{A}$ comme $\mathbb{K}$-espace vectoriel et la famille $\{\mathbf{1}_{\zeta_1}, \ldots, \mathbf{1}_{\zeta_d}\}$ est une base de $\widehat{\mathcal{A}}$ duale de la base des idempotent. On dispose alors de la formule de Cauchy : $\forall f \in \mathcal{A}$, on a*

$$f(x) = \sum_{i=1}^{d} \mathbf{1}_{\zeta_i}(f)\, \mathbf{e}_{\zeta_i}(x) = \sum_{i=1}^{d} f(\zeta_i)\, \mathbf{e}_{\zeta_i}(x) \tag{2.1}$$

Ce résultat peut être interprété comme un résultat d'interpolation car il généralise la formule d'interpolation de Lagrange. C'est ainsi que nous l'avons introduit dans [80]. Cette représentation de $\mathcal{A}$ a plusieurs avantages. L'un d'eux est la simplicité de la structure multiplicative, comme dans le cas univarié. En effet, soient $a$ et $b \in \mathcal{A}$, on a $ab = \sum_{i=1}^{d} \mathbf{1}_{\zeta_i}(ab)\, \mathbf{e}_{\zeta_i} = \sum_{i=1}^{d} a(\zeta_i)\, b(\zeta_i)\, \mathbf{e}_{\zeta_i}$.

**Définition 2.4.4** *Soient $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_d\} \subset \overline{\mathbb{K}}^n$ et $E = \{\alpha_1, \ldots, \alpha_d\} \subset \mathbb{N}^n$, on dénote par $\mathbf{x}^E = \{\mathbf{x}^\alpha \mid \alpha \in E\}$. On appelle matrice de Vandermonde* *associée à $E$ et à $\mathcal{Z}$ la matrice*

$$V_{E,\mathcal{Z}} = \begin{pmatrix} \zeta_1^{\alpha_1} & \cdots & \zeta_1^{\alpha_d} \\ \vdots & \ddots & \vdots \\ \zeta_d^{\alpha_1} & \cdots & \zeta_d^{\alpha_d} \end{pmatrix}.$$

*Le déterminant de Vandermonde associé à $E$ et à $\mathcal{Z}$ est noté $\mathbf{v}_{E,\mathcal{Z}} = det(V_{E,\mathcal{Z}})$.*

**Définition 2.4.5** *Soit $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_d\} \subset \overline{\mathbb{K}}^n$ tel que $\zeta_i \neq \zeta_j$ si $i \neq j$. On note $\mathcal{I}_\mathcal{Z}$ l'idéal qui lui est associé, i.e. l'idéal $\mathcal{I}_\mathcal{Z} \in \overline{\mathbb{K}}[x_1, \ldots, x_n]$ tel que $\mathcal{Z}(\mathcal{I}_\mathcal{Z}) = \mathcal{Z}$.*

**Proposition 2.4.6** *Soient $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_d\} \subset \overline{\mathbb{K}}^n$ sans point multiple et $E = \{\alpha_1, \ldots, \alpha_d\} \subset \mathbb{N}^n$. L'ensemble de monômes $\mathbf{x}^E$ est une base monomiale de $\mathcal{A}_\mathcal{Z} = \overline{\mathbb{K}}[x_1, \ldots, x_n]/\mathcal{I}_Z$ si et seulement si le déterminant de Vandermonde associé à $E$ et $\mathcal{Z}$ est non nul.*

*Preuve* : D'après la proposition 2.4.3 on a, $\forall i \in \{1, \ldots, d\}$, $\mathbf{x}^{\alpha_i} = \sum_{j=1}^{d} 1_{\zeta_j} \mathbf{e}_{\zeta_j}(\mathbf{x}) = \sum_{j=1}^{d} \zeta_j^{\alpha_i} \mathbf{e}_{\zeta_j}(\mathbf{x})$. La matrice $V_{E,\mathcal{Z}}$ peut s'écrire sous la forme suivante :

$$V_{E,\mathcal{Z}} = \begin{pmatrix} 1_{\zeta_1}(\mathbf{x}^{\alpha_1}) & \cdots & 1_{\zeta_1}(\mathbf{x}^{\alpha_d}) \\ \vdots & \ddots & \vdots \\ 1_{\zeta_d}(\mathbf{x}^{\alpha_1}) & \cdots & 1_{\zeta_d}(\mathbf{x}^{\alpha_d}) \end{pmatrix}.$$

La colonne $i$ de la matrice est donc formée des coordonnées de $\mathbf{x}^{\alpha_i}$ dans la base des idempotents de $\mathcal{A}$. Si le déterminant de cette matrice est non nul, cela signifie que la transposée de cette matrice est la matrice de changement de base allant de la base des idempotents dans une base formée des $(\mathbf{x}^\alpha)_{\alpha \in E}$. Ce qui implique que $\mathbf{x}^E$ est une base monomiale de $\mathcal{A}$. Si le déterminant est nul, cela signifie que les représentants des monômes de $\mathbf{x}^E$ sont liés dans $\mathcal{A}$, donc qu'ils ne forment pas une base de $\mathcal{A}$. ♣

**Définition 2.4.7** *Soit $E = \{\alpha_1, \ldots, \alpha_d\} \subset \mathcal{M}^n$, on note par $\mathbb{K}[x_1, \ldots, x_n]_E = \left\{ p \in \mathbb{K}[x_1, \ldots, x_n] \,|\, p = \sum_{\alpha \in E} p_\alpha \mathbf{x}^\alpha \right\}$, c'est-à-dire l'espace vectoriel des polynômes à support dans $\mathbf{x}^E$.*

**Définition 2.4.8** *Soit $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_d\} \subset \overline{\mathbb{K}}^n$ et soit $E = \{\alpha_1, \ldots, \alpha_d\} \subset \mathbb{N}^n$ tels que $\mathbf{v}_{E,\mathcal{Z}} \neq 0$ (i.e. $\mathbf{x}^E$ est une base monomiale de $\mathcal{A}_{\mathcal{Z}}$). On définit le polynôme de Lagrange généralisé (on dira polynôme de Lagrange par abus de langage) associé à $\zeta_i$ comme suit :*

$$\mathbf{e}_i = \frac{-1}{\mathbf{v}_{E,\mathcal{Z}}} \begin{vmatrix} \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_d} \\ \zeta_1^{\alpha_1} & \cdots & \zeta_1^{\alpha_d} \\ \vdots & & \vdots \\ \zeta_{i-1}^{\alpha_1} & \cdots & \zeta_{i-1}^{\alpha_d} \\ \zeta_{i+1}^{\alpha_1} & \cdots & \zeta_{i+1}^{\alpha_d} \\ \vdots & & \vdots \\ \zeta_d^{\alpha_1} & \cdots & \zeta_d^{\alpha_d} \end{vmatrix}$$

**Propriété 2.4.9** *Soient $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ tels que $\mathcal{Z} = \mathcal{Z}(f_1, \ldots, f_n) = \{\zeta_1, \ldots, \zeta_d\}$ sans point multiple. Soit $E \in \mathbb{N}^n$ tel que $\mathbf{v}_{E,\mathcal{Z}} \neq 0$. Alors la classe de $\mathbf{e}_i$ dans $\mathcal{A}$ est la classe de l'idempotent associé à $\zeta_i$ et $\mathbf{e}_i \in \mathbb{K}[x_1, \ldots, x_n]_E$, $\forall i \in \{1, \ldots, d\}$.*

*Preuve :* Il suffit de vérifier que ces polynômes vérifient $\mathbf{e}_i(\zeta_j) = \delta_{i,j}$. ♣

On dispose alors par la formule de Cauchy d'un analogue effectif de la formule d'interpolation de Lagrange :

**Théorème 2.4.10** *On suppose que $\mathbf{v}_{E,\mathcal{Z}} \neq 0$, alors pour tout $\mathbf{v} = (v_1, \ldots, v_d) \in \overline{\mathbb{K}}^d$, il existe un unique polynôme $p \in \mathbb{K}[x_1, \ldots, x_n]_E$ tel que $p(\zeta_i) = v_i$, $\forall i \in \{1, \ldots, d\}$. De plus ce polynôme est donné par :*

$$p(\mathbf{x}) = \sum_{i=1}^{d} v_i \mathbf{e}_i(\mathbf{x}).$$

**Remarque 2.4.11** *La démarche consistant à utiliser les idempotents d'une algèbre quotient pour faire de l'interpolation n'est pas neuve. Elle est déjà présente dans les travaux de L. Kronecker [61] (et même de C. G. J. Jacobi) qui donne une formule explicite dans le cas des intersections complètes projectives. Son approche est basée sur le bézoutien (nous décrirons d'ailleurs une généralisation des formules de L. Kronecker dans le chapitre suivant). L'utilisation des structures quotients dans le contexte de l'interpolation a peu évoluée jusqu'à une date récente avec les travaux d'auteurs comme M. Gasca et T. Sauer qui utilisent des outils comme les bases de Gröbner pour construire des espaces d'interpolation* ad hoc *(voir [86]). Pour plus de détails historiques sur le sujet, nous renvoyons à [49].*

### 2.4.3 Cas de racines multiples

Il s'agit ici de donner des extensions des résultats précédents pour la représentation des algèbres de dimension zéro non réduites. On traduit aussi cette approche en termes de problèmes d'interpolation. Il s'agit alors de généraliser l'interpolation d'Hermite.

Nous avons déjà vu que le problème d'interpolation de Lagrange consiste à se donner un ensemble de points $\{z_1, \ldots, z_d\} \subset \mathbb{K}$ distincts et un ensemble de valeurs $\{v_1, \ldots, v_d\} \subset \mathbb{K}$. On cherche alors un unique polynôme unitaire $P(x) \in \mathbb{K}[x]_d$ vérifiant $P(z_i) = v_i$, $\forall i \in \{1, \ldots, d\}$. Le problème d'interpolation d'Hermite consiste lui à se donner un ensemble de points $\{z_1, \ldots, z_d\} \subset \mathbb{K}$ distincts, un ensemble de polynômes en $\frac{d}{dx}$, $\left\{f_{1,1}\left(\frac{d}{dx}\right), \ldots, f_{1,\mu_1}\left(\frac{d}{dx}\right),\right.$ $\left.\ldots, f_{d,1}\left(\frac{d}{dx}\right), \ldots, f_{d,\mu_d}\left(\frac{d}{dx}\right)\right\}$ et un ensemble de valeurs $\{v_{1,1}, \ldots, v_{1,\mu_1}, \ldots, v_{d,1}, \ldots, v_{d,\mu_d}\}$, c'est-à-dire un ensemble de conditions différentielles en chaque point de l'ensemble des points sur lequel on interpole. On cherche alors un unique polynôme unitaire $P(x) \in \mathbb{K}[x]_D$, avec $D = \sum_{i=1}^{d} \mu_i$, vérifiant $\left(f_{i,j}\left(\frac{d}{dx}\right) P\right)(z_i) = v_{i,j}$, $\forall i \{1, \ldots, d\}$ et $j \in \{1, \ldots, \mu_i\}$. Nous ne traitons pas ici des conditions que doivent vérifier les familles $\{f_{i,1}, \ldots, f_{i,\mu_i}\}$, mais ces polynômes ne peuvent pas être choisis arbitrairement (voir [69]). Quand le problème a une solution, on sait construire explicitement le polynôme $P$.

Dans cette partie, nous traitons une généralisation de ce problème dans le cas multivarié. Nous décrivons maintenant le problème d'interpolation d'Hermite dans ce cas. On considère un ensemble de points $\{\zeta_1, \ldots, \zeta_d\} \subset \mathbb{K}^d$ distincts et un ensemble de polynômes différentiels $\left(\Lambda_j^{(i)}, i \in \{1, \ldots, d\}\, j \in \{1, \ldots, \mu_i\} \text{ et } i \in \{1, \ldots, d\}\right) \subset \mathbb{K}[\partial_1, \ldots, \partial_n]$ représentant nos conditions différentielles en chaque nœud de l'ensemble des points d'interpolation. On suppose que $(\Lambda_{i,j})_{j \in \{1,\ldots,\mu_i\}}$ engendre un espace vectoriel de $\mathbb{K}[\partial_1, \ldots, \partial_n]$ stable par dérivation, si bien que $\langle\langle \lambda_j^{(i)} e^{\zeta_i, \partial}, j \in \{1, \ldots, \mu_i\} \text{ et } i \in \{1, \ldots, d\}\rangle\rangle^{\perp} = \mathcal{I}_\Lambda$ est un idéal de $\mathbb{K}[x_1, \ldots, x_n]$. On note $\mathcal{A}_\Lambda = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_\Lambda$ l'algèbre quotient associée. C'est l'algèbre des coordonnées de l'ensemble algébrique $Z(\mathcal{I}_\Lambda)$. Ainsi le dual de l'algèbre locale $\mathcal{A}_{\zeta_i}$ est l'espace vectoriel engendré par $\left(\Lambda_j^{(i)}\right)_{j \in \{1,\ldots,\mu_i\}}$. Comme cet espace vectoriel est stable sous l'action de $\partial_{\partial_k}$, $k \in \{1, \ldots, n\}$, il contient 1. On suppose donc sans perte de généralité que $\Lambda_1^{(i)} = 1$, $\forall i \in \{1, \ldots, d\}$ et que les $\Lambda_j^{(i)}$, $j \neq 1$, sont sans termes constants. On suppose de plus qu'on connaît une base monomiale $\mathbf{x}^E$ de $\mathcal{A}_\Lambda$. On se donne des valeurs $\{v_{1,1}, \ldots, v_{1,\mu_1}, \ldots, v_{d,1}, \ldots, v_{d,\mu_d}\} \subset \mathbb{K}$. On cherche alors $P \in \mathcal{A}_\Lambda$ vérifiant $\langle \Lambda_j^{(i)}, P\rangle_{\zeta_i} = v_{i,j}$, $\forall i \in \{1,\ldots,d\}$ et $j \in \{1,\ldots,\mu_i\}$.

On commence par définir une généralisation de la matrice de Vandermonde :

**Définition 2.4.12** *Avec les hypothèses et notations précédentes, la matrice de Vandermonde associée à $E$ et $\mathcal{Z}(\mathcal{I}_\Lambda) = \{\zeta_1,\ldots,\zeta_d\}$, est définie de la façon suivante :*

$$V_{E,\Lambda} = \begin{pmatrix} \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1}\rangle_{\zeta_1} & \ldots & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_D}\rangle_{\zeta_1} \\ \vdots & & \vdots \\ \langle \Lambda_{\mu_1}^{1}, \mathbf{x}^{\alpha_1}\rangle_{\zeta_1} & & \langle \Lambda_{\mu_1}^{(1)}, \mathbf{x}^{\alpha_d}\rangle_{\zeta_1} \\ \vdots & & \vdots \\ \langle \Lambda_1^{(d)}, \mathbf{x}^{\alpha_1}\rangle_{\zeta_d} & & \langle \Lambda_1^{(d)}, \mathbf{x}^{\alpha_D}\rangle_{\zeta_d} \\ \vdots & & \vdots \\ \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1}\rangle_{\zeta_d} & & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1}\rangle_{\zeta_d} \end{pmatrix}.$$

*Le déterminant de Vandermonde associé à $\Lambda$ et $E$ est défini par $\mathbf{v}_{\Lambda,E} = det(V_{\Lambda,E})$.*

**Théorème 2.4.13** *Soient $\mathcal{Z} = \{\zeta_1,\ldots,\zeta_d\} \subset \mathbb{K}^n$ et $E = \{\alpha_1,\ldots,\alpha_D\} \subset \mathbb{N}^n$. Alors $\mathbf{x}^E$ est une base monomiale de $\mathcal{A}_\Lambda = \mathbb{K}[x_1,\ldots,x_n]/\mathcal{I}_\Lambda$ si et seulement si le déterminant de Vandermonde $\mathbf{v}_{\Lambda,E} \neq 0$.*

*Preuve* : La preuve n'est pas fondamentalement différente de celle du cas des racines simples. On sait que $\left(\Lambda_j^{(i)} \mid i \in \{1,\ldots,d\}, j \in \{1,\ldots,\mu_i\}\right)$ est une base de $\mathcal{I}_\Lambda^\perp = \widehat{\mathcal{A}}_\Lambda$. On remarque alors que la $i$-ème colonne de la matrice de Vandermonde est formée par les coordonnées de $\mathbf{x}^{\alpha_i}$ dans la base $\mathcal{A}_\Lambda$ duale de la base $\left(\Lambda_j^{(i)}\right)$ pour la forme bilinéaire $\langle .,.\rangle_{\mathcal{Z}(\mathcal{I}_\Lambda)}$. Donc, comme dans le cas des racines simples, si le déterminant de cette matrice est non nul, alors la transposée de cette matrice est une matrice de changement de bases et si son déterminant est nul, alors la famille $(\mathbf{x}^\alpha)$ est liée dans $\mathcal{A}_\Lambda$ et elle ne peut pas en être une base. ♣

**Définition 2.4.14** *Soient $\mathcal{Z} = \{\zeta_1,\ldots,\zeta_d\} \subset \mathbb{K}^n$ et $E = \{\alpha_1,\ldots,\alpha_D\} \subset \mathbb{N}^n$ tels que $\mathbf{x}^E$ est une base monomiale de $\mathcal{A}_\Lambda = \mathbb{K}[x_1,\ldots,x_n]/\mathcal{I}_\Lambda$. On définit les polynômes de Lagrange $\mathbf{e}_i^{(j)}$, $j \in \{1,\ldots,\mu_i\}$, associés à $\zeta_i$ de la façon* *suivante :*

$$\mathbf{e}_i^{(j)} = \frac{-1}{\mathbf{v}_{\Lambda,E}} det \begin{pmatrix} \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_D} \\ \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_{\mu_1}^{(1)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_1} \\ \vdots & & \vdots \\ \langle \Lambda_{j-1}^{(i)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_i} & & \langle \Lambda_{j-1}^{(i)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_i} \\ \langle \Lambda_{j+1}^{(i)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_i} & & \langle \Lambda_{j+1}^{(i)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_i} \\ \vdots & & \vdots \\ \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} & \cdots & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_d} \end{pmatrix}$$

*pour tout* $i \in \{1, \ldots, d\}$ *et* $j \in \{1, \ldots, \mu_i\}$.

**Proposition 2.4.15** *Les polynômes* $\mathbf{e}_i^{(1)}$, $i \in \{1, \ldots, d\}$, *sont les idempotents associés aux* $\zeta_i$, $i \in \{1, \ldots, d\}$ *et les familles* $\left(\mathbf{e}_i^{(1)}, \ldots, \mathbf{e}_i^{(\mu_i)}\right)$ *sont des bases des algèbres locales* $\mathcal{A}_{\zeta_i}$, $i \in \{1, \ldots, d\}$.

*Preuve* : On remarque que :

$$\langle \Lambda_j^{(i)}, \mathbf{e}_{i'}^{(j')} \rangle_{\zeta_i} = \frac{-1}{\mathbf{v}_{\Lambda,E}} \begin{pmatrix} \langle \Lambda_j^{(i)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_i} & \cdots & \langle \Lambda_j^{(i)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_i} \\ \vdots & & \vdots \\ \langle \Lambda_1^{(i')}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_{i'}} & \cdots & \langle \Lambda_1^{(i')}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_{i'}} \\ \vdots & & \vdots \\ \langle \Lambda_{j'-1}^{(i')}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_{i'}} & \cdots & \langle \Lambda_{j'-1}^{(i')}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_{i'}} \\ \langle \Lambda_{j'+1}^{(i')}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_{i'}} & \cdots & \langle \Lambda_{j'+1}^{(i')}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_{i'}} \\ \vdots & & \vdots \\ \langle \Lambda_{\mu_{i'}}^{(i')}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_{i'}} & \cdots & \langle \Lambda_{\mu_{i'}}^{(i')}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_{i'}} \end{pmatrix} = \delta_{i,i'}\delta_{j,j'}$$

Ainsi les éléments $\mathbf{e}_i^{(j)}$, $j \in 1, \ldots, \mu_i$ forment une base duale de la base $\left(\Lambda_j^{(i)}\right)$ de $D_{\zeta_i}$. De plus, comme les $\mathbf{e}_i^{(1)}$ sont les éléments duaux des $\Lambda_1^{(j)} = 1$, alors $\mathbf{e}_i^{(1)}$ est l'idempotent associé à $\zeta_i$. On a aussi, puisque les $\Lambda_2^{(i)}, \ldots, \Lambda_{\mu_i}^{(i)}$ sont sans termes constants, les $\mathbf{e}_i^{(2)}, \ldots, \mathbf{e}_i^{(\mu_i)}$ qui sont dans l'idéal maximal $\mathbf{m}_{\zeta_i}$ de $\mathcal{A}_{\zeta_i}$. ♣

**Proposition 2.4.16** *Sous les hypothèses précédentes et avec les mêmes notations, pour tout* $f$ *dans* $\mathcal{A}$, *on a* $f = \sum_{i=1}^{d} \sum_{j=1}^{\mu_i} \langle \Lambda_j^{(i)}, f \rangle_{\zeta_i} \mathbf{e}_i^{(j)}$.

*Preuve* : Il s'agit simplement d'un corollaire du fait que $\Lambda_j^{(i)}$ et $\mathbf{e}_i^{(j)}$ sont duaux pour $\langle .,. \rangle$. ♣

Cette dernière proposition donne directement une solution au problème d'Hermite généralisé. C'est ce que nous explicitons dans le théorème suivant :

**Théorème 2.4.17** *Sous les hypothèses précédentes et avec les mêmes notations, alors* $\forall (v_{1,1}, \ldots, v_{1,\mu_i}, \ldots, v_{d,1}, \ldots, v_{d,\mu_d}) \in \mathbb{K}^D$*, il existe un unique polynôme* $f \in \mathcal{A}_\Lambda$ *tel que pour tout* $i \in \{1, \ldots, d\}$ *et* $j \in \{1, \ldots, \mu_i\}$*, on a* $\langle \Lambda_j^{(i)}, f \rangle_{\zeta_i} = v_{i,j}$ *et ce polynôme est donné par :*

$$f(\mathbf{x}) = \sum_{i=1}^{d} \sum_{j=1}^{\mu_i} v_{i,j} \mathbf{e}_i^{(j)}(\mathbf{x}) \tag{2.2}$$

**Remarque 2.4.18** *On remarque qu'on n'a fait aucune hypothèse sur le type d'intersection de l'idéal* $\mathcal{I}_\Lambda$*. Cela rend notre approche très générale et permet d'envisager un grand nombre d'applications à ce genre de méthodes d'interpolation.*

### 2.4.4 Polynômes de relation

On introduit maintenant des polynômes qui joueront un rôle important dans l'étude des relations entre coefficients d'un système algébrique et les coordonnées des zéros de ce système, la construction de systèmes contenant un ensemble algébrique donné comme sous-ensemble de son ensemble de solutions et dans la conception de méthodes itératives pour la résolution de systèmes algébriques. On se place sous les mêmes hypothèses que pour l'interpolation de Hermite généralisée.

Soit $Q \in \mathbb{K}[x_1, \ldots, x_n]$, on note $N_Q(\mathbf{x}) = \sum_{\alpha \in E} n_{Q,\alpha} \mathbf{x}^\alpha$ la forme normale de $Q$ dans la base $\mathbf{x}^E$ modulo un idéal $\mathcal{I}_\lambda$ représenté de la même façon que pour l'interpolation d'Hermite. On considère alors le polynôme $P_Q(\mathbf{x}) = Q(\mathbf{x}) - N_Q(\mathbf{x})$. On a alors $P_Q \in \mathcal{I}_\Lambda$.

**Définition 2.4.19** *On définit le polynôme* $R_Q(\Lambda, \mathbf{x})$ *comme le déterminant suivant :*

$$R_Q(\Lambda, \mathbf{x}) = \begin{vmatrix} Q(\mathbf{x}) & \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_D} \\ \langle \Lambda_1^{(1)}, Q(\mathbf{x}) \rangle_{\zeta_1} & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_1} \\ \vdots & \vdots & \ddots & \vdots \\ \langle \Lambda_{\mu_d}^{(d)}, Q(\mathbf{x}) \rangle_{\zeta_d} & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} & \cdots & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_D} \rangle_{\zeta_d} \end{vmatrix} \tag{2.3}$$

On vérifie facilement les propriétés suivantes :

**Propriétés 2.4.20**

- $R_Q(\Lambda, \zeta_i) = 0$,
- $R_Q(\Lambda, \mathbf{x}) = \mathbf{v}_{\Lambda,\mathbf{x}} P_Q(\mathbf{x})$.

Nous allons maintenant donner une propriété importante de ces polynômes. Pour tout $i \in \{1, \ldots, n\}$, on note $\nu_i = (\delta_{i,j})_{j \in \{1,\ldots,n\}} \in \mathbb{N}^n$. Soit $Q \in \mathbb{K}[x_1, \ldots, x_n] \setminus \mathbb{K}[x_1, \ldots, x_n]_E$. Alors les dérivées partielles de $R_Q$ par rapport aux coordonnées des $\zeta_i$ vérifient :

**Proposition 2.4.21**

$$\frac{\partial}{\partial \zeta_{i,j}} R_Q(\Lambda, \mathbf{x}) = \sum_{k=1}^{\mu_i} \langle \Lambda_k^{(i)}, \frac{\partial}{\partial x_j} R_Q(\Lambda, \mathbf{x}) \rangle_{\zeta_i} \mathbf{e}_i^{(k)} \in \mathcal{A}_{\zeta_i} \tag{2.4}$$

*Preuve* : On revient à l'expression déterminantale de $R_Q(\Lambda, \mathbf{x})$ pour obtenir :

$$\frac{\partial}{\partial \zeta_{i,j}} R_Q(\Lambda, \mathbf{x}) = \frac{\partial}{\partial \zeta_{i,j}} \begin{vmatrix} Q(\mathbf{x}) & \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_D} \\ \langle \Lambda_1^{(1)}, Q \rangle_{\zeta_1} & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} \\ \vdots & \vdots & \ddots & \vdots \\ \langle \Lambda_{\mu_d}^{(d)}, Q \rangle_{\zeta_d} & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} & \cdots & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} \end{vmatrix}$$

D'où l'on tire facilement l'égalité suivante :

$$\frac{\partial}{\partial \zeta_{i,j}} R_Q(\Lambda, \mathbf{x}) = \begin{vmatrix} Q(\mathbf{x}) & \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_D} \\ \langle \Lambda_1^{(1)}, Q \rangle_{\zeta_1} & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} & \cdots & \langle \Lambda_1^{(1)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_1} \\ \vdots & \vdots & \ddots & \vdots \\ \langle \Lambda_1^{(i)}, \frac{\partial}{\partial x_j} Q \rangle_{\zeta_i} & \langle \Lambda_1^{(i)}, \frac{\partial}{\partial x_j} \mathbf{x}^{\alpha_1} \rangle_{\zeta_i} & \cdots & \langle \Lambda_1^{(i)}, \frac{\partial}{\partial x_j} \mathbf{x}^{\alpha_d} \rangle_{\zeta_i} \\ \vdots & \vdots & \cdots & \vdots \\ \langle \Lambda_{\mu_i}^{(i)}, \frac{\partial}{\partial x_j} Q \rangle_{\zeta_i} & \langle \Lambda_{\mu_i}^{(i)}, \frac{\partial}{\partial x_j} \mathbf{x}^{\alpha_1} \rangle_{\zeta_i} & \cdots & \langle \Lambda_{\mu_i}^{(i)}, \frac{\partial}{\partial x_j} \mathbf{x}^{\alpha_d} \rangle_{\zeta_i} \\ \vdots & \vdots & \cdots & \vdots \\ \langle \Lambda_{\mu_d}^{(d)}, Q \rangle_{\zeta_d} & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} & \cdots & \langle \Lambda_{\mu_d}^{(d)}, \mathbf{x}^{\alpha_1} \rangle_{\zeta_d} \end{vmatrix}$$

On remarque alors que $R_Q(\Lambda, \zeta_k) = 0$ si $i \neq k$. Donc $\frac{\partial}{\partial \zeta_{i,j}} R_Q(\Lambda, \mathbf{x}) \in \mathcal{A}_{\zeta_i}$. ♣

**Corollaire 2.4.22** *Si la racine $\zeta_i$ est simple, alors :*

$$\frac{\partial}{\partial \zeta_{i,j}} R_Q(\Lambda, \mathbf{x}) = \langle 1, \frac{\partial}{\partial x_j} R_Q(\Lambda, \mathbf{x}) \rangle_{\zeta_i} \mathbf{e}_{\zeta_i} = \frac{\partial R_Q}{\partial x_j}(\Lambda, \zeta_i) \, \mathbf{e}_{\zeta_i}.$$

### 2.4.5 Relations entre racines et coefficients

Nous donnons maintenant des relations entre les coefficients d'un système algébrique définissant un idéal de dimension 0 et les racines de ce système. Ces relations étendent naturellement les relations entre coefficients et racines données par les fonctions symétriques élémentaires dans le cadre univarié. Soient donc $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ tels que l'idéal $\mathcal{I} = (f_1, \ldots, f_m)$ soit de dimension zéro. On note par $\mathcal{Z}(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_d\}$ l'ensemble algébrique qui lui est associé et $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ son algèbre des coordonnées. On suppose connue $\mathbf{x}^E$, une base monomiale de $\mathcal{A}$ et $\left(\Lambda_j^{(i)}\right)_{j\in\{1,\ldots,\mu_i\}}$, $i \in \{1, \ldots, d\}$, des bases duales des algèbres locales $\mathcal{A}_{\zeta_i}$.

Soit $Q \in \mathbb{K}[x_1, \ldots, x_n]$, on note par $N_Q(\mathbf{x}) = \sum_{\alpha\in E} n_{Q,\alpha}\mathbf{x}^\alpha$ la forme normale de $Q$ dans la base $\mathbf{x}^E$ de $\mathcal{A}$. En corollaire des propriétés 2.4.20, on a $\frac{R_{f_i}(\Lambda,x)}{\mathbf{v}_{\Lambda,E}} = f_i(\mathbf{x})$ pour tout $i \in \{1, \ldots, m\}$. On décompose alors chacun des $f_i(\mathbf{x}) = \sum_{\alpha\in\mathbb{N}^n} f_{i,\alpha}\mathbf{x}^\alpha$ de la façon suivante : $\overline{f_i} + \sum_{\alpha\in E} f_{i,\alpha}\mathbf{x}^\alpha$ où $\overline{f_i}$ a un support monomial disjoint de $\mathbf{x}^E$. On a alors $\frac{R_{\overline{f_i}}(\Lambda,\mathbf{x})}{\mathbf{v}_{\Lambda,E}} = \overline{f_i}(\mathbf{x}) - N_{\overline{f_i}}(\mathbf{x}) = f_i(\mathbf{x})$ puisque $N_{f_i}(\mathbf{x}) = 0$, et ainsi $\sum_{\alpha\in E} f_{i,\alpha}\mathbf{x}^\alpha = N_{\overline{f_i}}(\mathbf{x})$. On en déduit que

$$\frac{R_{\overline{f_i}}(\Lambda,\mathbf{x})}{\mathbf{v}_{\Lambda,E}} - \overline{f_i} = \sum_{\alpha\in E} f_{i,\alpha}\mathbf{x}^\alpha.$$

On note $\left|R_{\overline{f_i}}(\Lambda,\mathbf{x})\right|_{\alpha_i}$ le mineur de la matrice associée à $R_{\overline{f_i}}(\Lambda,\mathbf{x})$ obtenue en retirant la première ligne et la colonne correspondant à $\mathbf{x}^{\alpha_i}$, pour $i \in \{1, \ldots, D\}$. Le théorème suivant est alors facile à vérifier :

**Théorème 2.4.23** *Soit $i \in \{1, \ldots, D\}$, on a* $\left|\frac{R_{\overline{f_i}}(\Lambda,\mathbf{x})}{\mathbf{v}_{\Lambda,E}}\right|_\alpha = f_{i,\alpha}$.

*Preuve :* On a $\left|\frac{R_{\overline{f_i}}(\Lambda,\mathbf{x})}{\mathbf{v}_{\Lambda,E}}\right|_\alpha$ qui est le mineur de la matrice associée à $R_{\overline{f_i}}(\Lambda,\mathbf{x})$ obtenu en enlevant la première ligne et la colonne indexée par $\mathbf{x}^\alpha$ puis en divisant par $\mathbf{v}_{\Lambda,E}$. C'est donc le coefficient de $\mathbf{x}^\alpha$ dans le polynôme $\frac{R_{\overline{f_i}}(\Lambda,\mathbf{x})}{\mathbf{v}_{\Lambda,E}}$, ce qui prouve le théorème puisque par définition $\overline{f_i}$ ne contient pas $\mathbf{x}^\alpha$ dans son support. ♣

Cette dernière égalité généralise les relations bien connues entre les fonctions symétriques des racines et les coefficients d'une équation algébrique univariée.

### 2.4.6 Application des polynômes de relation à l'interpolation

On s'intéresse ici à un nouveau problème d'interpolation qui est une variante du problème d'Hermite. On considère des points $\{\zeta_1, \ldots, \zeta_d\} \subset \mathbb{K}^n$ distincts et des conditions différentielles $\left(\Lambda_j^{(i)}\right)_{i\in\{1,\ldots,\mu_i\}}$, $i \in \{1, \ldots, d\}$ vérifiant les mêmes hypothèses que pour l'interpolation d'Hermite. On a donc un idéal $\mathcal{I}_\Lambda$ et une algèbre $\mathcal{A}_\Lambda$ dont on suppose connaître une base monomiale $\mathbf{x}^E$. Le problème est ici de construire une famille de polynômes engendrant $\mathcal{I}_\Lambda$. Dans le cas où toutes les racines sont simples, le problème consiste à trouver une famille de polynômes définissant la variété algébrique $\{\zeta_1, \ldots, \zeta_d\}$.

**Définition 2.4.24** *On note $\Omega = \{\beta \in \mathbb{N}^n \,|\, \exists \alpha \in E$ et $k \in \{1, \ldots, n\}$ avec $x_k \mathbf{x}^\alpha = \mathbf{x}^\beta$ et $\beta \notin E\}$. Cet ensemble est appelé, par abus de langage, la frontière du quotient.*

**Proposition 2.4.25** *L'ensemble $\{R_{x^\beta}(\Lambda, \mathbf{x}) \,|\, \beta \in \Omega\}$ est une solution du problème d'Hermite modifié, c'est-à-dire que $(R_{x^\beta}(\Lambda, \mathbf{x}))_{\beta\in\Omega} = \mathcal{I}_\Lambda$. De plus comme $\mathcal{Z}\left((R_{x^\beta}(\Lambda, \mathbf{x}))_{\beta\in\Omega}\right) = \{\zeta_1, \ldots, \zeta_d\}$, si on note $\mathcal{A}_{\zeta_i}$ l'algèbre locale associée à $\zeta_i$ dans $\mathbb{K}[x_1, \ldots, x_n]/(R_{x^\beta}(\Lambda, \mathbf{x}))_{\beta\in\Omega}$ alors $\mathcal{A}_{\zeta_i} = \langle \Lambda_j^{(i)} | j \in \{1, \ldots, \mu_i\}\rangle^\perp$, pour tout $i \in \{1, \ldots, d\}$.*

*Preuve :* On montre d'abord que $\mathbf{x}^E$ est une base de $\mathbb{K}[x_1, \ldots, x_n]/(R_{x^\beta}(\Lambda, \mathbf{x}))_{\beta\in\Omega}$. Si $\gamma \in \mathbb{N}^n$ est tel que $\mathbf{x}^\gamma$ ne soit pas dans $E$ alors il serait réductible par un $\mathbf{x}^\beta$, $\beta \in \Omega$. Donc $\mathbf{x}^E$ est une famille génératrice du quotient. Puisque le déterminant de Vandermonde $\mathbf{v}_{\Lambda,E}$ est non nul, c'est une famille libre. Par conséquent, $\mathbf{x}^E$ est une base de $\mathcal{A}_\Lambda$. On a $\{\zeta_1, \ldots, \zeta_d\} \subset \mathcal{Z}\left((R_{\mathbf{x}^\beta}(\Lambda, \mathbf{x}))_{\beta\in\omega}\right)$ par construction. De plus, toujours par construction, $\langle \Lambda_j^{(i)}, R_{\mathbf{x}^\beta}(\Lambda, \mathbf{x})\rangle_{\zeta_i} = 0$. Donc $\zeta_i$ a au moins la multiplicité $\mu_i$. Comme $\mathbf{x}^E$ est une base de $\mathcal{A}_\Lambda$ et que $\sum_{i=1}^{d} \mu_i = \#(E)$, la multiplicité de $\zeta_i$ dans $\mathcal{Z}\left((R_{\mathbf{x}^\beta}(\Lambda, \mathbf{x}))_{\beta\in\omega}\right)$ est exactement $\mu_i$. ♣

Si on choisit un système de générateurs d'exactement $n$ polynômes, ce système définit un ensemble algébrique contenant $\{\zeta_1, \ldots, \zeta_d\}$. Le problème de définir $\mathcal{A}_\Lambda$ comme une intersection complète est un problème beaucoup plus difficile. Dans notre approche, nous choisissons beaucoup trop de générateurs. Le problème de trouver un nombre de générateurs minimal de l'idéal revient alors à trouver une famille $f_\beta \in \mathbb{K}[x] \setminus \mathbb{K}[x_1, \ldots, x_n]_E$ minimale dont les initiaux d'une base de Gröbner définissent $\Omega$ comme "escalier". Cette formulation révèle la difficulté de la question posée. C'est l'objet de ce qui suit, même si on se limite au cas des racines simples.

Nous retrouverons des questions analogues dans le cadre des méthodes de Weierstrass modifiées, où les questions de platitudes d'homotopies sont cruciales.

## 2.5 Deux autres problèmes d'interpolation

### 2.5.1 Restriction d'idéaux

On s'intéresse ici au problème suivant : on se donne un ensemble de points $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_d\}$ dans $\mathbb{K}^n$, d'algèbre des coordonnées $\mathcal{A}$ pour laquelle on suppose que toutes les racines sont simples (i.e. cette algèbre est réduite) et dont on suppose connaître une base monomiale $\mathbf{x}^E$. On cherche alors à décrire une famille de polynômes $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ définissant un idéal $\mathcal{I}_{\mathcal{A}}$ tel que $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_{\mathcal{A}}$. De plus on souhaiterait que $m$ soit le plus proche possible de $n$.

**Proposition 2.5.1** *Soient $X$ et $Y$ avec $Y \subset X$ deux sous-ensembles finis de $\mathbb{K}^n$, on a alors :*

$$\mathcal{I}_{(X\setminus Y)} = \mathcal{I}_X + \left(\sum_{\mathbf{z}\in Y} \mathbf{e_z}(\mathbf{x})\right) = \mathcal{I}_X + \sum_{\mathbf{z}\in Y} (\mathbf{e_z}(\mathbf{x}))\,.$$

*Preuve* : On commence par remarquer que dans $\mathcal{A}_X$ on a $\left(\sum_{\mathbf{z}\in Y} \mathbf{e_z}(\mathbf{x})\right) = \sum_{\mathbf{z}\in Y} (\mathbf{e_z}(\mathbf{x}))$ puisque les idéaux $(\mathbf{e_z}(\mathbf{x}))$ sont premiers entre eux dans $\mathcal{A}_X$ car les polynômes $\mathbf{e_z}(\mathbf{x})$ sont premiers entre eux dans $\mathcal{A}_X$.

Soit $p \in \mathcal{I}_X + \sum_{\mathbf{z}\in Y} (\mathbf{e_z}(\mathbf{x}))$ non nul, alors $p(\mathbf{x}) = \sum_{\mathbf{z}\in Y} p_\mathbf{z}\mathbf{e_z}(\mathbf{x})$ dans $\mathcal{A}_X$ avec les $p_\mathbf{z}$ non tous nuls. On a donc pour tout $\mathbf{w} \in X\setminus Y$, $p(\mathbf{w}) = \sum_{\mathbf{z}\in Y} p_\mathbf{z}\mathbf{e_z}(\mathbf{w}) = 0$ dans $\mathcal{A}_X$. De plus il existe $\mathbf{y} \in Y$ tel que $p_\mathbf{y} \neq 0$ et alors $p(\mathbf{y}) = p_\mathbf{y} \in \mathcal{A}_X$. Donc $p \in \mathcal{I}_{X\setminus Y}$. Donc $\mathcal{I}_X + \sum_{\mathbf{z}\in Y} (\mathbf{e_z}(\mathbf{x})) \subset \mathcal{I}_{X\setminus Y}$.

Soit $p \in \mathcal{I}_{(X\setminus Y)}$, et supposons que $p \notin \mathcal{I}_X + \sum_{\mathbf{z}\in Y} (\mathbf{e_z}(\mathbf{x}))$. Dans $\mathcal{A}_x$ on a $p(\mathbf{x}) = \sum_{\mathbf{z}\in X} p_\mathbf{z}\mathbf{e_z}(\mathbf{x})$. Comme $p \in \mathcal{I}_{X\setminus Y}$, on a $p_\mathbf{w} = 0$, $\forall \mathbf{w} \in X \setminus Y$ puisque

$p(\mathbf{w}) = p_{\mathbf{w}}$. Donc $p(\mathbf{x}) = \sum_{\mathbf{y}\in Y} p_{\mathbf{y}}\mathbf{e}_{\mathbf{y}}(\mathbf{x})$ ce qui contredit l'hypothèse et $\mathcal{I}_{X\setminus Y} \subset \mathcal{I}_X + \sum_{\mathbf{z}\in Y}(\mathbf{e}_{\mathbf{z}}(\mathbf{x}))$. ♣

Pour des raisons pratiques, nous nous placerons systèmatiquent sous l'hypothèse suivantes :

**Hypothèse 2.5.2** *On suppose que tous les points de $Z$ ont leurs coordonnées distinctes deux à deux, i.e. en notant $\zeta_i = (\zeta_{i,1}, \ldots, \zeta_{i,n})$, $\zeta_{i,l} \neq \zeta_{j,k}$ si $i \neq j \in \{1, \ldots, D\}$ et $k \neq l \in \{1, \ldots, n\}$.*

**Proposition 2.5.3** *L'idéal $\mathcal{I}_Z$ est engendré par un idéal engendré par $n+1$ polynômes.*

*Preuve* : On note $\zeta_i = (\zeta_{i,1}, \ldots, \zeta_{i,n})$ pour tout $i \in \{1, \ldots, D\}$. On considère alors les polynômes $p_j\,(x_j)\,\mathbb{K}[x_i]$ ,pour $j \in \{1, \ldots, n\}$, définis par $p_i\,(x_i) = \prod_{i=1}^{D}(x_i - \zeta_{i,j})$. On a $(p_1, \ldots, p_n) \subset \mathcal{I}_Z$. Ils définissent un ensemble algébrique $X$ fini et on note $Y = X - Z$ qui est aussi un ensemble fini. On applique alors la proposition précédente pour avoir $\mathcal{I}_Z = \mathcal{I}_{X-Y}$. ♣

Ces deux dernières propositions permettent d'ailleurs de construire effectivement les $n{+}1$ générateurs de $\mathcal{I}_Z$ en admettant que l'hypothèse précédente est vérifiée (elle l'est toujours modulo un changement linéaire de coordonnées), c'est lobjet de la proposition suivante :

**Proposition 2.5.4** *Sous l'hypothèse précédente, l'idéal $\mathcal{I}_Z$ est défini par les polynômes $p_i\,(x_i) = \prod_{j=1}^{D}(x_i - \zeta_{j,i})$,$i \in \{1, \ldots, D\}$ et par le polynôme $\chi$ défini comme suit : on considère l'ensemble $Y$ des points de la forme $(\zeta_{i_1,1}, \ldots, \zeta_{i_n,n})$ avec les $i_j$ non tous égaux. On définit alors $\chi = \sum_{\mathbf{y}\in Y} \mathbf{e}_{\mathbf{y}}$.*

*Preuve* : La variété définie par les $p_i$, $i \in \{1, \ldots, n\}$ est exactement $X = \mathcal{Z} \cup Y$. On applique alors le théorème précédent à $X \setminus Y$. ♣

Bien qu'on ait défini $\mathcal{Z}$ avec $n+1$ polynômes, le calcul du polynôme $\chi$ reste un facteur limitatif. En effet, l'ensemble $Y$ contient $n^D - D$ points, puisque $X$ en contient $n^D$ et que $\mathcal{Z}$ en contient $D$. De plus, il faudrait une base monomiale de $\mathcal{A}_X$ pour mener à bien ce calcul, ce qui impliquerait de manipuler des matrices carrées de taille $n^D$.

### 2.5.2 Configurations de points et restrictions d'idéaux

Dans la sous-section précédente, on a vu que si $\mathcal{I}$ et $\mathcal{J}$ sont deux idéaux radicaux de dimension zéro tels que $\mathcal{J} \subset \mathcal{I}$, alors on peut toujours trouver un polynôme $h \in \mathbb{K}[x_1, \ldots, x_n]$ tel que $\mathcal{I} = \mathcal{J} + (h)$. Dans cette nouvelle sous-section on est intéressé par un problème de même nature. En effet, la solution proposée pour calculer le polynôme $h$ à partir des idempotents de $\mathcal{B} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{J}$ associés aux zéros supplémentaires de $\mathcal{J}$ implique de connaître beaucoup d'informations sur $\mathcal{B}$. Dans cette sous-section, nous nous intéressons à une méthode de calcul d'un polynôme $h \in \mathbb{K}[x_1, \ldots, x_n]$ tel que $\mathcal{I} = \mathcal{J} + (h)$ en utilisant uniquement des informations sur $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ et des polynômes de relation. Nous cherchons des informations de deux types : quels polynômes $h$ peut-on rajouter pour avoir génériquement $\mathcal{I} = \mathcal{J} + (h)$ ? Et dans le cas où on connaît de tels polynômes, quelles sont les conditions sur la configuration des zéros de $\mathcal{J}$ pour que les polynômes calculés n'excluent pas tous les zéros supplémentaires.

#### Construction de conditions algébriques

On considère $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ des polynômes en intersection complète. On note $F = (f_1, \ldots, f_n)$ l'idéal qu'ils engendrent et $\mathcal{Z} = Z(F) = \{\zeta_1, \ldots, \zeta_d\} \subset \mathbb{K}^n$ l'ensemble algébrique associé. Toutes les racines sont supposées simples, i.e. de multiplicité 1 dans $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/F$.

On considère une autre famille de polynômes $g_1, \ldots, g_n \in \mathbb{K}[x_1, \ldots, x_n]$ en intersection complète. On note $G = (g_1, \ldots, g_n)$ l'idéal qu'ils engendrent et $X = Z(G)$ l'ensemble algébrique associé.

On suppose que $G \subset F$, ou de façon équivalente que $\mathcal{Z} \subset X$. On suppose que toutes les racines communes de $F$ et $G$ sont simples dans $\mathcal{B} = \mathbb{K}[x_1, \ldots, x_n]/G$.

Soit $E = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{N}^n$ tel que $\mathbf{x}^E$ soit une base monomiale de $\mathcal{A}$. Soit $p \in \mathbb{K}[x_1, \ldots, x_n]$ un polynôme tel que son support monomial contienne au moins un monôme qui n'est pas dans $\mathbf{x}^E$, on note alors $h = R_p(\mathcal{Z}, \mathbf{x})$ le polynôme de relation qui lui est associé.

**Définition 2.5.5** *Un polynôme $p \in \mathbb{K}[x_1, \ldots, x_n]$ tel que $G + (p) = F$ est appelé un polynôme séparant de $\mathcal{Z}$ relativement à $X$.*

On donne maintenant une caractérisation des polynômes de relation qui sont des séparants de $\mathcal{Z}$ relativement à $X$ :

**Proposition 2.5.6** *Soit $p \in \mathbb{K}[x_1, \ldots, x_n]$ un polynôme dont le support monomial contient au moins un monôme qui n'est pas dans $\mathbf{x}^E$. Alors $R_p(\mathcal{Z}, \mathbf{x})$*

*est un polynôme séparant de $\mathcal{Z}$ relativement à $X$ si et seulement si pour tout $\xi \in X \setminus \mathcal{Z}$, $R_p(\mathcal{Z}, \mathbf{x}) \neq 0$.*

*Preuve :* On commence par remarquer que $h(\mathbf{x}) = R_p(\mathcal{Z}, \mathbf{x}) \in F$. Alors s'il existe $\xi \in X$ tel que $h(\xi) = 0$, on a $Z(G + (h))$ qui contient strictement $\mathcal{Z}$ et $\xi$. Donc $\mathcal{Z}$ est strictement inclus dans $G + (h)$. Supposons alors que pour tout $\xi \in X$, on a $h(\xi) \neq 0$, alors $(h) \subset F$, donc comme $G \subset F$, on a $F \subset G + (h)$. Comme l'inclusion dans l'autre sens est toujours vérifiée, la proposition est démontrée. ♣

Dans la sous-section suivante, on s'intéresse au lien entre les configurations de points de $X$ et au fait qu'un polynôme de relation soit un séparant de $\mathcal{Z}$ relativement à $X$.

### Configurations de points et polynômes séparants

On cherche maintenant à savoir sous quelles conditions, pour un polynôme de relation donné, il existe un $\xi \in X \setminus \mathcal{Z}$ tel que ce polynôme ne s'annule pas en $\xi$. On commence par le cas d'un polynôme de relation associé à un monôme. Soit $E = \{\alpha_1, \ldots, \alpha_d\} \subset \mathbb{N}^n$ tel que $\mathbf{x}^E$ soit une base monomiale de $\mathcal{A}$. Soit $\beta \in \mathbb{N}^n \setminus E$, on note $h(\mathbf{x}) = R_{\mathbf{x}^\beta}(\mathcal{Z}, \mathbf{x})$. Par définition des polynômes de relation, on a :

$$h(\mathbf{x}) = \begin{vmatrix} \mathbf{x}^\beta & \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_d} \\ \zeta_1^\beta & \zeta_1^{\alpha_1} & \cdots & \zeta_1^{\alpha_d} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_d^\beta & \zeta_d^{\alpha_1} & \cdots & \zeta_d^{\alpha_d} \end{vmatrix}.$$

Si $h(\xi) = 0$, et comme :

$$h(\xi) = \begin{vmatrix} \xi^\beta & \xi^{\alpha_1} & \cdots & \xi^{\alpha_d} \\ \zeta_1^\beta & \zeta_1^{\alpha_1} & \cdots & \zeta_1^{\alpha_d} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_d^\beta & \zeta_d^{\alpha_1} & \cdots & \zeta_d^{\alpha_d} \end{vmatrix}.$$

On sait alors qu'il existe un unique (puisque le déterminant de Vandermonde est inversible) $d$-uplet $(\lambda_1, \ldots, \lambda_d)$, avec les $\lambda_i$ non tous nuls tel que :

$$\begin{cases} \xi^\beta = \displaystyle\sum_{i=1}^{d} \lambda_i \, \zeta_i^\beta \\ \xi^{\alpha_i} = \displaystyle\sum_{i=1}^{d} \lambda_i \, \zeta_i^{\alpha_i}, \; \forall i \in \{1, \ldots, d\} \end{cases} \tag{2.5}$$

On a alors facilement la proposition suivante :

**Proposition 2.5.7** *Une condition nécessaire et suffisante pour que $G + (h) \neq F$ est qu'il existe $\xi \in X \setminus \mathcal{Z}$ vérifiant les conditions (2.5).*

L'ensemble des points vérifiant la condition (2.5) est défini par $d+1$ équations algébriques, mais ces équations ne sont pas indépendantes. Cependant c'est au plus une hypersurface de $\mathbb{K}^n$. Il y a donc peu de configurations de points pour lesquelles $h$ ne sera pas un polynôme séparant de $\mathcal{Z}$ relativement à $X$. Dans ce qui suit on va voir qu'on peut augmenter le nombre de conditions sans pour cela augmenter le nombre de polynômes de relation.

Soient $k$ un entier et $C = \{\beta_1, \dots, \beta_k\} \subset \mathbb{N}^k \setminus E$. On considère alors un vecteur $(h_1, \dots, h_k) \in \mathbb{K}^k$ dont les coordonnées sont toutes non nulles. On considère alors le polynôme $H(\mathbf{x}) = \sum_{i=1}^{k} h_i \mathbf{x}^{\beta_i}$ et on définit $h(\mathbf{x}) = R_H(\mathcal{Z}, \mathbf{x})$. Comme précédemment on commence par supposer qu'il existe $\xi \in X \setminus \mathcal{Z}$ tel que $h(\xi) = 0$.

Si $h(\xi) = 0$, on a :

$$h_H(\xi) = \begin{vmatrix} H(\xi) & \xi^{\alpha_1} & \cdots & \xi^{\alpha_d} \\ H(\zeta_1) & \zeta_1^{\alpha_1} & \cdots & \zeta_1^{\alpha_d} \\ \vdots & \vdots & \dots & \vdots \\ H(\zeta_d) & \zeta_d^{\alpha_1} & \cdots & \zeta_d^{\alpha_d} \end{vmatrix} = 0.$$

Comme précédemment, la condition $h(\xi) = 0$ implique qu'il existe un unique $(\lambda_1, \dots, \lambda_d) \in \mathbb{K}^d$, dont les coordonnées sont non toutes nulles tel que :

$$H(\xi) = \sum_{i=1}^{d} \lambda_i H(\zeta_i). \tag{2.6}$$

Ce qu'on peut réécrire de la façon suivante :

$$\sum_{j=1}^{k} \xi^{\beta_j} = \sum_{i=1}^{n} \lambda_i \sum_{j=1}^{k} \zeta_i^{\beta_j}. \tag{2.7}$$

D'où on tire que :

$$\begin{cases} \xi^{\alpha_j} = \sum_{i=1}^{d} \lambda_i \zeta_i^{\alpha_j}, \, \forall j \in \{1, \dots, d\} \\ \xi^{\beta_j} = \sum_{i=1}^{d} \lambda_i \zeta_i^{\beta_j}, \, \forall j \in \{1, \dots, k\} \end{cases}. \tag{2.8}$$

On a alors facilement la proposition suivante :

**Proposition 2.5.8** *Une condition nécessaire et suffisante pour que* $G + (h) \neq F$ *est qu'il existe* $\xi \in X \setminus \mathcal{Z}$ *vérifiant le système d'équations (2.8).*

On voit que si toutes les équations du système (2.8) ne sont pas indépendantes, à chaque fois qu'on rajoute un monôme dans le support de $H$ tel qu'il donne une condition indépendante des autres, on fait chuter de 1 la dimension de la variété algébrique des points tels que $h$ n'est pas un polynôme séparant de $\mathcal{Z}$ relativement à $X$. Cette proposition nous fournit un outil qui nous sera très utile pour le contrôle du nombre de solutions dans les méthodes de calcul simultanés des racines par homotopie surcontrainte.

## 2.6 Conclusion

Dans ce chapitre nous avons décrit les structures algébriques associées aux ensembles algébriques de dimension zéro. Nous avons montré que le point de vue algébrique permettait d'obtenir des méthodes d'interpolation. Nous avons ainsi complètement traité les problèmes d'interpolation de Lagrange et d'Hermite dans le cas multivarié. Ces problèmes sont importants non seulement théoriquement, puisqu'ils nous ont permis de donner des relations entre coefficients et racines généralisant les relations connues en une variable, mais aussi pratiquement comme le montrera l'application que nous en ferons au chapitre 3 pour la conception de méthodes itératives pour le calcul simultané de toutes les racines d'un système algébrique.

# Chapitre 3

# Méthode d'approximation simultanée des solutions d'un système algébrique

## 3.1 Introduction

Dans ce chapitre, nous nous intéressons aux méthodes itératives pour le calcul simultané des solutions d'un système d'équations algébriques définissant un ensemble algébrique de dimension zéro. Les systèmes considérés ici sont des systèmes en intersection complète ou surcontraints avec comme corps de base $\mathbb{R}$ ou $\mathbb{C}$ (et même essentiellement $\mathbb{C}$).

Les idées soutenant ces méthodes remontent à Weierstrass pour le cas du calcul simultané des racines d'un polynôme univarié n'ayant que des racines simples. Nous rappelons brièvement le principe de la méthode de Weierstrass (c'est surtout cette dernière qui nous intéressera).

Soit $P$ un polynôme unitaire de degré $d$ n'ayant que des racines simples. On note $\Delta = \{\mathbf{z} \in \mathbb{C}^n \mid \exists i \text{ et } j \in \{1, \ldots, d\}, \, i \neq j, \text{ tels que } z_i = z_j\}$. On considère l'application suivante :

$$I : \left\{ \begin{array}{ccc} \mathbb{C}^d \setminus \Delta & \longrightarrow & \mathbb{C}^d \\ \mathbf{z} = (z_1, \ldots, z_d) & \longmapsto & I(\mathbf{z}) = (I_1(\mathbf{z}), \ldots, I_d(\mathbf{z})) \end{array} \right.$$

telle que :

$$I_i(\mathbf{z}) = z_i - \frac{P(z_i)}{\prod_{j \neq i} (z_i - z_j)}.$$

Soit $\mathbf{z}^{(0)} = \left(z_1^{(0)}, \ldots, z_d^{(0)}\right)$, on considère alors la suite des itérés de $\mathbf{z}^{(0)}$ par $I$, i.e. la suite $\left(\mathbf{z}^{(k)}\right)_{k_i n \mathbb{N}}$ définie par $\mathbf{z}^{(k)} = I^k\left(\mathbf{z}^{(0)}\right)$. Soit $(\zeta_1, \ldots, \zeta_d) \in \mathbb{K}^n$ un vecteur formé des racines de $P$, alors pour $\mathbf{z}^{(0)}$ dans un voisinage (suffisamment petit) de $(\zeta_1, \ldots, \zeta_d)$, la suite $\left(\mathbf{z}^{(k)}\right)_{k_i n \mathbb{N}}$ converge quadratiquement vers $(\zeta_1, \ldots, \zeta_d)$. Autrement dit, les itérés par $I$ permettent d'approximer simultanément toutes les racines de $P$.

On s'intéresse aussi à d'autres méthodes de ce type, obtenues à partir de fonctions d'itération différentes. Par exemple, la méthode d'Aberth correspond à la fonction d'itération

$$I^A(\mathbf{z}) = \left(I_1^A(\mathbf{z}), \ldots, I_d^A(\mathbf{z})\right)$$

avec

$$I_i^A(\mathbf{z}) = z_i - \frac{P(z_i)}{P'(z_i) - P(z_i)\sum_{j \neq i}(z_i - z_j)}.$$

La convergence locale de cette méthode est cubique.

Des logiciels de résolution d'équations algébriques reposent en partie sur ces fonctions d'itération, tel le logiciel MPsolve [13, 14] qui décompose la résolution en deux étapes. La première étape consiste à calculer des points initiaux garantissant, dans la seconde étape, la convergence de la méthode d'Aberth. Ce logiciel, très complexe, comprend une analyse des clusters (regroupements de racines proches) et une adaptation dynamique de l'arithmétique utilisée (bien que l'arithmétique des nombres flottants double précision suffise généralement). Notre approche est différente. Nous proposons d'utiliser la méthode de Weierstrass comme opérateur de correction dans un procédé de suivi de chemin. D'autres méthodes basées sur des méthodes d'homotopie existent, comme celles proposées par T. Y. Li [67] et J. Verschelde [94]. Ces deux méthodes utilisent la méthode de Newton comme opérateur de correction et suivent par conséquent les racines indépendamment. L'originalité de la méthode proposée ici, par rapport aux méthodes de ces deux auteurs, est de suivre un seul chemin pour toutes les racines à la fois.

Le reste de ce chapitre se décompose comme suit : nous construisons la fonction d'itération de Weierstrass dans le cadre univarié, en adoptant une approche algébrique. Nous introduisons ensuite l'approche due à A. Frommer et A. Bellido qui est un peu plus analytique. Dans une deuxième partie nous montrons comment l'approche algébrique au cadre multivarié à la méthode de Weierstrass, que nous étudions en détail, puis à la méthode d'Aberth pour laquelle nous ne possédons pas de démonstration suffisamment rigoureuse de la convergence dans le cas multivarié. Ensuite nous proposons d'utiliser la méthode de Weierstrass dans un procédé de suivi de chemin afin d'obtenir des méthodes globales dans le cas univarié et multivarié. Enfin nous exposons quelques expérimentations numériques.

## 3.2 Méthodes univariées

### 3.2.1 La méthode de Weierstrass univariée

On considère un polynôme $P \in \mathbb{K}[x]$ unitaire de degré $d$ n'ayant que des racines simples, c'est-à-dire que $P$ a des racines $\zeta_1, \ldots, \zeta_d$ distinctes, i.e. $\zeta_i \neq \zeta_j$ si $i \neq j$. Autrement dit, $p$ s'écrit de la façon suivante :

$$P(x) = \prod_{i=1}^{d} (x - \zeta_i) = x^d + \sum_{i=0}^{d-1} p_i x^i \tag{3.1}$$

Nous avons déjà introduit les fonctions symétriques élémentaires sur $\mathbb{K}^d$ :

$$\sigma_i(\mathbf{z}) = (-1)^i \sum_{j_1 < \ldots < j_i} z_{j_1} \cdots z_{j_i}. \tag{3.2}$$

Une simple identification dans l'égalité 3.1 permet de constater que $\sigma_i(\zeta_1, \ldots, \zeta_d) = p_i, \forall i \in \{1, \ldots, d\}$. On définit alors l'application :

$$\Sigma(\mathbf{z}) = \begin{pmatrix} \sigma_1(\mathbf{z}) - p_1 \\ \vdots \\ \sigma_d - p_d \end{pmatrix} \tag{3.3}$$

Le système $\Sigma(\mathbf{z}) = 0$ définit alors les relations bien connues entre les racines et les coefficients d'une équation algébrique. On dénote par $\mathcal{S}_d$ l'ensemble des permutations de l'ensemble $\{1, \ldots, d\}$.

**Proposition 3.2.1** *Soit $\mathbf{z} \in \mathbb{K}^d$, alors on a $\Sigma(\mathbf{z}) = 0$ si et seulement s'il existe une permutation $\tau \in \mathcal{S}_d$ telle que $\mathbf{z}^\tau = \left(z_{\tau(1)}, \ldots, z_{\tau(d)}\right) = (\zeta_1, \ldots, \zeta_d)$.*

Soit $\mathbf{z} \in \mathbb{K}^d$ tel que $z_i \neq z_j$ si $i \neq j$. On définit alors les polynômes $P_{\mathbf{z}}(x) = \prod_{i=1}^{d}(x - z_i)$ et $F_{\mathbf{z}}(x) = P_{\mathbf{z}}(x) - P(x)$. On note $\mathcal{A} = \mathbb{K}[x]/(P)$ et $\mathcal{A}_{\mathbf{z}} = \mathbb{K}[x]/(P_{\mathbf{z}})$. On a alors $F_{\mathbf{z}} \in \mathbb{K}[x]_{d-1}$ et, en tant que $\mathbb{K}$-espaces vectoriels, $\mathcal{A} \equiv \mathbb{K}[x]_{d-1} \equiv \mathcal{A}_{\mathbf{z}}$.

Une idée déjà évoquée pour approximer simultanément toutes les racines de $P$ consiste à appliquer la méthode de Newton à $\Sigma(\mathbf{z})$. Etant donné la complexité de cette application, on n'applique pas directement la méthode de Newton à $\Sigma(\mathbf{z})$, mais on interprète cette application de façon à ce qu'on obtienne une fonction d'itération (équivalente à calculer les itérés par la méthode de Newton) sans avoir à inverser numériquement la matrice jacobienne de $\Sigma(\mathbf{z})$. On considère à cette fin l'application suivante :

$$\overrightarrow{F} : \begin{cases} \mathbb{K}^d & \longrightarrow & \mathbb{K}[x]_{d-1} \\ \mathbf{z} & \longmapsto & F_{\mathbf{z}}(x) \end{cases}$$

Clairement $\overrightarrow{F}(\mathbf{z}) = 0$ si et seulement si $\Sigma(\mathbf{z}) = 0$. On introduit alors les polynômes de Lagrange associés aux points $z_i$ :

$$\mathbf{e}_{z_i}(x) = \frac{\prod_{j \neq i}(x - z_j)}{\prod_{j \neq i}(z_i - z_j)}$$

qui conduisent à la décomposition $\mathcal{A}_{\mathbf{z}} = \mathbb{K}\mathbf{e}_{z_1} \oplus \cdots \oplus \mathbb{K}\mathbf{e}_{z_d}$. La méthode de Weierstrass consiste alors à appliquer la méthode de Newton à $\overrightarrow{F}$. Nous devons alors calculer :

$$\mathrm{Jac}_{\overrightarrow{F}}(\mathbf{z})^{-1}\,\overrightarrow{F} = \mathbf{u} \tag{3.4}$$

ou de façon équivalente, nous devons résoudre le système linéaire suivant :

$$\mathrm{Jac}_{\overrightarrow{F}}(\mathbf{z})\,\mathbf{u} = \overrightarrow{F}(z) \tag{3.5}$$

Ce système linéaire se traduit par :

$$\sum_{i=1}^{d} \frac{\partial}{\partial z_i} F_{\mathbf{z}}\, u_i = F_{\mathbf{z}}$$

Comme on a $\frac{\partial}{\partial z_i} F_{\mathbf{z}} = \frac{\partial}{\partial z_i}\left(\prod_{j=1}^{d}(x - z_j)\right) = -\left(\prod_{i \neq j}(x - z_j)\right) = -\left(\prod_{j \neq i}(z_i - z_j)\right)\mathbf{e}_{z_i}(x)$ et comme $F_{\mathbf{z}}(x) = \sum_{i=1}^{d} F_{\mathbf{z}}(z_i)\,\mathbf{e}_{z_i}(x) =$

$-\sum_{i=1}^{d} P(z_i)\,\mathbf{e}_{z_i}(x)$ on déduit, par identification dans (3.5) que :

$$u_i = \frac{P(z_i)}{\prod_{j \neq i}(z_i - z_j)} \tag{3.6}$$

A l'aide de cette identité, on a une façon simple d'exprimer la suite $\left(\mathbf{z}^{(k)}\right)_{k\in\mathbb{N}}$ des points itérés de la méthode de Newton appliquée à $\overrightarrow{F}$ :

$$\forall i \in \{1, \ldots, d\}\,,\; z_i^{(k+1)} = I_i\left(\mathbf{z}^{(k)}\right) = z_i^{(k)} - \frac{z_i^{(k)}}{\prod_{j\neq i}\left(z_i^{(k)} - z_j^{(k)}\right)} \tag{3.7}$$

Cela nous permet de décrire les coordonnées de la fonction d'itération de la méthode de Weierstrass :

$$\mathbf{z}^{(k+1)} = I\left(\mathbf{z}^{(k)}\right) = \left(I_1\left(\mathbf{z}^{(k)}\right), \ldots, I_d\left(\mathbf{z}^{(k)}\right)\right) \tag{3.8}$$

Nous suivrons la même trame de raisonnement dans le cadre des systèmes d'équations algébriques. Une telle présentation permet d'obtenir *ipso facto* la convergence quadratique locale de la méthode. C'est la très bonne connaissance des structures des algèbres quotients qui nous permet d'exprimer la fonction d'itération. Les résultats du premier chapitre de cette thèse nous permettront d'adapter ce raisonnement au cadre multivarié.

### 3.2.2 L'approche de Frommer-Bellido

Nous exposons ici brièvement une méthode assez systématique pour construire des fonctions d'itération (voir [8, 9, 10, 46]). C'est une approche qui généralise assez directement la démarche que nous avons suivie pour obtenir la fonction d'itération de Weierstrass. Elle permet d'ailleurs de traiter une classe de problèmes plus large que celle des problèmes polynomiaux. Comme nous le montrerons, elle repose sur des notions d'analyse fonctionnelle et par là-même, sur l'interpolation. Cependant, pour des raisons de clarté de l'exposé, nous ne donnerons pas l'approche la plus générale.

#### Principe de la démarche

La démarche initiée par Frommer puis étoffée par Bellido est la suivante : on considère un ouvert $\Omega \subset \mathbb{K}$. Soit alors $P \in \mathcal{C}^2(\Omega)$ ayant $d$ zéros dans $\Omega$.

On considère un sous-espace vectoriel $V$ de $\mathcal{C}^2(\Omega)$ de dimension $d+1$ et tel que $P \in V$. On considère alors une forme linéaire $\Lambda$ sur $V$ non nulle et telle que $\Lambda(P) \neq 0$. On cherche une fonction $g \in V \setminus \mathrm{Ker}(\Lambda)$ telle que :

$$\begin{cases} g(z, z_i) = 0 \\ \Lambda(g) = \Lambda(P) \end{cases}$$

pour des points $z_1, \ldots, z_d \in \Omega$ choisis. Soit $(b_i)_{i\in\{1,\ldots,d\}}$ une base de $\mathrm{Ker}(\Lambda)$, la fonction $g$ vérifie alors :

$$g(\mathbf{z}, z_i) - P(z_i) = \sum_{i=1}^{d} \phi_i(\mathbf{z})\, b_i(x).$$

On a alors $g(\mathbf{z}, x) = P$ si et seulement si $\phi_i(\mathbf{z}) = 0$, $\forall \in \{1, \ldots, d\}$.

Par exemple, pour la méthode de Weierstrass, on a $P \in \mathbb{K}[x]_d$, $P(x) = \sum_{i=0}^{d} a_i x^i$, avec $a_d \neq 0$. Puis on choisit $\Lambda : \sum_{i=0}^{d} f_i x^i \mapsto f_d$. On a alors clairement $\mathrm{Ker}(\Lambda) = \mathbb{K}[x]_{d-1}$ dont une base est formée des polynômes de Lagrange associés à $\mathbf{z}$ (on peut choisir d'autres bases) et donc

$$g(\mathbf{z}, x) - P(x) = \sum_{i=1}^{d} \left(g(\mathbf{z}, z_i) - P(z_i)\right) \mathbf{e}_i(x).$$

Une fois les $\phi_i$ calculés, on obtient un nouveau système appelé système résolvant, qui est de la forme :

$$(\Phi) : \begin{cases} \phi_i(\mathbf{z}) = 0 \\ \forall i \in \{1, \ldots, d\} \end{cases}$$

auquel on cherche à appliquer la méthode de Newton. Dans le cas de la méthode de Weierstrass, on choisit $g(\mathbf{z}, x) = a_d \left(\prod_{i=1}^{d} (x - z_i)\right)$ et on obtient la formule (3.3) comme système résolvant. Dans le cas général, en appliquant la méthode de Newton au système résolvant, les mêmes simplifications que pour la méthode de Weierstrass apparaissent et on obtient une fonction d'itération dont les coordonnées sont données par :

$$I_i(\mathbf{z}) = z_i - \frac{P(z_i)}{\frac{\partial g}{\partial z_i}(\mathbf{z}, z_i)}, \forall i \in \{1, \ldots, d\}.$$

Plusieurs choix interviennent : le choix de $\Lambda$ et celui de $g$. Par contre le choix de la base de $\mathrm{Ker}(\Lambda)$ n'intervient pas. Nous renvoyons à la thèse de Anne Bellido [9] pour un exposé complet de cette théorie.

## 3.3 Méthodes multivariées

### 3.3.1 Méthode de Weierstrass

On note $\mathcal{I} = (f_1, \ldots, f_n)$ une intersection complète de dimension 0 de $\mathbb{K}[x_1, \ldots, x_n]$ ne définissant que des zéros simples (i.e. de multiplicité 1) $\mathcal{Z}(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_D\} \subset \mathbb{K}^n$.

**Hypothèse 3.3.1** *On suppose que nous connaissons un ensemble* $E = \{\alpha_1, \ldots, \alpha_D\} \subset \mathbb{Z}^n$ *tel que* $\mathbf{x}^E$ *soit une base de* $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$.

**Remarque 3.3.2** *Cette base peut être obtenue avec une bonne probabilité de succès par le calcul d'une base de Gröbner en utilisant une arithmétique modulaire.*

On note $\Delta = \left\{\mathbf{z} \in (\mathbb{K}^n)^D \parallel \exists i \text{ et } j,\, i \neq j \text{ et } \mathbf{z}_i = \mathbf{z}_j\right\}$.

#### Calcul de la fonction d'itération

Nous commençons par décrire la construction d'un système équivalent au système algébrique initial. Nous définissons l'application suivante :

$$\mathcal{F} : \left\{ \begin{array}{ccc} (\mathbb{K}^n)^D \setminus \Delta & \longrightarrow & (\mathbb{K}[x_1, \ldots, x_n]_E)^n \\ \mathbf{z} & \longmapsto & \mathcal{F}(\mathbf{z}, \mathbf{x}) = \begin{pmatrix} F_{f_1}(\mathbf{z}, \mathbf{x}) \\ \vdots \\ F_{f_n}(\mathbf{z}, \mathbf{x}) \end{pmatrix} \end{array} \right.$$

où $F_{f_i}(\mathbf{z}, \mathbf{x}) = \frac{R_{f_i}(\mathbf{z}, \mathbf{x})}{\mathbf{v}_{E,\mathbf{z}}} - f_i(z, \mathbf{x})$. On associe au système $\mathcal{F}(\mathbf{z}, \mathbf{x}) = 0 \in (\mathbb{K}[x_1, \ldots, x_n]_E)^n$ un nouveau système que nous décrivons dans ce qui suit. Si on regarde les polynômes $F_{f_i}(\mathbf{z}, \mathbf{x}) = \frac{R_{f_i}(\mathbf{z}, \mathbf{x})}{\mathbf{v}_{\mathcal{Z}(\mathcal{I}),E}} - f_i$, on remarque qu'ils admettent tous $\mathbf{x}^E$ comme support monomial. On a donc $F_{f_i}(\mathbf{z}, \mathbf{x}) = \sum_{\alpha \in E} \psi_{i,\alpha}(\mathbf{z})\, \mathbf{x}^\alpha$, $\forall i \in \{1, \ldots, n\}$ On obtient alors le système carré suivant :

$$(\Psi) : \left\{ \begin{array}{c} \psi_{i,\alpha}(\mathbf{z}) = 0 \\ \forall i \in \{1, \ldots, n\} \text{ et } \forall \alpha \in E \end{array} \right. \tag{3.9}$$

Par construction on a $\psi_{i,\alpha}(\mathcal{Z}) = 0$, $\forall i \in \{1, \ldots, d\}$ et $\forall \alpha \in E$. Le système (3.9) est l'analogue du système (3.3) dans le cas multivarié. L'idée est encore d'appliquer la méthode de Newton au système (3.9). Comme dans le cas univarié, nous allons exploiter la structure du problème pour inverser explicitement le jacobien de ce système et donner une fonction d'itération simple.

On introduit les application suivantes :

- $\Phi : \begin{cases} \mathbb{K}[x_1, \ldots, x_n]_E & \longrightarrow & \mathbb{K}^E \\ P = \sum_{\alpha \in E} p_\alpha \mathbf{x}^\alpha & \longmapsto & (p_\alpha)_{\alpha \in E} \end{cases}$
- $\overrightarrow{\mathcal{F}} : \begin{cases} (\mathbb{K}^n)^D & \longrightarrow & \left(\mathbb{K}^E\right)^n \\ \mathbf{z} & \longrightarrow & \overrightarrow{\mathcal{F}}(\mathbf{z}) = \left(\Phi\left(F_{f_1}(\mathbf{z}, \mathbf{x})\right), \ldots, \Phi\left(\mathcal{F}_{f_n}(\mathbf{z}, \mathbf{x})\right)\right) \end{cases}$

On a $\overrightarrow{\mathcal{F}}(\mathbf{z}) = 0$ si et seulement si $\{\mathbf{z}_1, \ldots, \mathbf{z}_D\} = \{\zeta_1, \ldots, \zeta_D\}$. L'idée est alors d'appliquer la méthode de Newton à $\overrightarrow{\mathcal{F}}$ et à cette fin on a à calculer la suite des points itérés de Newton :

$$\mathbf{z}^{(k+1)} = \mathbf{z}^{(k)} - \mathrm{Jac}_{\overrightarrow{\mathcal{F}}}\left(\mathbf{z}^{(k)}\right)^{-1} \overrightarrow{\mathcal{F}}\left(\mathbf{z}^{(k)}\right) \tag{3.10}$$

**Théorème 3.3.3** *Sous les conditions décrites précédemment, pour appliquer la méthode de Newton à $\overrightarrow{\mathcal{F}}$, pour $i \in \{1, \ldots, D\}$, on doit calculer*

$$\mathbf{z}_i^{(k+1)} = \mathbf{z}_i^{(k)} - \begin{pmatrix} \frac{\frac{\partial R_{f_1}}{\partial x_1}\left(\mathbf{z}^{(k)}, \mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)}, E}} & \cdots & \frac{\frac{\partial R_{f_1}}{\partial x_n}\left(\mathbf{z}^{(k)}, \mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)}, E}} \\ \vdots & \ddots & \vdots \\ \frac{\frac{\partial R_{f_n}}{\partial x_1}\left(\mathbf{z}^{(k)}, \mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)}, E}} & \cdots & \frac{\frac{\partial R_{f_n}}{\partial x_n}\left(\mathbf{z}^{(k)}, \mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)}, E}} \end{pmatrix}^{-1} \begin{pmatrix} f_1\left(\mathbf{z}_i^{(k)}\right) \\ \vdots \\ f_n\left(\mathbf{z}_i^{(k)}\right) \end{pmatrix} \tag{3.11}$$

*Et la suite $\left(z^{(k)}\right)_{k \in \mathbb{N}}$ converge quadratiquement dans un voisinage des solutions du système.*

**Remarque 3.3.4** *Par linéarité de $\Phi$, on a $\frac{\partial}{\partial z_{i,j}} \Phi\left(F_{f_k}(\mathbf{z})\right) = \Phi\left(\frac{\partial}{\partial z_{i,j}} F_{f_k}(\mathbf{z})\right)$ pour tout $k \in \{1, \ldots, n\}$ et $i \in \{1, \ldots, D\}$.*

*Preuve* : [du théorème]. Soit à résoudre $J_{\overrightarrow{\mathcal{F}}}(\mathbf{z})\,\mathbf{u} = \overrightarrow{\mathcal{F}}(\mathbf{z})$. Par le corollaire 2.4.22, pour tout $k \in \{1, \ldots, n\}$, on a :

$$\Phi\left(\sum_{i=1}^{D} \sum_{j=1}^{n} -\frac{\frac{\partial R_{f_k}(\mathbf{z}, \mathbf{z}_i)}{\partial x_j}}{\mathbf{v}_{\mathbf{z}, E}} u_{i,j} \mathbf{e}_i(\mathbf{z}, \mathbf{x})\right) = \Phi\left(F_{f_k}(\mathbf{z}, \mathbf{z}_i)\, \mathbf{e}_i(\mathbf{z}, \mathbf{x})\right).$$

ou de façon équivalente :

$$\sum_{i=1}^{D} \sum_{j=1}^{n} -\frac{\frac{\partial R_{f_k}(\mathbf{z}, \mathbf{z}_i)}{\partial x_j}}{\mathbf{v}_{\mathbf{z}, E}} u_{i,j} \mathbf{w}_i = \sum_{i=1}^{D} F_{f_k}(\mathbf{z}, \mathbf{z}_i)\, \mathbf{w}_i,$$

en notant $\mathbf{w}_i = \Phi(\mathbf{e}_i(\mathbf{z}, \mathbf{z}_i))$. Ainsi pour $i \in \{1, \ldots, D\}$, on a le système suivant :

$$\left\{ \begin{array}{l} \displaystyle\sum_{j=1}^{n} -\frac{\frac{\partial R_{f_k}(\mathbf{z},\mathbf{z}_i)}{\partial x_j}}{\mathbf{v}_{\mathbf{z},E}} u_{i,j} = F_{f_k}(\mathbf{z}, \mathbf{z}_i) \\ \qquad \forall k \in \{1, \ldots, n\} \end{array} \right. \tag{3.12}$$

Alors pour tout $i \in \{1, \ldots, D\}$ on définit :

$$\Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z}) = \begin{pmatrix} \frac{\frac{\partial R_{f_1}(\mathbf{z},\mathbf{z}_i)}{\partial x_1}}{\mathbf{v}_{\mathbf{z},E}} & \ldots & \frac{\frac{\partial R_{f_1}(\mathbf{z},\mathbf{z}_i)}{\partial x_n}}{\mathbf{v}_{\mathbf{z},E}} \\ \vdots & \ddots & \vdots \\ \frac{\frac{\partial R_{f_n}(\mathbf{z},\mathbf{z}_i)}{\partial x_1}}{\mathbf{v}_{\mathbf{z},E}} & \ldots & \frac{\frac{\partial R_{f_n}(\mathbf{z},\mathbf{z}_i)}{\partial x_n}}{\mathbf{v}_{\mathbf{z},E}} \end{pmatrix}.$$

A partir de cette définition, comme $F_{f_k}(\mathbf{z}, \mathbf{z}_k) = -f_k(\mathbf{z}_i)$, le système (3.12) se réécrit sous la forme suivante :

$$\begin{pmatrix} u_{i,1} \\ \vdots \\ u_{i,n} \end{pmatrix} = \Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z})^{-1} \begin{pmatrix} f_1(\mathbf{z}_i) \\ \vdots \\ f_n(\mathbf{z}_i) \end{pmatrix}.$$

La formule du théorème est donc prouvée. La convergence de la méthode découle du fait que cette méthode équivaut à appliquer la méthode de Newton et que toutes les racines sont supposées simples. ♣

**Remarque 3.3.5** *Si le système a une seule racine, alors la formule (3.11) donne l'itération de Newton classique et s'il n'y a qu'une seule variable, la formule donne l'itération de Weierstrass classique.*

### Algorithme et complexité arithmétique

Nous rappelons que nous supposons connue une base du $\mathbb{K}$-espace vectoriel $\mathcal{A}$. Nous utilisons les même notations que précédemment.

Les points initiaux sont donnés sous la forme d'une matrice $\mathbf{z}$ dont les colonnes sont les coordonnées des points de départs.

### Algorithme 3.3.6 (Itération de Weierstrass)

- Entrée : *La matrice $\mathbf{z}$ formée des coordonnées des points initiaux, les polynômes $f_1, \ldots, f_n$ et $E$.*

- *Etape 1. Calculer les matrices suivantes (spécialisées en* $\mathbf{z}$*)*

$$MV_E(\mathbf{z}) = \begin{pmatrix} \mathbf{z}_1^{\alpha_1} & \cdots & \mathbf{z}_1^{\alpha_D} \\ \vdots & \ddots & \vdots \\ \mathbf{z}_D^{\alpha_1} & \cdots & \mathbf{z}_D^{\alpha_D} \end{pmatrix}$$

$$MR_{f_k}(\mathbf{z}) = \begin{pmatrix} f_k(\mathbf{z}_1) & \mathbf{z}_1^{\alpha_1} & \cdots & \mathbf{z}_1^{\alpha_D} \\ \vdots & \vdots & \ddots & \vdots \\ f_k(\mathbf{z}_D) & \mathbf{z}_D^{\alpha_1} & \cdots & \mathbf{z}_D^{\alpha_D} \end{pmatrix}$$

*pour* $i \in \{1, \ldots, D\}$*. Puis nous calculons les colonnes :*

$$dv_{f_k}^{(i)}(\mathbf{x}) = \left(\frac{\partial}{\partial x_i} f_k(\mathbf{x}), \frac{\partial}{\partial x_i}\mathbf{x}^{\alpha_1}, \cdots, \frac{\partial}{\partial x_i}\mathbf{x}^{\alpha_D}\right)$$

*pour* $i \in \{1, \ldots, n\}$ *et* $k \in \{1, \ldots, n\}$*.*
- *Etape 2. Décomposer LU de* $MV_E(\mathbf{z})$*. On utilise cette décomposition pour calculer les noyaux des matrices* $MR_{f_k}(\mathbf{z})$*. Ce qui donne des vecteurs* $r_{f_k} \in \mathbb{K}^{D+1}$*, pour chaque* $k \in \{1, \ldots, n\}$*. Si la dimension du noyau de* $MV_E(\mathbf{z})$ *n'est pas nulle, l'algorithme renvoie un message d'erreur.*
- *Etape 3. Pour chaque* $i \in \{1, \ldots, D\}$*, on construit les matrices* $\Delta_{\mathbf{z}_i}\overrightarrow{\mathcal{F}}(\mathbf{z})$ *en calculant leurs coefficients comme suit : on spécialise* $dv_{f_k}^{(i)}$ *en* $\mathbf{z}_i$*, puis on calcule leurs produits scalaires avec* $r_{f_k}(\mathbf{z})$ *que l'on a normalisé par le dernier coefficient du résultat (i.e. le déterminant de Vandermonde), pour* $k \in \{1, \ldots, n\}$*. On obtient ainsi* $\Delta_{\mathbf{z}_i}\overrightarrow{\mathcal{F}}(\mathbf{z})$ *par concaténation.*
- *Etape 4. Pour chaque* $i \in \{1, \ldots, D\}$*, on résout le système*

$$(f_1(\mathbf{z}_i), \ldots, f_n(\mathbf{z}_i))^t = \Delta_{\mathbf{z}_i}\overrightarrow{\mathcal{F}}(\mathbf{z})\,\mathbf{z}_i',$$

*où* $\mathbf{z}_i'$ *est la colonne d'indice i de la matrice du résultat.*
- *Sortie :* *La matrice* $\mathbf{z}'$*.*

**Proposition 3.3.7** *La complexité arithmétique d'une itération de l'algorithme 3.3.6 est en* $\mathcal{O}\left(D^3 + n^2D^2 + Dn^3\right)$ *opérations arithmétiques.*

*Preuve* : On détaille le coût des différentes étapes :
- A l'étape 1, on commence par spécialiser n matrices de taille $D \times (D+1)$, ce qui nécessite $\mathcal{O}\left(nD^2\right)$ opérations arithmétiques.

- A l'étape 2 et 3, on calcule une décomposition LU de la matrice $MV_E(\mathbf{z})$. Cela se fait avec $\mathcal{O}\left(D^3\right)$ opérations arithmétiques. Puis on utilise cette décomposition pour calculer les noyaux des $n$ matrices $MR_{f_k}(_z)$, ce qui coûte $\mathcal{O}\left(nD^2\right)$ opérations arithmétiques. On spécialise $nD$ vecteurs de longueur $D+1$, ce qui a une complexité en $\mathcal{O}\left(nD^2\right)$. Ensuite on calcule $n^2D$ produits de vecteurs de longueur $D+1$, on obtient une complexité en $\mathcal{O}\left(n^2D^2\right)$ pour ces calculs.
- Dans l'étape 4, on spécialise $D$ vecteurs de longueurs $n$. Ce qui donne une complexité en $\mathcal{O}(nD)$. Puis on résout $D$ systèmes linéaires de taille $n\times n$, ce qui coûte $\mathcal{O}\left(Dn^3\right)$ opérations arithmétiques. Finalement on calcule n produits de matrices de taille $n \times n$ par des vecteurs ce qui donne une complexité en $\mathcal{O}\left(n^2\right)$. On note $L$ le coût maximal de l'évaluation des polynômes $f_k$. On réalise $D$ évaluations de chacun des $n$ polynômes, ce donne la complexité $\mathcal{O}(nDL)$.

Avec tous ces éléments on obtient une complexité en $\mathcal{O}\left(D^3+n^2D^2+Dn^3+nDL\right)$ opérations arithmétiques. ♣

**Remarque 3.3.8** *Dans l'étape 2, on ne fait pas usage de la structure de la matrice de Vandermonde. L'utilisation de cette structure peut améliorer la complexité. On renvoie à [78] pour l'utilisation des structures des matrices dans la résolution de systèmes.*

### 3.3.2 Méthode de Aberth

Dans cette sous-section, nous proposons une fonction d'itération qui étend la fonction d'itération d'Aberth. Ce travail a été effectué en commun avec Anne Bellido. Nous commençons par rappeler une méthode pour calculer la fonction d'itération d'Aberth dans le cas d'une variable. Puis nous montrons que cette méthode peut être utilisée dans le cas multivarié. L'intérêt de cette méthode dans le cas univarié est que la convergence est localement cubique et non quadratique comme l'est la méthode de Weierstrass. De très bons logiciels de résolution numérique d'équations algébriques univariées sont basés sur cette itération comme MPsolve [13, 14]. Cela a motivé la construction d'une fonction d'itération dans le cas multivarié. Malheureusement, nous ne sommes pas, pour l'instant, en mesure de démontrer que la méthode converge de façon cubique localement.

**Fonction d'itération en une variable**

On considère un polynôme monique $P(x) = x^d + \sum_{i=1}^{d} a_i x^{d-i} = \prod_{i=1}^{d}(x-\zeta_i)$. On suppose que $P$ n'a que des racines simples, i.e. $\zeta_i \neq \zeta_j$ pour $i \neq j \in \{1,\ldots,d\}$. Soit $\mathbf{z} = (z_1,\ldots,z_d) \in \mathbb{K}^d$ tel que $z_i \neq z_j$ pour $i \neq j \in \{1,\ldots,d\}$. On remarque alors que :

$$\frac{d}{dx} g_i(\mathbf{z},x) = \frac{1}{\mathbf{e}_i(\mathbf{z},x)}(P'(x) - P(x)\frac{\mathbf{e}_i'(\mathbf{z},x)}{\mathbf{e}_i(\mathbf{z},x)}). \tag{3.13}$$

De plus, $e_i'(\mathbf{z},x) = \dfrac{\displaystyle\sum_{j\neq i} \prod_{k\neq i,\, k\neq j} (x-z_k)}{\displaystyle\prod_{j\neq i}(z_i - z_j)}$. On en déduit que :

$$\frac{\mathbf{e}_i'(\mathbf{z},x)}{\mathbf{e}_i(\mathbf{z},x)} = \frac{\dfrac{\displaystyle\sum_{j\neq i} \prod_{k\neq i,\, k\neq j} (x-z_k)}{\displaystyle\prod_{j\neq i}(z_i - z_j)}}{\dfrac{\displaystyle\prod_{j\neq i}(x - z_j)}{\displaystyle\prod_{j\neq i}(z_i - z_j)}} = \sum_{j\neq i} \frac{1}{(x - z_j)}.$$

Cette dernière égalité, avec l'égalité 3.13, implique que :

$$\frac{d}{dx} g_i(\mathbf{z},z_i) = P'(z_i) - P(z_i)\sum_{j\neq i}\frac{1}{(z_i - z_j)} \tag{3.14}$$

On considère alors l'application $G(\mathbf{z}) = (g_1(\mathbf{z},x),\ldots,g_d(\mathbf{z},x))$. Il n'est pas difficile de constater que $G(\mathbf{z}) = 0$ si et seulement si $\mathbf{z} = (\zeta_1,\ldots,\zeta_d)$. L'idée est alors de chercher les zéros de $\mathbf{z}$ en appliquant l'opérateur de correction défini comme suit. On cherche $\mathbf{u} = (u_1,\ldots,u_d) \in \mathbb{K}^d$ tel que :

$$\forall i \in \{1,\ldots,d\}\,,\ \frac{d}{dx} g_i(\mathbf{z},z_i)u_i = g_i(\mathbf{z},\mathbf{z}_i).$$

C'est-à-dire que $u_i = \frac{g_i(\mathbf{z},z_i)}{\frac{d}{dx}g_i(\mathbf{z},z_i)}$. La fonction d'itération d'Aberth est alors donnée par $I^A(\mathbf{z}) = (I_1^A(\mathbf{z}),\ldots,I_d^A(\mathbf{z}))$ où $I_i^A(\mathbf{z}) = z_i - \frac{g_i(\mathbf{z},z_i)}{\frac{d}{dx}g_i(\mathbf{z},z_i)}$ et elle est définie de $\mathbb{K}^d \setminus \Delta$ dans $\mathbb{K}^d$, où $\Delta = \{\mathbf{z} \in \mathbb{K}^d \mid \exists i \text{ et } j,\, i \neq j \text{ et } z_i = z_j\}$. En utilisant l'égalité 3.14, on obtient :

$$I_i^A(\mathbf{z}) = z_i - \frac{P(z_i)}{P'(z_i) - P(z_i)\displaystyle\sum_{j\neq i} \frac{1}{(z_i - z_j)}} \tag{3.15}$$

qui est bien la formule classique de l'itération de Aberth.

### Méthode d'Aberth multivariée

On considère $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ des polynômes définissant une variété de dimension zéro $\{\zeta_1, \ldots, \zeta_d\} \subset \mathbb{K}^n$ où toutes les racines $\zeta_i = (\zeta_{i,1}, \ldots, \zeta_{i,n})$ sont simples. Soit $\mathbf{z} = (\mathbf{z}_1, \ldots, \mathbf{z}_d) \in (\mathbb{K}^n)^d$, i.e.
$\mathbf{z}_i = (\mathbf{z}_{i,1}, \ldots, \mathbf{z}_{i,n}) \in \mathbb{K}^n$. On suppose connu $E = \{\alpha_1, \ldots, \alpha_d\} \subset \mathbb{N}^n$ tel que $\mathbf{x}^E$ soit une base monomiale de $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$. On fera le même raisonnement que pour le cas d'une seule variable. On définit $g_i(\mathbf{z}, \mathbf{x}) = (\frac{f_i(x)}{\mathbf{e}_1(\mathbf{z},\mathbf{x})}, \ldots, \frac{f_i(\mathbf{x})}{\mathbf{e}_d(\mathbf{z},\mathbf{x})})$, $\forall i \in \{1, \ldots, d\}$, où $\mathbf{e}_i(\mathbf{z}, \mathbf{x})$ est l'idempotent associé à $\mathbf{z}_i$. On commence par remarquer que :

$$\frac{\partial}{\partial x_k} g_{i,j}(\mathbf{z}, \mathbf{x}) = \frac{\partial}{\partial x_k} \frac{f_i(\mathbf{x})}{\mathbf{e}_j(\mathbf{z}, \mathbf{x})} = \frac{1}{\mathbf{e}_j(\mathbf{z}, \mathbf{x})} \left( \frac{\partial}{\partial x_k} f_i(\mathbf{x}) - f_i(\mathbf{x}) \frac{\frac{d}{dx_k}\mathbf{e}_j(\mathbf{z}, \mathbf{x})}{\mathbf{e}_j(\mathbf{z}, \mathbf{x})} \right)$$

$\forall i, k \in \{1, \ldots, n\}$ et $j \in \{i, \ldots, d\}$. On constate que :

$$\frac{\partial}{\partial z_k} g_{i,j}(\mathbf{z}, \mathbf{z}_j) = \frac{\partial}{\partial x_k} f_i(\mathbf{z}_j) - f_i(\mathbf{z}_j) \frac{\partial}{\partial x_k} \mathbf{e}_j(\mathbf{z}, \mathbf{z}_j).$$

Comme dans le cas d'une seule variable, on cherche $u_{j,1}^i, \ldots, u_{j,n}^i$ tel que :

$$\sum_{k=1}^{n} \frac{\partial}{\partial x_k} g_{i,j}(\mathbf{z}, \mathbf{z}_j) u_{j,k}^i = g_{i,j}(\mathbf{z}, \mathbf{z}_j).$$

Cela nous amène à considérer l'opérateur suivant :

$$A^{(j)}(\mathbf{z}) = \begin{pmatrix} \frac{\partial}{\partial x_1} f_1(\mathbf{z}_j) - f_1(\mathbf{z}_j) \frac{\partial \mathbf{e}_j}{\partial x_1}(\mathbf{z}, \mathbf{z}_j) & \cdots & \frac{\partial}{\partial x_n} f_1(\mathbf{z}_j) - f_1(\mathbf{z}_j) \frac{\partial \mathbf{e}_j}{\partial x_n}(\mathbf{z}, \mathbf{z}_j) \\ \vdots & \ddots & \vdots \\ \frac{\partial}{\partial x_1} f_n(\mathbf{z}_j) - f_n(\mathbf{z}_j) \frac{\partial \mathbf{e}_j}{\partial x_n}(\mathbf{z}, \mathbf{z}_j) & \cdots & \frac{\partial}{\partial x_n} f_n(\mathbf{z}_j) - f_n(\mathbf{z}_j) \frac{\partial \mathbf{e}_j}{\partial x_n}(\mathbf{z}, \mathbf{z}_j) \end{pmatrix} \tag{3.16}$$

La méthode d'Aberth généralisée consiste alors à appliquer la fonction d'itération suivante :

$$I^A(\mathbf{z}) = (I_1^A(\mathbf{z}), \ldots, I_d^A(\mathbf{z}))$$

avec :

$$I_i^A(\mathbf{z}) = \mathbf{z}_i - A^{(i)}(\mathbf{z})^{-1} \begin{pmatrix} f_1(\mathbf{z}_i) \\ \vdots \\ f_n(\mathbf{z}_i) \end{pmatrix}, \forall i \in \{1, \ldots, d\}.$$

Pour $\mathbf{z} \in (\mathbb{K}^n)^d \backslash \Delta$ où $\Delta = \left\{\mathbf{z} \in (\mathbb{K}^n)^d \,|\, \exists i \text{ et } j \in \{1, \ldots, d\}, i \neq j \text{ et } \mathbf{z}_i = \mathbf{z}_j\right\}$.

## 3.4 Fonction d'itération de Gauss-Weierstrass

Dans cette section nous nous intéressons à la possibilité de définir une fonction d'itération du type de celle de Weierstrass dans le cas des systèmes surcontraints. La méthode proposée ici est d'une grande importance pour concevoir des méthodes modifiées comme celles proposée dans la section suivante.

On note $\mathcal{I} = (f_1, \ldots, f_n) \subset \mathbb{K}[x_1, \ldots, x_n]$ avec $m > n$ un système algébrique définissant un idéal de dimension zéro. On suppose de plus que $Z(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_d\}$ est formé de racines simples. On reprend l'hypothèse 3.3.1.

### 3.4.1 Calcul de la fonction d'itération

Nous commençons par décrire la construction d'un système équivalent au système algébrique initial. On note $\Delta = \left\{\mathbf{z} \in (\mathbb{K}^n)^d \,|\, \exists i \text{ et } j \in \{1, \ldots, d\}, i \neq j \text{ et } \mathbf{z}_i = \mathbf{z}_j\right\}$. On considère alors l'application suivante :

$$\mathcal{F} : \left\{ \begin{array}{ccc} (\mathbb{K}^n)^d \setminus \Delta & \longrightarrow & (\mathbb{K}[x_1, \ldots, x_n]_E)^m \\ \mathbf{z} & \longmapsto & \mathcal{F}(\mathbf{z}, \mathbf{x}) = \begin{pmatrix} F_{f_1}(\mathbf{z}, \mathbf{x}) \\ \vdots \\ F_{f_m}(\mathbf{z}, \mathbf{x}) \end{pmatrix} \end{array} \right.$$

On associe au nouveau système $\mathcal{F}(\mathbf{z}, \mathbf{x}) = 0$ dans $(\mathbb{K}[x_1, \ldots, x_n]_E)^m$ un nouveau système que nous décrivons comme suit. Comme tous les polynômes $F_{f_i}(\mathbf{z}, \mathbf{x})$ sont à support inclus dans $\mathbb{K}[x_1, \ldots, x_n]_E$, on a $F_{f_i}(\mathbf{z}, \mathbf{x}) = \sum_{\alpha \in E} \psi_{i,\alpha}(\mathbf{z}) \mathbf{x}^\alpha$, $\forall i \in \{1, \ldots, m\}$. On obtient alors le système suivant :

$$(\Psi) : \left\{ \begin{array}{c} \psi_{i,\alpha}(z) = 0 \\ \forall \alpha \in E, \forall i \in \{1, \ldots, m\} \end{array} \right.$$

Par construction de ce système rectangulaire (il est surcontraint), on a $\psi_{\alpha,i}(Z(\mathcal{I})) = 0$, $\forall \alpha \in E$ et $i \in \{1,\ldots,m\}$. De plus toute solution de ce système s'obtient par permutation de $(\zeta_1,\ldots,\zeta_d)$. L'idée est alors d'appliquer la méthode de Newton surcontrainte à ce système. Comme nous le verrons, nous ne pouvons pas donner de formule close pour cette fonction d'itération. Mais nous pouvons néanmoins exploiter en partie le travail que nous avons déjà effectué.

Comme précédemment on considère les applications suivantes :

- $\Phi : \left\{ \begin{array}{lcl} \mathbb{K}[x_1,\ldots,x_n]_E & \longrightarrow & \mathbb{K}^E \\ P = \sum\limits_{\alpha\in E} p_\alpha \mathbf{x}^\alpha & \longmapsto & (p_\alpha)_\alpha \end{array} \right.$.
- $\overrightarrow{\mathcal{F}} : \left\{ \begin{array}{lcl} (\mathbb{K}^n)^d \setminus \Delta & \longrightarrow & \left(\mathbb{K}^E\right)^m \\ \mathbf{z} & \longmapsto & \overrightarrow{\mathcal{F}}(\mathbf{z}) = \left(\Phi\left(F_{f_1}(\mathbf{z},\mathbf{x})\right),\ldots,\Phi\left(F_{f_m}(\mathbf{z},\mathbf{x})\right)\right) \end{array} \right.$.

On peut voir assez facilement que $\overrightarrow{\mathcal{F}}(\mathbf{z}) = 0$ si et seulement si $(\mathbf{z}_1,\ldots,\mathbf{z}_d) = (\zeta_1,\ldots,\zeta_d)$ à permutation près. Comme pour le cas de l'intersection complète, c'est à $\overrightarrow{\mathcal{F}}$ qu'on va appliquer la méthode de Newton, ce qui revient à calculer les itérés de Newton :

$$\mathbf{z}^{(k+1)} = \mathbf{z}^{(k)} - \mathrm{Jac}_{\overrightarrow{\mathcal{F}}}\left(\mathbf{z}^{(k)}\right)^\dagger \overrightarrow{\mathcal{F}}\left(\mathbf{z}^{(k)}\right)$$

où $\mathrm{Jac}_{\overrightarrow{\mathcal{F}}}(\mathbf{z})^\dagger$ représente l'inverse de Moore-Penrose de $\mathrm{Jac}_{\overrightarrow{\mathcal{F}}}(\mathbf{z})$. Il s'agit donc de remplacer l'itération de Newton par celle de Gauss-Newton (pour plus de détail, le lecteur pourra se rapporter à [2]).

**Théorème 3.4.1** *Sous les conditions décrites précédemment, pour appliquer la méthode de Newton surcontrainte à $\overrightarrow{\mathcal{F}}$, pour chaque $i \in \{1,\ldots,d\}$ on doit calculer*

$$\mathbf{z}_i^{(k+1)} = \mathbf{z}_i^{(k)} - \begin{pmatrix} \dfrac{\frac{\partial R_{f_1}}{\partial x_1}\left(\mathbf{z}^{(k)},\mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)},E}} & \cdots & \dfrac{\frac{\partial R_{f_1}}{\partial x_n}\left(\mathbf{z}^{(k)},\mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)},E}} \\ \vdots & \ddots & \vdots \\ \dfrac{\frac{\partial R_{f_m}}{\partial x_1}\left(\mathbf{z}^{(k)},\mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)},E}} & \cdots & \dfrac{\frac{\partial R_{f_m}}{\partial x_n}\left(\mathbf{z}^{(k)},\mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)},E}} \end{pmatrix}^\dagger \begin{pmatrix} f_1\left(\mathbf{z}_i^{(k)}\right) \\ \vdots \\ f_m\left(\mathbf{z}_i^{(k)}\right) \end{pmatrix}$$

*Preuve* : A chaque itération, on a donc à résoudre un système de la forme $J_{\overrightarrow{\mathcal{F}}}(\mathbf{z})\,\mathbf{u} = \overrightarrow{\mathcal{F}}(\mathbf{z})$. Pour les mêmes raisons que pour le cas de l'intersection complète, pour tout $k \in \{1,\ldots,m\}$, on a :

$$\Phi\left(\sum_{i=1}^{d}\sum_{j=1}^{n} \frac{\frac{\partial R_{f_k}}{\partial x_j}(\mathbf{z},\mathbf{z}_i)}{\mathbf{v}_{\mathbf{z},E}} u_{i,j}\mathbf{e}_i(\mathbf{z},\mathbf{x})\right) = \Phi\left(\sum_{i=1}^{d} F_{f_k}(\mathbf{z},\mathbf{z}_i)\,\mathbf{e}_i(\mathbf{z},\mathbf{x})\right)$$

Et comme $F_{f_k}(\mathbf{z}, \mathbf{z}_i) = f_k(\mathbf{z}_i)$, pour tout $k \in \{1, \ldots, m\}$, cela équivaut à :

$$\sum_{i=1}^{d} \sum_{j=1}^{n} \frac{\frac{\partial R_{f_k}}{\partial x_j}(\mathbf{z}, \mathbf{z}_i)}{\mathbf{v}_{\mathbf{z},E}} u_{i,j} \mathbf{w}_i = \sum_{i=1}^{d} f_k(\mathbf{z}_i)\, \mathbf{w}_i$$

En notant $\mathbf{w}_i = \Phi(\mathbf{e}_i(\mathbf{z}, \mathbf{x}))$. Ainsi, $\forall i \in \{1, \ldots, d\}$, on a à résoudre le système suivant :

$$\left\{ \begin{array}{c} \displaystyle\sum_{j=1}^{n} \frac{\frac{\partial R_{f_k}}{\partial x_j}(\mathbf{z}, \mathbf{z}_i)}{\mathbf{v}_{\mathbf{z},E}} u_{i,j} = f_k(\mathbf{z}_i) \\ \forall k \in \{1, \ldots, m\} \end{array} \right.$$

On note alors :

$$\Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z}) = \begin{pmatrix} \frac{\frac{\partial R_{f_1}}{\partial x_1}\left(\mathbf{z}^{(k)}, \mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)},E}} & \cdots & \frac{\frac{\partial R_{f_1}}{\partial x_n}\left(\mathbf{z}^{(k)}, \mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)},E}} \\ \vdots & \ddots & \vdots \\ \frac{\frac{\partial R_{f_m}}{\partial x_1}\left(\mathbf{z}^{(k)}, \mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)},E}} & \cdots & \frac{\frac{\partial R_{f_m}}{\partial x_n}\left(\mathbf{z}^{(k)}, \mathbf{z}_i^{(k)}\right)}{\mathbf{v}_{\mathbf{z}^{(k)},E}} \end{pmatrix}$$

Pour tout $i \in \{1, \ldots, d\}$, on a alors à résoudre :

$$\Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z}) \begin{pmatrix} u_{i,1} \\ \vdots \\ u_{i,n} \end{pmatrix} = \begin{pmatrix} f_1(\mathbf{z}_i) \\ \vdots \\ f_m(\mathbf{z}_i) \end{pmatrix}$$

D'où, en utilisant l'inverse de Moore-Penrose :

$$\begin{pmatrix} u_{i,1} \\ \vdots \\ u_{i,n} \end{pmatrix} = \Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z})^{\dagger} \begin{pmatrix} f_1(\mathbf{z}_i) \\ \vdots \\ f_m(\mathbf{z}_i) \end{pmatrix}$$

Ce qui achève la preuve du théorème. ♣

**Remarque 3.4.2** *Même si on ne donne pas une formule close pour la fonction d'itération, puisque l'inverse de Moore-Penrose n'est pas donné par une formule, la fonction d'itération est très simple. Au lieu de résoudre aux moindres carrés un système $nD \times mD$, on a à résoudre $D$ systèmes $n \times m$ à chaque itération. La stabilité numérique de l'algorithme ne peut que profiter de cette division du travail numérique à effectuer. On obtient ainsi une fonction d'itération que nous appellerons itération de Gauss-Weierstrass.*

### Algorithme dans le cas surcontraint

Nous rappelons qu'ici nous supposons de nouveau connue une base monomiale de $\mathcal{A}$. Nous utilisons les mêmes notations que précédemment. On rappelle qu'appliquer l'inverse de Moore-Penrose est équivalent à résoudre le système équivalent aux moindre carrés.

### Algorithme 3.4.3 (Itération de Gauss-Weierstrass)

- *Entrée :* *La matrice* $\mathbf{z}$ *formée des coordonnées des points initiaux, les polynômes* $f_1, \ldots, f_m$ *et* $E$.
- *Etape 1. Calculer les matrices suivantes (spécialisées en* $\mathbf{z}$*)*

$$MV_E(\mathbf{z}) = \begin{pmatrix} \mathbf{z}_1^{\alpha_1} & \cdots & \mathbf{z}_1^{\alpha_D} \\ \vdots & \ddots & \vdots \\ \mathbf{z}_D^{\alpha_1} & \cdots & \mathbf{z}_D^{\alpha_D} \end{pmatrix}$$

$$MR_{f_k}(\mathbf{z}) = \begin{pmatrix} f_k(\mathbf{z}_1) & \mathbf{z}_1^{\alpha_1} & \cdots & \mathbf{z}_1^{\alpha_D} \\ \vdots & \vdots & \ddots & \vdots \\ f_k(\mathbf{z}_D) & \mathbf{z}_D^{\alpha_1} & \cdots & \mathbf{z}_D^{\alpha_D} \end{pmatrix}$$

  *pour* $i \in \{1, \ldots, D\}$. *Puis nous calculons les colonnes :*

$$dv_{f_k}^{(i)}(\mathbf{x}) = \left( \frac{\partial}{\partial x_i} f_k(\mathbf{x}), \frac{\partial}{\partial x_i} \mathbf{x}^{\alpha_1}, \cdots, \frac{\partial}{\partial x_i} \mathbf{x}^{\alpha_D} \right)$$

  *pour* $i \in \{1, \ldots, n\}$ *et* $k \in \{1, \ldots, m\}$.
- *Etape 2. On fait une décomposition LU de* $MV_E(\mathbf{z})$. *On utilise cette décomposition pour calculer les noyaux des matrices* $MR_{f_k}(\mathbf{z})$. *Ce qui donne des vecteurs* $r_{f_k} \in \mathbb{K}^{D+1}$, *pour chaque* $k \in \{1, \ldots, n\}$. *Si la dimension du noyau de* $MV_E(\mathbf{z})$ *n'est pas nulle, l'algorithme renvoie un message d'erreur.*
- *Etape 3. Pour chaque* $i \in \{1, \ldots, D\}$, *construire les matrices* $\Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z})$ *en calculant leurs coefficients comme suit : spécialiser* $dv_{f_k}^{(i)}$ *en* $\mathbf{z}_i$, *puis calculer leurs produits scalaires avec* $r_{f_k}(\mathbf{z})$ *que l'on a normalisé par le dernier coefficient du résultat (i.e. le déterminant de Vandermonde), pour* $k \in \{1, \ldots, m\}$. *On obtient ainsi* $\Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z})$ *par concaténation.*

- *Etape 4. Pour chaque $i \in \{1, \ldots, D\}$, résoudre à l'aide d'une SVD le système*

$$(f_1(\mathbf{z}_i), \ldots, f_n(\mathbf{z}_i))^t = \Delta_{\mathbf{z}_i} \overrightarrow{\mathcal{F}}(\mathbf{z})\, \mathbf{z}'_i,$$

*où $\mathbf{z}'_i$ est la colonne d'indice $i$ de la matrice du résultat.*
- *Sortie :* *La matrice $\mathbf{z}'$.*

**Proposition 3.4.4** *La complexité arithmétique d'une itération de l'algorithme 3.4.3 est $\mathcal{O}(D^3 + mnD^2 + Dmn^2 + LmD)$ opérations arithmétiques, où $L$ est un majorant pour la complexité arithmétique de l'évaluation des polynômes d'entrés.*

*Preuve* : La preuve est la même que pour la complexité de l'algorithme 3.3.6, mais on a $m^2D$ produits de vecteurs de longueur $D+1$ à l'étape 3 au lieu de $n^2D$ et on a $D$ résolutions de système $n \times m$ à faire à l'étape 4. ♣

## 3.5 Méthode de Weierstrass modifiée

L'objectif de cette section est de proposer une méthode basée sur l'itération de Weierstrass avec un comportement global mieux contrôlé. Nous proposons une adaptation de la "méthode de Newton globale" telle qu'introduite par Steve Smale [89], mais pour approximer toutes les racines d'un système algébrique simultanément. Notre approche consiste à utiliser la fonction d'itération de Weierstrass comme opérateur de correction dans une homotopie (voir [2]).

### 3.5.1 Cas univarié

#### Principe de la méthode

C'est le cas le plus simple. Mais nous pourrons déjà voir certaines limitations de notre méthode dans ce cas. Nous nous limitons également au cadre complexe, i.e. $\mathbb{K} = \mathbb{C}$. Soit $f(x) = x^d + \sum_{i=1}^{d} a_i x^{d-i} = \prod_{i=1}^{d} (x - \zeta_i)$ un polynôme de $\mathbb{C}[x]$ n'ayant que des racines simples. On construit alors le polynôme $f_{\mathbf{z}^{(0)}}(x) = \prod_{i=1}^{d} (x - z_i)$ pour $\mathbf{z} = (z_1, \ldots, z_d) \in \mathbb{C}^d$ et tel que $z_i \neq z_j$ si $i \neq j$.

L'idée est alors de déformer continuement $f_{\mathbf{z}^{(0)}}$ en $f$ et de suivre les racines durant la déformation. On considère alors l'homotopie suivante :

$$\mathcal{H} : \left\{ \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{C}[x] \\ t & \longmapsto & (1-t)f_{\mathbf{z}^{(0)}}(x) + tf(x) \end{array} \right.$$

On a évidemment $\mathcal{H}(0) = f_{\mathbf{z}^{(0)}}(x)$ et $\mathcal{H}(1) = f(x)$. On propose alors l'algorithme suivant :

**Algorithme 3.5.1**

*Entrée : Le polynôme $f$, le vecteur $\mathbf{z}^{(0)}$ et un entier $n$ (le nombre de pas dans l'homotopie).*
- *On pose $\Delta t = \frac{1}{n}$ et $\mathbf{z} = \mathbf{z}^{(0)}$.*
- *Pour $i$ allant de 1 à $n$ faire*

$$\mathbf{z} \leftarrow \mathbf{Weierstrass}\,(\mathcal{H}(i * \Delta t), \mathbf{z})$$

- *Fin du pour.*

*Sortie : Retourner le vecteur $\mathbf{z}$.*
*Où* **Weierstrass** *est la fonction d'itération de Weierstrass.*

**Remarques 3.5.2**

1. *L'utilisation de la fonction d'itération de Weierstrass peut être diversement paramétrée, ce qui conduit à plusieurs algorithmes différents. En effet, pour ne pas avoir à faire trop de pas (c'est-à-dire à prendre $n$ grand), on peut utiliser plusieurs fois la fonction d'itération à chaque pas. Plusieurs choix sont possibles. On peut par exemple choisir de faire un nombre constant de pas à chaque itération, ou on peut choisir d'appliquer la fonction d'itération tant que la différence entre deux itérés successifs n'est pas plus petite qu'une précision donnée. Dans ce dernier cas, l'algorithme consiste juste à appliquer la méthode de Weierstrass à chaque pas, ce qui paraît une solution convenable si les pas sont suffisamment petits puisque la méthode converge localement de façon quadratique.*
2. *On remarque que dans l'algorithme proposé, la taille des pas est constante. On peut penser à contrôler la taille des pas afin d'avancer plus vite quand les racines varient peu en fonction des coefficients.*

Toutes les améliorations données par les remarques précédentes sont classiques des améliorations possibles des méthodes d'homotopie. La première remarque consiste à utiliser un opérateur de correction plus intelligent et la seconde remarque correspond à l'introduction d'un opérateur de prédiction. Mais avant de vouloir accélérer la méthode il convient d'en démontrer la convergence globale, c'est-à-dire sur un ouvert dense de $\mathbb{C}^d$. L'interprétation que nous proposons est de nature géométrique.

### Convergence globale de la méthode

Les concepts que nous introduisons seront utilisés à plusieurs reprises au cours de ce texte. Ils jouerons également un rôle important dans l'étude de la géométrie de l'itération de Weierstrass. Les figures que nous réalisons au cours du texte sont les traces réelles (dans $\mathbb{R}^2$) de la géométrie de la méthode dans le cas des polynômes de degré 2 (i.e. dans $\mathbb{C}^2$) aussi certains aspects peuvent-ils être trompeurs. Néanmoins l'art de la géométrie n'est-il pas de faire des raisonnements justes avec des figures fausses ?

On note $\Delta = \left\{\mathbf{z} \in \mathbb{C}^d | \exists i \text{ et } j \in \{1, \ldots, d\} \text{ avec } i \neq j \text{ et } z_i = z_j\right\}$. On introduit une application qui jouera un rôle important par la suite :

$$W : \left\{ \begin{array}{ccc} \mathbb{C}^d & \longrightarrow & \mathbb{C}^d \\ \mathbf{z} & \longmapsto & \left(-\sigma_1(\mathbf{z}), \ldots, (-1)^d \sigma_d(\mathbf{z})\right) \end{array} \right.$$

où les $\sigma_i$, $i \in \{1, \ldots, d\}$, sont les fonctions symétriques élémentaires. On note $\mathcal{D} = W(\Delta)$ l'image de $\Delta$ par $W$. On définit alors deux ouverts algébriques : $\mathcal{U} = \mathbb{C}^d \setminus \Delta$ qui sera appelé espace des racines et $\mathcal{V} = \mathbb{C}^d \setminus \mathcal{D}$ qui sera appelé espace des coefficients. Cette terminologie se justifie par le fait qu'à tout point $(a_1, \ldots, a_d) \in \mathcal{V}$ on peut associer le polynôme $x^d + \sum_{i=1}^{d} a_i x^{d-i}$. La variété $\mathcal{D}$ est alors appelée variété discriminante puisqu'elle représente l'ensemble des polynômes ayant une racine double au moins.

Par abus de notation on note encore $W$ pour la restriction de $W$ de $\mathcal{U}$ sur $\mathcal{V}$. On voit facilement que $W$ définit un revêtement différentiel (i.e. c'est un difféomorphisme local) dont le cardinal des fibres est $d!$. Par exemple les fibres au-dessus de $f$ sont toutes les permutations du vecteur $(\zeta_1, \ldots, \zeta_d)$. On note $(a_1, \ldots, a_d)$ le vecteur de $\mathcal{V}$ associé à $f$. On définit alors le cône de Weierstrass, noté $C_f$, comme l'ensemble des points $(b_1, \ldots, b_d)$ de $\mathcal{V}$ tels que la droite réelle passant par $(a_1, \ldots, a_d)$ et $(b_1, \ldots, b_d)$ coupe le lieu discriminant $\mathcal{D}$. Comme $\mathcal{D}$ est une variété de codimension 1 complexe, donc de codimension 2 réelle, $C_f$ est une variété de codimension 1. On note alors

$$C_f^+ = \{(b_1, \ldots, b_d) \in \mathcal{V} | \forall t \in [0,1], \, (1-t)\,(b_1, \ldots, b_d) + t\,(a_1, \ldots, a_d) \notin \mathcal{D}\}$$

et

$$C_f^- = \{(b_1, \ldots, b_d) \in \mathcal{V} | \exists t \in [0,1], \, (1-t)\,(b_1, \ldots, b_d) + t\,(a_1, \ldots, a_d) \in \mathcal{D}\}.$$

Autrement dit, $C_f^+$ est l'ensemble des points tels que le segment le joignant à $(a_1, \ldots, a_d)$ ne coupe pas $\mathcal{D}$ et $C_f^-$ est l'ensemble des points tels que le segment le joignant à $(a_1, \ldots, a_d)$ coupe $\mathcal{D}$. On considère alors $\widehat{\mathcal{V}} = \mathcal{V} \setminus C_f^-$. On peut alors constater que $\widehat{\mathcal{V}}$ est étoilé par rapport à $(a_1, \ldots, a_n)$. Il est donc connexe. De plus, $C_f^-$ est un ensemble de mesure nulle (puisque de codimension 1).

Nous allons maintenant interpréter la méthode de Weierstrass modifiée dans ce contexte. Soit $\mathbf{z}^{(0)} \in \mathcal{U}$, alors $\mathcal{H}\,(t) = (1-t) f_{\mathbf{z}^{(0)}}\,(x) + tf\,(x) = \sum_{i=1}^{d} (1-t)(-1)^i \sigma_i \mathbf{z}^{(0)} + ta_i$ paramètre un segment de droite dans $\mathcal{V}$. On a alors la proposition suivante :

**Proposition 3.5.3** *Pour $\mathbf{z}^{(0)}$ dans un ensemble dense de $\mathcal{U}$, $\left(-\sigma_1 \mathbf{z}^{(0)}, \ldots, (-1)^d \sigma_d \mathbf{z}^{(0)}\right) \in \widehat{\mathcal{V}}$. Autrement dit, pour un choix générique de $\mathbf{z}^{(0)}$ dans $\mathcal{U}$, le segment paramétré par l'homotopie $\mathcal{H}$ ne coupe pas $\mathcal{D}$.*

*Preuve* : Supposons qu'il existe un sous-ensemble $L$ de mesure non nulle de $\mathcal{U}$ tel que $\forall \mathbf{z}^{(0)} \in L$, $f_{\mathbf{z}^{(0)}}$ soit tel que $\mathcal{H}$ paramètre un segment rencontrant $\mathcal{D}$. Alors $L$ serait d'intérieur $int\,(L)$ non vide. Soit alors $\mathbf{z}^{(0)} \in int\,(L)$. Il existerait alors un voisinage $U_0$ de $\mathbf{z}^{(0)}$ inclus dans $int\,(L)$ et de mesure non nul tel que la restriction $W|_{U_0}$ est un difféomorphisme de $U_0$ sur $W\,(U_0)$. Comme $W$ est un difféomorphisme local entre espaces de même dimension, $W\,(U_0)$ serait de mesure non nulle. Donc $\forall\,(b_1, \ldots, b_d) \in W\,(U_0)$, le segment joignant $(b_1, \ldots, b_d)$ à $(a_1, \ldots, a_d)$ rencontrerait $\mathcal{D}$. Ce qui contredirait le fait que $C_f^-$ est de mesure nulle. ♣

On obtient de la proposition précédente le théorème suivant :

**Théorème 3.5.4** *La méthode de Weierstrass modifiée est globalement convergente.*

*Preuve* : Nous allons montrer que la méthode de Weierstrass modifiée converge pour tout point initial $\mathbf{z}^{(0)}$ pris dans $\widehat{\mathcal{U}}$. On note $\mathcal{H}(t) \; : \; t \mapsto$

$(1-t)f_{\mathbf{z}^{(0)}}(x)+tf(x)$ et $\mathbf{x}(t)$ un vecteur des racines de $\mathcal{H}(t)$. Comme $\mathcal{H}$ est une fonction continue sur $[0,1]$ pour $\mathbf{z}^{(0)}$ pris dans $\widehat{\mathcal{U}}$ puisqu'il paramètre un segment $\mathcal{S}$ dans $\widehat{\mathcal{V}}$, alors $x$ est une fonction continue de $[0,1]$ dans $\widehat{\mathcal{U}}$, donc uniformément continue puisque $[0,1]$ est compacte. Dont pour tout $\epsilon \in \mathbb{R}$ il existe $\eta = \eta(\epsilon) \in \mathbb{R}$ tel que pour tout $\Delta t \in \mathbb{R}$ avec $\|\Delta t\| \leq \eta$, on ait $\|\mathbf{x}(t+\Delta t)-\mathbf{x}(t)\| \leq \epsilon$, pour tout $t \in [0,1]$. Considérons un $\epsilon \in \mathbb{R}$ tel que pour tout $t \in [0,1]$, la méthode de Weierstrass converge quadratiquement dans la boule $B_{\mathcal{H}(t),\epsilon}$. Un tel $\epsilon$ existe car la méthode converge localement au voisinage de tout point de $\mathcal{S}$ et que $\mathcal{S}$ est compacte. On considère alors $n \in \mathbb{N}$ tel que $\Delta t = \frac{1}{n}$ vérifie $\|\Delta t\| \leq \eta(\epsilon)$. On note alors $\mathbf{x}^{(i)} = \mathbf{x}(i\Delta t)$, pour $i \in \{0,\ldots,n\}$ et $\mathbf{z}^{(i)}$ le point obtenu après $i$ étapes de la méthode de Weierstrass modifiée. On remarque alors que $\|\mathbf{x}^{(i+1)} - \mathbf{x}(i)\| \leq \epsilon$. On considère alors $\rho \in \mathbb{R}$ tel que $B_{\mathbf{x}^{(i)},\rho} \subset B_{\mathbf{x}^{(i+1)},\epsilon}$. Comme la méthode de Weierstrass converge quadratiquement dans $B_{\mathcal{H}(t),\epsilon}$, en notant $W$ l'application de l'itération de Weierstrass, il existe $k \in \mathbb{N}$ tel que $W^k(B_{\mathbf{x}^{(i)},\epsilon}) \subset B_{\mathbf{x}^{(i)},\rho}$ pour tout $i \in \{0,\ldots,n\}$. La fin de la preuve procède par récurrence. L'hypothèse de récurrence est que pour tout $j \leq i-1$, $z^{(j+1)} = W^k(\mathbf{z}^{(j)}) \in B_{\mathbf{x}^{(i)},\rho} \subset B_{x^{(i+1)},\epsilon}$. Sous cette hypothèse $\mathbf{z}^{(i-1)} \in B_{\mathbf{x}^{(i)},\epsilon}$ donc $\mathbf{z}^{(i)} = W^k(\mathbf{z}^{(i-1)}) \in B_{\mathbf{x}^{(i)},\rho} \subset B_{\mathbf{x}^{(i+1)},\epsilon}$, ce qui montre que si la propriété est vraie pour $i$, alors elle est vraie pour $i+1$ (voir figure 3.1). Il est alors facile de vérifié que la récurrence est bien initialisée puisque $z^{(0)} = \mathbf{x}^{(0)} \in B_{\mathbf{x}^{(1)},\epsilon}$. Ceci finit la preuve de la proposition par récurrence. ♣

Si ce théorème est un apport théorique intéressant, il ne donne cependant pas d'idée sur la complexité de la méthode. Par complexité on entend ici complexité numérique. C'est-à-dire le nombre d'étapes de nécessaire à l'algorithme pour assurer qu'on va converger à chaque étape. Cela pour répondre à la question suivante : connaissant $f$ et $\mathbf{z}^{(0)}$, quelle valeur prendre pour $n$ ? Une réponse à cette question guiderait d'ailleurs sans doute le choix d'un point initial convenable connaissant $f$. On voit néanmoins qu'un certain nombre de phénomènes intrinsèques intervient, comme la distance du segment paramétré par l'homotopie au lieu discriminant ou par la séparation des racines.

### Interprétation en termes de champs de vecteurs

Un point de vue intéressant sur la méthode de Weierstrass modifiée consiste à l'interpréter en termes d'intégration de champs de vecteurs. On considère le champ de vecteurs $\overrightarrow{\mathbf{v}}$ de $\mathcal{V}$ sur $T\mathcal{V}$ défini par $\forall p \in \mathcal{V} \rightarrow \overrightarrow{\mathbf{v}} = p - f \in T_p\mathcal{V}$. Ce champ induit un autre champ sur $\mathcal{U}$ par l'intermédiaire de $W$ de la façon suivante : pour tout $\mathbf{z} \in \mathcal{U}$, on associe le vecteur $\overrightarrow{\mathbf{u}}(\mathbf{z}) = W^*\overrightarrow{\mathbf{v}}(\mathbf{z}) = Jac_W(\mathbf{z})^{-1}\overrightarrow{\mathbf{v}}(W(\mathbf{z})) \in T_{\mathbf{z}}\mathcal{U}$. On vérifie facilement que

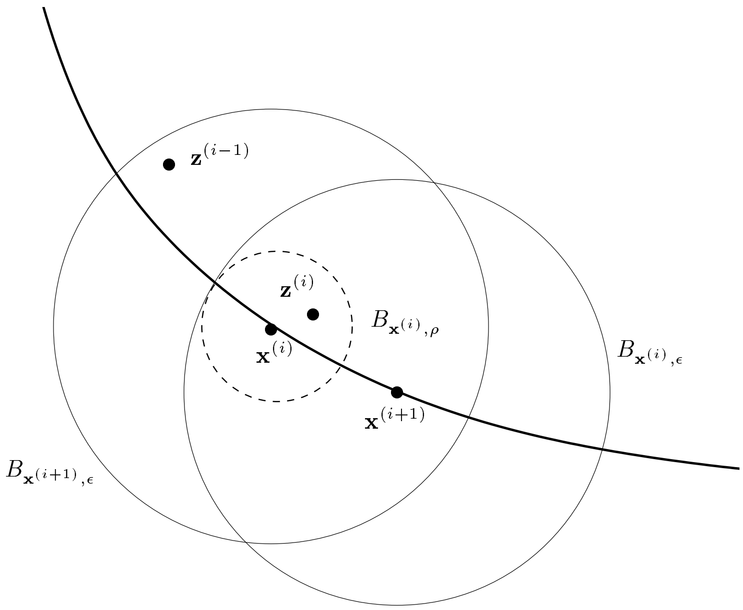


FIG. 3.1 – Convergence globale de la méthode de Weierstrass modifiée

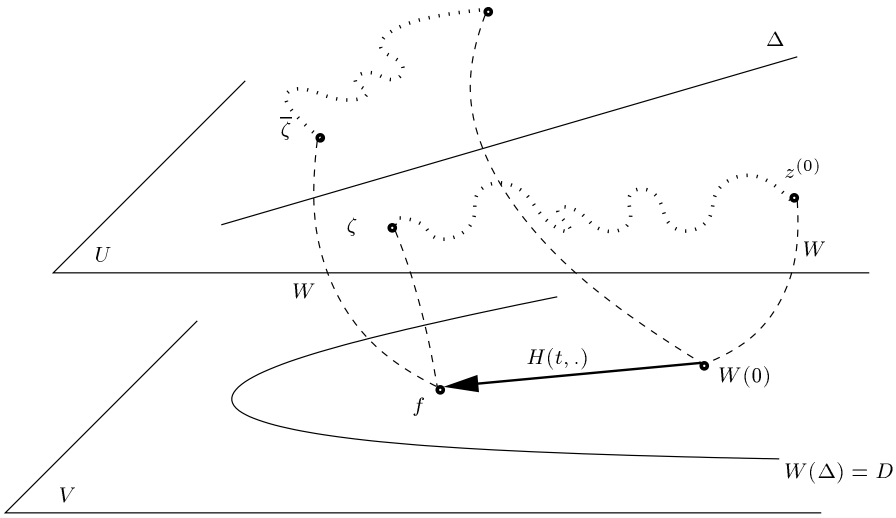


FIG. 3.2 – Suivit de courbe et méthode de Weierstrass

$\overrightarrow{\mathbf{u}}$ est bien un champ de vecteurs sur $\mathcal{U}$ appelé champ remonté de $\overrightarrow{\mathbf{v}}$ par $W$.

On considère alors alors l'équation différentielle suivante : on cherche $\gamma : [0,1] \to \mathcal{U}$ vérifiant $\frac{d\gamma(t)}{dt} = \overrightarrow{\mathbf{u}}(\gamma(t))$ avec comme condition initiale $\gamma(0) = \mathbf{z}^{(0)}$. A la trajectoire décrite par la solution de cette équation différentielle, on associe l'image de cette trajectoire donnée par $\alpha(t) = W(\gamma(t))$. On a alors $\frac{d\alpha(t)}{dt} = \frac{dW(\gamma(t))}{dt} = Jac_w(\gamma(t))\frac{d\gamma(t)}{dt}$, d'où
$\frac{d\alpha(t)}{dt} = Jac_W(\gamma(t))Jac_W(\gamma(t))^{-1}\overrightarrow{\mathbf{v}}(t)$, ce qui donne finalement que $\alpha$ est solution de l'équation différentielle

$$\frac{d\alpha(t)}{dt} = \overrightarrow{\mathbf{v}}(t)$$

avec la condition initiale $\alpha(0) = W(\gamma(0)) = W(\mathbf{z}^{(0)})$.

La méthode de Weierstrass modifiée consiste alors à appliquer la méthode d'Euler à $\overrightarrow{\mathbf{v}}$ pour laquelle les trajectoires sont des droites, à remonter le résultat de chaque itération sur $\mathcal{U}$ par $W$ et à prendre comme point d'itération suivant l'image du résultat de l'itération précédente par $W$.

Ce point de vue présente l'intérêt suivant : on peut alors utiliser d'autres méthodes que la méthode d'Euler, comme les méthodes de Runge et Kutta. Une autre perspective qui nous semble interessante serait d'étudier d'autres champs de vecteurs que ceux que nous venons d'étudier.

### 3.5.2 Cas multivarié

On considère maintenant le cas des systèmes algébriques définissant une intersection complète de dimension zéro. Ce cas est nettement plus compliqué, pas uniquement pour des raisons techniques, mais aussi pour des raisons structurelles comme nous le verrons.

#### Méthode naïve

La méthode naïve consiste à recopier brutalement ce que nous avons fait pour le cas univarié. Soient $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$, $\mathcal{I} = (f_1, \ldots, f_n)$ et $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$. On suppose que $Z(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_D\} \subset \mathbb{K}^n$ est un ensemble de racines simples et qu'on connaît un ensemble $E = \{\alpha_1, \ldots, \alpha_D\} \subset \mathbb{N}^n$ tel que $\mathbf{x}^E$ soit une base de $\mathcal{A}$. On considère alors $\mathbf{z}^{(0)} = (\mathbf{z}_1, \ldots, \mathbf{z}_D) \in (\mathbb{K}^n)^D$, un vecteur de points distincts de $\mathbb{K}^n$. On considère alors l'homotopie suivante :

**Définition 3.5.5** *Avec les notations précédentes, on définit :*

$$\mathcal{H}_{\mathbf{z}^{(0)}} : \begin{cases} [0,1] & \longrightarrow & \mathbb{K}[x_1, \ldots, x_n]^n \\ t & \longmapsto & \begin{pmatrix} tf_1(\mathbf{x}) + (1-t)R_{f_1}\left(\mathbf{z}^{(0)}, \mathbf{x}\right) \\ \vdots \\ tf_n(\mathbf{x}) + (1-t)R_{f_n}\left(\mathbf{z}^{(0)}, \mathbf{x}\right) \end{pmatrix} \end{cases}$$

L'idée est alors la même que dans le cas d'une variable :

**Algorithme 3.5.6**

<u>*Entrée*</u> *:* $n \in \mathbb{N}$, $\mathbf{z}^{(0)} \in (\mathbb{K}^n)^d$ *et* $\mathcal{H}_{\mathbf{z}^{(0)}}(t)$.
- *On pose* $\Delta t = \frac{1}{n}$ *et* $\mathbf{z} = \mathbf{z}^{(0)}$.
- *Pour i allant de 1 à n faire*

$$\mathbf{z} \leftarrow \textbf{Weierstrass}\left(\mathcal{H}\left(i\Delta t\right), \mathbf{z}\right)$$

- *Fin du pour.*

<u>*Sortie*</u> *: Retourner la valeur de* $\mathbf{z}$.

En utilisant expérimentalement cet algorithme, nous avons constaté que si le nombre de solutions du système à résoudre atteint la borne de Bézout, alors l'algorithme a un très bon comportement. Par contre, quand le nombre de solutions du système est strictement inférieur au nombre de Bézout, la méthode diverge souvent à la fin de l'homotopie. Ce qui indique qu'il ne s'agit pas d'un effet numérique. En fait, cela s'explique par un défaut de platitude de l'homotopie précédemment introduite. Dans ce qui suit nous analysons plus en détail le phénomène.

### Analyse de l'homotopie

La divergence de la méthode proposée tient au fait que l'homotopie n'est pas plate. Nous expliquons maintenant pourquoi elle ne conserve pas le nombre de racines. On note $d$ le nombre de racines du système défini par $f_1, \ldots, f_n$, qu'on suppose ici inférieur à la borne de Bézout. On considère alors le système défini par $R_{f_1}\left(\mathbf{z}^{(0)}, \mathbf{x}\right), \ldots R_{f_n}\left(\mathbf{z}^{(0)}, \mathbf{x}\right)$. On note alors $\mathcal{I}_{\mathbf{z}^{(0)}}$ l'idéal qu'ils engendrent et par $\mathcal{A}_{\mathbf{z}^{(0)}} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_{\mathbf{z}^{(0)}}$. On voit sans difficulté que pour un choix générique de $\mathbf{z}^{(0)}$, $\mathbf{x}^E$ est une famille libre de $\mathcal{A}_{\mathbf{z}^{(0)}}$ puisque génériquement $\mathbf{v}_{\mathbf{z}^{(0)},E} \neq 0$. Il se peut que génériquement $\mathbf{x}^E$ ne soit pas une base de $\mathcal{A}_{\mathbf{z}^{(0)}}$. En effet, le nombre de points de $Z\left(\mathcal{I}_{\mathbf{z}^{(0)}}\right)$, noté $D$, est généralement plus grand que $d$ et il atteint même la borne de Bézout *a priori*.

Par exemple une intersection de quadrique en deux variables ayant trois racines à coordonnées réelles, donnera, du fait que les points qu'on choisit $\mathbf{z}^{(0)}$ dans à coordonnées complexes, quatre solutions à coordonnées complexes génériquement. De plus au cours de l'homotopie, il n'y a, à première vue, aucune raison pour que le nombre de solutions reste constant. C'est même le contraire puisque le système final n'a que $d$ racines. Par contre au cours de l'homotopie, on verra qu'on garde au moins $d$ solutions. Ce qui signifie qu'on suit $d$ racines parmi $D$. Or si le nombre de racines chute, c'est que certaines racines du système initial partent à l'infini (en projectif le nombre de racine est constant). Il n'y a pas de méthode pour vérifier qu'on n'a pas choisi une des racines qui partent à l'infini au début de l'homotopie. En effet, il y a $d!$ chemins menant vers les bonnes solutions parmi $D!$. Cela donne une très faible probabilité d'aboutir en tirant au hasard.

Il est donc nécessaire de trouver une méthode pour garantir que le nombre de solutions est constant au cours de l'homotopie. Cette problématique est assez neuve car généralement dans les méthodes par homotopie, on cherche à ne pas perdre de racines, alors qu'ici on souhaite ne pas en rajouter. L'idée naturelle pour résoudre notre problème est de rajouter une condition qui contrôle le nombre de solutions, c'est-à-dire une nouvelle équation qui contrôle le nombre de monômes engendrant l'idéal défini par les polynômes au cours de l'homotopie. Mais dans ce cas, nous avons besoin d'avoir une fonction d'itération dans le cas surcontraint (donc en dehors du cas de l'intersection complète). C'est l'objet de ce qui suit.

### 3.5.3 Méthode de Gauss-Weierstrass modifiée

Pour la méthode de Weierstrass modifiée naïve, pour tout $\mathbf{z}^{(0)}$, on a construit une homotopie $\mathcal{H} : [0,1] \to \mathbb{K}[x_1, \ldots, x_n]^n$ qui pour tout $t \in [0,1]$ définit un système $\mathcal{H}(t)$. On a vu que le nombre de solutions de ces systèmes peut varier, même s'il est toujours plus grand ou égal au nombre de solutions $d$ du système $\mathcal{H}(1)$. Cela pose des problèmes pour suivre un chemin continu de $d$ solutions de $\mathcal{H}(0)$ vers les $d$ solutions de $\mathcal{H}(1)$. Une démarche naturelle pour pallier ce problème est alors de rajouter des équations pour "tuer" les solutions parasites au départ de l'homotopie. On utiliserait alors une homotopie surcontrainte, basée sur l'itération de Gauss-Weierstrass. Mais avant cela, il convient de résoudre le problème suivant : quelles équations peut-on rajouter afin de garantir le nombre de racines au début de l'homotopie ?

Dans la suite de cette sous-section, on suppose que le système à résoudre définit un intersection complète affine. On peut néanmoins reprendre tous les résultats exposés ici pour le cas où le système à résoudre est surcontraint sans difficultés supplémentaires.

### Application de Gauss-Weierstrass

On considère $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$. On suppose que $Z(f_1, \ldots, f_n)$ est un ensemble fini $\{\zeta_1, \ldots, \zeta_d\}$ et que toutes ces racines sont simples. On suppose également qu'on dispose d'un ensemble $E = \{\alpha_1, \ldots, \alpha_d\} \subset \mathbb{N}^n$, tel que $\mathbf{x}^E$ est une base de $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$. On peut toujours supposer qu'il existe $i$ et $j \in \{1, \ldots, n\}$ tels que le support monomial de $f_{n+1} = x_j f_i$ contient des monômes qui ne sont ni dans les supports des $f_k$, $k \in \{1, \ldots, n\}$, ni dans $E$. On définit alors l'application polynomiale $\mathbf{f} = (f_1, \ldots, f_n, f_{n+1})$. On a $Z(f_1, \ldots, f_n) = \mathbf{f}^{-1}(0) = Z(f_1, \ldots, f_n, f_{n+1})$. Pour tout $i \in \{1, \ldots, n+1\}$, on définit $A_i$ comme l'union des exposants des monômes du support de $f_i$ avec $E$. On définit l'application suivante :

**Définition 3.5.7** *L'application de Gauss-Weierstrass est définie par :*

$$GW : \left\{ \begin{array}{ccc} (\mathbb{K}^n)^d & \longrightarrow & \displaystyle\prod_{i=1}^{n+1} \mathbf{x}^{A_i} \\ \mathbf{z} & \longmapsto & \begin{pmatrix} R_{f_1}(\mathbf{z}, \mathbf{x}) \\ \vdots \\ R_{f_{n+1}}(\mathbf{z}, \mathbf{x}) \end{pmatrix} \end{array} \right.$$

*La source de $GW$ est appelée espace des racines et le but espace des systèmes.*

On définit $\Delta = \left\{ \mathbf{z} \in (\mathbb{K}^n)^d \parallel \exists i \neq j \in \{1, \ldots, d\} \text{ avec } \mathbf{z}_i = \mathbf{z}_j \right\}$. On a la proposition suivante :

**Proposition 3.5.8**
*Pour $\mathbf{z}$ pris dans un ouvert dense de $(\mathbb{K}^n)^d$, on a $GW^{-1}(GW(\mathbf{z})) = \{\mathbf{z}^\sigma \parallel \sigma \in S_d\}$.*

*Preuve* : On peut supposer que $\mathbf{z} \notin \Delta$ puisque $\Delta$ est un sous-ensemble algébrique de codimension 1 et qui est donc de mesure nulle. On note $X = Z(R_{f_1}, \ldots, R_{f_n})$. Comme $R_{f_{n+1}}$ contient des monômes qui ne sont pas dans $\cup_{i=1}^n \mathbf{x}^{A_i}$, alors $R_{f_{n+1}}$ est un polynôme séparant de $\mathbf{z}$ relativement à $X$ par la proposition 2.5.8, pour $\mathbf{z}$ pris dans un ouvert dense de $(\mathbb{K}^n)^d$. Ce qui prouve la proposition. ♣

On note $\Xi$ l'ensemble des points de $(\mathbb{K}^n)^d$ tel que $R_{f_{n+1}}$ ne soit pas un polynôme séparant de $\mathbf{z}$. On définit alors $\mathcal{U} = (\mathbb{K}^n)^d \backslash (\Delta \cup \Xi)$. C'est un ouvert dense de $(\mathbb{K}^n)^d$. Par abus de langage on note encore $GW$ la restriction de l'application de Gauss-Weierstrass à $\mathcal{U}$. On note $\mathcal{V} = GW(\mathcal{U})$. On a alors la proposition suivante :

**Proposition 3.5.9** *L'appication $GW : \mathcal{U} \to \mathcal{V}$ est un revétement différentiel dont les fibres sont de cardinal $d!$.*

*Preuve* : Puisque $GW$ est une application polynomiale, elle est différentiable. De plus, pour tout $\mathbf{g} \in \mathcal{V}$, il existe $\mathbf{z} \in \mathcal{U}$ tel que $\mathbf{g} = GW(\mathbf{z})$. Alors par la proposition 3.5.8, $GW^{-1}(\mathbf{g}) = GW^{-1}(GW(\mathbf{z})) = \{\mathbf{z}^\sigma \parallel \sigma \in S_d\}$. ♣

Avec ces notations, $GW$ paramètre l'ensemble des systèmes de $\prod_{i=1}^{n+1} \mathbf{x}^{A_i}$ ademettant $\mathbf{x}^E$ comme base de l'algèbre quotient associée et dont les $d$ solutions sont distincts. L'idée est maintenat de définir une homotopie de $GW(\mathbf{z}^{(0)})$ à $\mathbf{f}$, pour $\mathbf{z}^{(0)} \in \mathcal{U}$, et de suivre les racines dans $\mathcal{U}$ en remontant par $GW$. Cela entraîne des difficultés nouvelles, au niveau de la pratique et en théorie.

### Métode de Gauss-Weiertrass modifiée

L'idée première est de définir l'homotopie suivante : pour tout $\mathbf{z}^{(0)} \in \mathcal{U}$, on définit :

$$H_{\mathbf{z}^{(0)}} : t \in [0,1] \;\to\; (1-t)GW(\mathbf{z}^{(0)}) + t\mathbf{f}.$$

Cela nous conduit à l'algorithme suivant :

**Algorithme 3.5.10 (Gauss-Weiertrass modifié)**

<u>*Entrée*</u> *:* $\mathbf{z}^{(0)} \in \mathcal{U}$, $H_{\mathbf{z}^{(0)}}$ *et un entier* $N$.
- *On pose* $\Delta t = \frac{1}{N}$ *et* $\mathbf{z} = \mathbf{z}^{(0)}$.
- *Pour* $i$ *allant de* 1 *à* $N$ *faire*

$$\mathbf{z} \leftarrow \mathbf{GaussWeiers}\,(H_{\mathbf{z}^{(0)}}(i * \Delta t), \mathbf{z})$$

- *Fin du faire.*

<u>*Sortie*</u> *: Retourner* $\mathbf{z}$.

Où **GaussWeiers** est l'itération de Gauss-Weierstrass décrite dans l'algorithme 3.4.3. Nous proposons maintenant une interprétation gométrique de cette méthode.

On remarque que l'homotopie $H_{\mathbf{z}^{(0)}}$ paramètre un ségment qui n'est pas contenu dans $\mathcal{V}$. Cela rend l'interprétation globale de cette méthode difficile. Néanmoins cela reste possible à partir de l'interprétation d'un pas de la méthode. Supposons qu'on ait calculé $\mathbf{z}^{(i)} \in \mathcal{U}$, la i-ème valeur prise par $\mathbf{z}$ au cours du procéd'e. L'itération de Gauss-Weiertrass revient alors à projetter

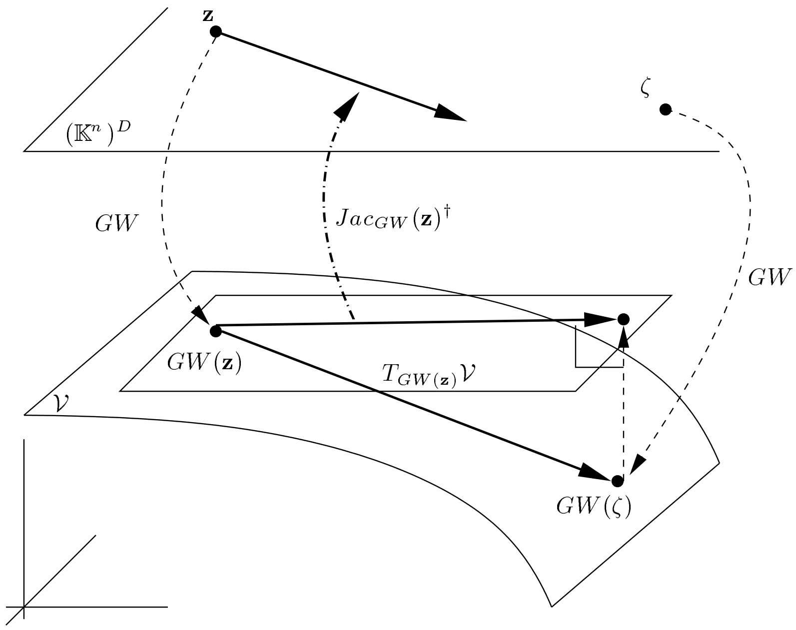


FIG. 3.3 – Interprétation de la méthode de Gauss-Weierstrass

le vecteur $\overrightarrow{GW(\mathbf{z}^{(i)})H((i+1)\Delta t)}$ sur l'espace $T_{GW(\mathbf{z}^{(i)})}\mathcal{V}$ orthogonalement à ce dernier, afin d'obtenir un vecteur de $T_{GW(\mathbf{z}^{(i)})}\mathcal{V}$ que l'on remonte par $GW$ sur $T_{\mathbf{z}^{(i)}}\mathcal{U}$ (voir la figure 3.5.3). Le vecteur remonté est le terme correctif de la méthode.

On peut encore donner une interprétation de cette méthode en termes de champs de vecteurs. Mais, comme nous le verrons, le champ de vecteur impliqué n'est pas autonome.

Pour tout $\mathbf{g} \in \mathcal{V}$, on note $\Pi_g$ la projection sur $T_{\mathbf{g}}\mathcal{V}$ orthogonalement à cet espace. On considère alors l'application suivante :

$$\rho : \left\{ \begin{array}{ccc} [0,1] \times \mathcal{V} & \longrightarrow & T\mathcal{V} \\ (t, \mathbf{g}) & \longmapsto & \Pi_g\left(\overrightarrow{\mathbf{g}H_{\mathbf{z}^{(0)}}(t)}\right) \end{array} \right.$$

La méthode proposée revient alors à intégrer l'équation différentielle suivante :

$$\frac{d}{dt}\gamma(t) = \rho(t, \gamma(t)) \tag{3.17}$$

avec comme condition initiale $\gamma(0) = GW(\mathbf{z}^{(0)})$, et à suivre le chemin correspondant dans l'espace des racines. Nous ne sommes malheureusement

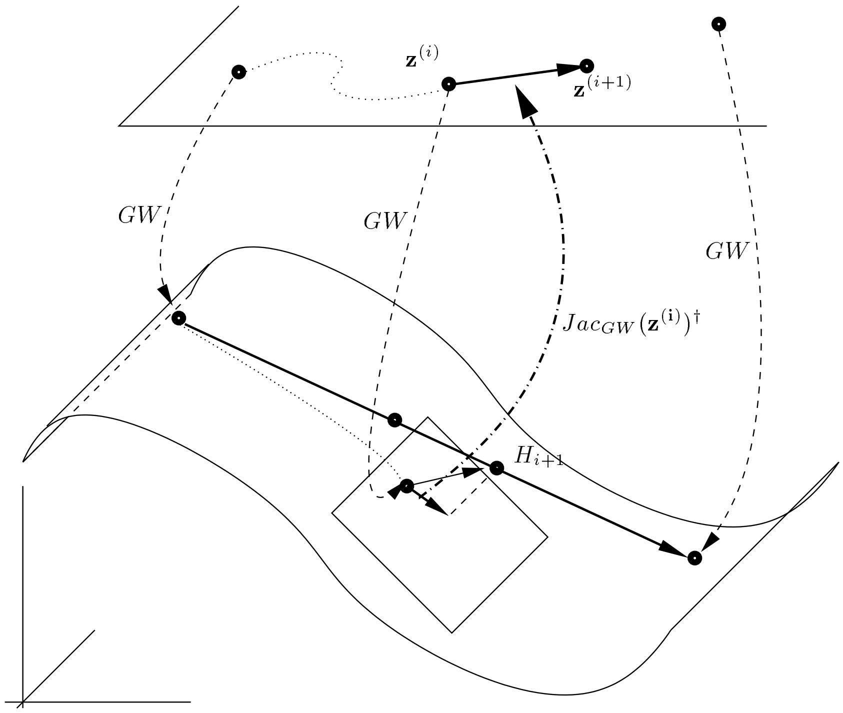


FIG. 3.4 – Interprétation locale-globale de la méthode de Gauss-Weierstrass modifiée

pas capable de certifié ou d'infirmer la correction de cette approche. En effet, si la formulation que nous vennons de donner permet de voir que nous définissons un chemin continuement dérivable sur $\mathcal{V}$, rien ne nous permet de garantir que $\gamma(1) = \mathbf{f}$.

## 3.6 Expérimentations

Dans cette section on présente les résultats d'expériences numériques de la méthode de Weierstrass modifiée multivariée.

### 3.6.1 Implémentation

On a implémenté l'algorithme de Weierstrass multivarié modifié pour les intersections complètes sans zéro à l'infini. Cette implémentation repose sur la bibliothèque de fonctions C++ appelée SYNAPS et développée au sein du projet GALAAD. Cette bibliothèque regroupe un ensemble cohérent de fonctions pour le calcul scientifique avec de l'algèbre polynomiale et linéaire. Nos fonctions n'utilisent que l'arithmétique des nombres flottants double précision (double float) ou des nombres complexes utilisant cette arithmétique. On peut adapter notre implémentation pour d'autres types d'arithmétiques, mais on risque alors de perdre les avantages de nombreuses bibliothèques très spécialisées connectées à SYNAPS. Nous utilisons notamment les fonctions d'algèbre linéaire de la bibliothèque LAPACK qui est une bibliothèque FORTRAN très éprouvée et fiable.

### 3.6.2 Expériences numériques

Nos expériences avaient pour but d'étudier l'impact sur les performances de la méthode de deux paramètres :

- le nombre de pas effectués durant le procédé d'homotopie (qui sera noté *nbstep* par la suite),
- le nombre d'appels à la fonction d'itération de Weierstrass effectués à chaque pas de l'homotopie (qui sera notée *nbiter* par la suite).

Le temps est donné en secondes et la précision (qui sera notée *prec*) est la norme du vecteur formé des polynômes du système à résoudre évalués aux approximations fournies par l'algorithme. Les calculs ont été effectués avec un ordinateur doté d'un processeur pentium 3 (933 MHz) et de 500 Mo de SDRAM.

#### Intersections de quadriques

On calcule ici une approximation des 8 racines d'un système formé de 3 quadriques génériques en trois variables.

| nbiter | 10 | | 7 | | 5 | | 3 | |
|---|---|---|---|---|---|---|---|---|
| nbstep | time | prec | time | prec | time | prec | time | prec |
| 55 | 0.15 | $10^{-21}$ | 0.1 | $10^{-22}$ | 0.05 | $10^{-18}$ | 0.04 | 10 |
| 60 | 0.18 | $10^{-21}$ | 0.12 | $10^{-22}$ | 0.08 | $10^{-20}$ | 0.05 | 1 |
| 75 | 0.2 | $10^{-22}$ | 0.15 | $10^{-22}$ | 0.12 | $10^{-22}$ | 0.08 | $10^{-1}$ |
| 100 | 0.2 | $10^{-22}$ | 0.17 | $10^{-22}$ | 0.15 | $10^{-22}$ | 0.09 | $10^{-2}$ |

On calcule maintenant une approximation des 16 racines d'un système formé de 4 quadriques en 4 variables. On traite deux problèmes différents afin de montrer l'impact du conditionnement des racines sur la méthode :

| nbiter | 5 | | 3 | |
|---|---|---|---|---|
| Premier problème. | | | | |
| nbstep | time | prec | time | prec |
| 300 | 7 | $10^{-21}$ | 4 | $10^{-10}$ |
| 250 | 6 | $10^{-22}$ | 3 | $10^{-12}$ |
| Second problème. | | | | |
| 200 | 4 | $10^{-7}$ | 3 | $10^{-1}$ |
| 300 | 6 | $10^{-9}$ | 5 | $10^{-2}$ |
| 400 | 8 | $10^{-9}$ | 6 | $10^{-2}$ |

On remarque qu'on ne perd pas beaucoup de précision en diminuant le nombre de pas. Cependant pour le deuxième problème, qui est mal conditionné, on doit garder une précision d'au moins $10^{-10}$ pour assurer une bonne convergence globale. Ce qui nous oblige à faire au moins 250 pas dans le cas présent.

### Intersections d'une cubique avec des quadriques

On calcule une approximation des 12 racines d'un système formé de 2 quadriques génériques avec une cubique en trois variables. On traite de nouveau deux problèmes ayant des conditionnements différents.

| nbiter | 10 | | 7 | | 5 | |
|---|---|---|---|---|---|---|
| nbstep | time | prec | time | prec | time | prec |
| Premier problème. | | | | | | |
| 10 | 0.7 | $10^{-17}$ | 0.4 | $10^{-17}$ | $\infty$ | $\infty$ |
| 25 | 1.2 | $10^{-17}$ | 0.7 | $10^{-17}$ | $\infty$ | $\infty$ |
| 50 | 1.9 | $10^{-17}$ | 1 | $10^{-17}$ | 0.9 | $10^{-16}$ |
| 100 | 5 | $10^{-18}$ | 1.7 | $10^{-18}$ | 1.5 | $10^{-18}$ |
| Second problème. | | | | | | |
| 20 | 0.5 | $10^{-19}$ | 0.4 | $10^{-20}$ | 0.1 | $10^{-18}$ |
| 30 | 0.6 | $10^{-20}$ | 0.5 | $10^{-20}$ | 0.1 | $10^{-19}$ |

De nouveau, on constate qu'on a besoin de garder une précision d'autant plus grande que les racines du système à résoudre sont proches.

### Intersections de cubiques

On calcule une approximation des 27 racines d'un système formé de 3 cubiques en 3 variables.

| nbiter | 10 | | 7 | | 5 | | 3 | |
|---|---|---|---|---|---|---|---|---|
| nbstep | time | prec | time | prec | time | prec | time | prec |
| 10 | 1 | $10^{-14}$ | 0.2 | $10^{-14}$ | 0.1 | $10^{-1}$ | $\infty$ | $\infty$ |
| 20 | 2 | $10^{-17}$ | 0.5 | $10^{-15}$ | 0.1 | $10^{-4}$ | $\infty$ | $\infty$ |
| 30 | 3 | $10^{-17}$ | 0.8 | $10^{-17}$ | 0.2 | $10^{-17}$ | 0.1 | $10^{-8}$ |

**D'autres expériences**

D'autres expériences ont été menées avec des systèmes ayant plus de racines, mais on atteint alors les limites de l'arithmétique utilisée (comme pour l'approximation des 54 racines de l'intersection de 3 cubiques avec une quadrique en 4 variables). Mais cela a nécessité la mise en œuvre de techniques différentes comme le contrôle dynamique de la précision au cours du suivit de chemin. Le problème de la résolution de grands systèmes de type Vandermonde demeure. L'utilisation d'arithmétiques étendues s'est vue limitée par l'efficacité des procédures d'algèbre linéaire utilisées. Le temps de calcul devient alors déraisonnable.

### 3.6.3 Conclusions

Nos expériences ont montré que la méthode proposée est efficace. Beaucoup d'optimisations sont encore possibles, au niveau pratique, mais aussi théorique. La mise en œuvre de cet algorithme nous a également permis d'implémenter des fonctions pour le calcul de la plupart des objets décrits au chapitre 2.

Comme nous l'avions supposé, les paramètres comme le conditionnement des racines jouent un rôle important dans le comportement de l'algorithme. De plus la méthode proposée semble bien adaptée à des problèmes pratiques comme la déformation de modèle géométrique en CAO.

Une implémentation de la méthode de Gauss-Weiersrass modifiée reste à faire et semble une voie prometteuse même si elle nécessitera la mise en place d'outils logiciels différents (algèbre linéaire efficace avec les arithmétiques étendues).

## 3.7 Conclusion

Dans ce chapitre, nous avons généralisé les méthodes de Weierstrass et d'Aberth dans le cas multivarié en nous basant sur les outils développés au chapitre 2. Nous avons aussi donné une fonction d'itération de type Weierstrass multivariée pour les systèmes surcontraints aboutissant ainsi à un méthode que nous avons appelée méthode de Gauss-Weierstrass. Nous avons ensuite utilisé les fonctions d'itérations de Weierstrass et de Gauss-Weierstrass comme opérateurs de correction dans des procédés de suivi de chemin. Des expérimentations ont été faites illustrant l'efficacité de cette approche.

Nous avons vu que les méthodes de Weierstrass et de Gauss-Weierstrass modifiées peuvent être interprétées comme des méthodes d'intégration de champs de vecteurs. Cela ouvre des perspectives nouvelles puisque cette interprétation conduit naturellement à vouloir utiliser d'autres méthodes pour intégrer numériquement ces champs de vecteurs. Ce travail permet d'imaginer de nouveaux développements dans le domaine de la résolution numérique d'équations algébriques.

# Chapitre 4

# Algèbres de Gorenstein, résidu algébrique et bézoutien

## 4.1 Introduction

Les algèbres de Gorenstein sont un cadre de travail particulièrement agréable et assez général. Ce sont des algèbres pour lesquelles des formes linéaires particulières codent beaucoup d'informations sur ces algèbres. Notamment, toutes les algèbres quotients associés à des intersections complètes sont de Gorenstein. Dans ce cadre, la forme linéaire codant l'information peut être calculée à partir du bézoutien. L'étude des algèbres de Gorenstein est l'objet de la première section. Dans une deuxième section, nous montrons comment le bézoutien exprime le fait qu'une intersection complète est de Gorenstein et comment il permet de calculer une forme bilinéaire particulière appelée résidu algébrique. La troisième section est consacrée au calcul du résidu algébrique et à des applications de cet objet.

Les deux premières sections suivent d'assez pret l'exposé fait dans [39]. Beaucoup de résultats sont aussi dans [7] où les algèbres de Gorenstein sont appelées algèbres de Kronecker.

## 4.2 Algèbres de Gorenstein

### 4.2.1 Retour sur la dualité locale

Nous revenons ici sur la dualité des algèbres locales de dimension zéro sur un corps $\mathbb{K}$ de caractéristique zéro (bien que certains résultats et définitions restent valides dans un cadre plus large). Cela s'explique par le besoin d'introduire de nouvelles notions dont nous n'avions pas besoin jusque là. Nous nous plaçons systématiquement sur une algèbre locale de dimension zéro puisque nous avons vu que toute algèbre de dimension zéro se décompose comme somme directe de ses facteurs locaux.

Soit $\mathcal{A}$ une $\mathbb{K}$-algèbre locale de dimension zéro et d'idéal maximal $\mathbf{m}$. On définit alors :

**Définition 4.2.1** *Soit $M$ un $\mathcal{A}$-module de type fini. On définit le sommet de $M$ comme le quotient sommet$(M) = M/\mathbf{m}M$.*

On voit donc que si $\mathcal{A}$ est un quotient du type $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$, avec $Z(\mathcal{I}) = \{0\}$, on a $Sommet(\mathcal{A}) = \mathbb{K}$. Donc une telle algèbre a un sommet simple. Ce sera toujours le cas dans ce qui suivra puisque nous ne nous intéressons qu'à des algèbres de ce type.

Le lemme de Nakayama montre que le sommet de $M$ contrôle ses générateurs. C'est aussi le plus grand sous-module quotient de $M$ qui est une somme directe de sous-modules simples (i.e. libres de rang 1). Sa notion duale est définie comme suit :

**Définition 4.2.2** *Soit $M$ un $\mathcal{A}$-module de type fini. On définit alors le socle de $M$ comme l'annulateur de $\mathbf{m}$ dans $M$, ou de façon équivalente, comme la somme directe des sous-modules libres de $M$.*

On voit que comme le sommet de $\mathcal{A}$ est simple (comme $\mathcal{A}$-module), alors le socle de $\widehat{\mathcal{A}}$ est simple. On remarque que le socle d'un module gradué est naturellement un module gradué, mais il n'est pas toujours formé d'éléments de même degré. Ainsi par exemple une base monomiale de $\mathcal{A} = \mathbb{K}[x,y]/\left(x^2, x^2y, y^3\right)$ est $\left\{1, x, y, \mathbf{xy}, \mathbf{y}^2\right\}$ et une base duale de cette base est $\left\{\widehat{y^2}, \widehat{xy}, \widehat{y}, \widehat{x}, \widehat{\mathbf{1}}\right\}$. Pour chaque vecteur de $\mathcal{A}$ dans la base monomiale on note $\widehat{f}$ l'expression correspondante dans la base duale. Notons que pour passer d'un module gradué à son module dual, il faut renverser les graduations. Ici les sommets sont à gauche et les socles à droite dans les représentations des bases. On voit que si le sommet de $\mathcal{A}$ est simple, le socle de $\mathcal{A}$ ne l'est pas. Par conséquent le sommet de $\widehat{\mathcal{A}}$ n'est pas simple non plus.

Pour $\mathcal{A} = \left(x^2, y^3\right)$, une base monomiale est $\left\{1, x, y, xy, y^2, xy^2\right\}$ qui admet $\left\{\widehat{(xy^2)}\right\}$ comme base du sommet de $\widehat{\mathcal{A}}$ (donc ce sommet est simple). C'est une situation générale pour les intersections complètes (voir [35]). Dans le formalisme de l'algèbre commutative, $\mathcal{A} = \mathrm{Hom}_{\mathbb{K}}(\mathcal{A}, \mathbb{K})$ est le module canonique de $\mathcal{A}$.

### 4.2.2 Algèbres de Gorenstein

On note $\mathcal{A}$ une $\mathbb{K}$-algèbre commutative unitaire de dimension $D$ finie comme $\mathbb{K}$-espace vectoriel. On note $\widehat{\mathcal{A}}$ l'espace vectoriel dual de $\mathcal{A}$ (i.e. $\mathrm{Hom}_{\mathbb{K}}(\mathcal{A},\mathbb{K})$). On a déjà vu que $\widehat{\mathcal{A}}$ est naturellement muni d'une structure de $\mathcal{A}$-module. De même $\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}$ est muni d'une structure de $\mathcal{A}$-module de la façon suivante : $\forall\lambda\in\mathcal{A}$ et $a\otimes b\in\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}$ on a $\lambda(a\otimes b)=\lambda a\otimes b=a\otimes\lambda b$. Le noyau de l'application $\sum_{i=1}^{D} a_i\otimes b_i\in\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}\mapsto\sum_{i=1}^{D} a_ib_i\in\mathcal{A}$ sera noté $\mathcal{D}$. Il est engendré, pour la structure de $\mathcal{A}$-module, par les éléments de la forme $a\otimes 1-1\otimes a$, $a\in\mathcal{A}$.

On considère l'application $\overline{\chi}:\left\{\begin{array}{ccc}\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A} & \to & \mathrm{Hom}_{\mathbb{K}}\left(\widehat{\mathcal{A}},\mathcal{A}\right)\\ a\otimes b & \mapsto & \overline{\chi}(a\otimes b)\end{array}\right.$

définie par $\overline{\chi}(a\otimes b):\left\{\begin{array}{ccc}\widehat{\mathcal{A}} & \to & \mathcal{A}\\ \Lambda & \mapsto & (1\otimes\Lambda)(a\otimes b)\end{array}\right.$, i.e. $\overline{\chi}(a\otimes b)(\Lambda)=\Lambda(b)\,a$.

De façon analogue on peut définir $\underline{\chi}$ de $\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}$ dans $\mathrm{Hom}_{\mathbb{K}}\left(\widehat{\mathcal{A}},\mathcal{A}\right)$ par $\underline{\chi}(a\otimes b)(\Lambda)=\Lambda(a)\,b$. Considérons $\sum_{i=1}^{D} a_i\otimes b_i\in\mathrm{Ker}(\overline{\chi})$ avec $(a_i)$ et $(b_i)$ $\mathbb{K}$-linéairement indépendants. On considère alors $\Lambda\in\widehat{\mathcal{A}}$, une forme linéaire définie par $\Lambda(b_1)=1$ et $\Lambda(b_i)=0$, $\forall i\in\{1,\ldots,D\}$. D'où $\overline{\chi}\left(\sum_{i=1}^{D} a_i\otimes b_i\right)(\Lambda)=\sum_{i=1}^{D}\Lambda(b_i)\,a_i=a_1$, mais comme $\overline{\chi}\sum_{i=1}^{D} a_i\otimes b_i=0$, on a $a_1=0$, ce qui contredit l'hypothèse que $(a_i)$ est libre sur $\mathbb{K}$, donc finalement $\mathrm{Ker}(\overline{\chi})=\{0\}$. L'application $\overline{\chi}$ est donc injective. Comme $\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}$ et $\mathrm{Hom}_{\mathbb{K}}\left(\widehat{\mathcal{A}},\mathcal{A}\right)$ sont des $\mathbb{K}$-espaces vectoriels de dimension finie et qu'ils ont la même dimension, on en déduit la proposition suivante :

**Proposition 4.2.3** *Les applications $\overline{\chi}$ et $\underline{\chi}$ sont des isomorphismes de $\mathbb{K}$-espaces vectoriels entre $\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}$ et $\mathrm{Hom}_{\mathbb{K}}\left(\widehat{\mathcal{A}},\mathcal{A}\right)$.*

Après nous être intéressé à la structure de $\mathbb{K}$-espace vectoriel, nous traitons ici la structure de $\mathcal{A}$-module. Nous avons déjà vu que $\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}$ est muni d'une structure de $\mathcal{A}$-module, on s'intéresse désormais à $\mathrm{Hom}_{\mathcal{A}}\left(\widehat{\mathcal{A}},\mathcal{A}\right)$. Cet ensemble est muni d'une structure de $\mathcal{A}$-module de la façon suivante : $\forall f\in\mathrm{Hom}_{\mathcal{A}}\left(\widehat{\mathcal{A}},\mathcal{A}\right)$, $\forall a\in\mathcal{A}$, on définit $af\in\mathrm{Hom}_{\mathcal{A}}\left(\widehat{\mathcal{A}},\mathcal{A}\right)$ par $\forall\Lambda\in$

$\widehat{\mathcal{A}}$, $(af)(\Lambda) = af(\Lambda) \in \mathcal{A}$. On considère alors $\mathrm{Ann}_{\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}}(\mathcal{D}) = \{(a\otimes b) \in \mathcal{A}\otimes_{\mathbb{K}}\mathcal{A} | (a\otimes b)\,\delta = 0, \forall \delta \in \mathcal{D}\}$. Cet ensemble hérite la structure de $\mathcal{A}$-module de $\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}$. On a alors le théorème suivant :

**Théorème 4.2.4** *Les applications $\overline{\chi}$ et $\underline{\chi}$ induisent des isomorphismes de $\mathcal{A}$-modules entre $Ann_{\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}}(\mathcal{D})$ et $Hom_{\mathcal{A}}\left(\widehat{\mathcal{A}}, \mathcal{A}\right)$.*

*Preuve* : Soit $\sum_{i=1}^{D} a_i \otimes b_i \in \mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}$. On a $\sum_{i=1}^{D} a_i \otimes b_i \in \mathrm{Ann}_{\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}}(\mathcal{D})$ si et seulement si $\forall a \in \mathcal{A}$, $\sum_{i=1}^{D} (a_i\otimes b_i)(1\otimes a - a\otimes 1) = 0$ ce qui équivaut à dire que $\forall a \in \mathcal{A}$, $\sum_{i=1}^{D} (aa_i \otimes b_i) = \sum_{i=1}^{D} (a_i \otimes ab_i)$ ce qui est équivalent à dire que $\forall a \in \mathcal{A}$ et $\Lambda \in \widehat{\mathcal{A}}$, $a\overline{\chi}\left(\sum_{i=1}^{D} a_i\otimes b_i\right)(\Lambda) = \overline{\chi}\left(\sum_{i=1}^{D} a_i\otimes b_i\right)(a\Lambda)$ et finalement cela équivaut à dire que $\overline{\chi}\left(\sum_{i=1}^{D} a_i\otimes b_i\right) \in \mathrm{Hom}_{\mathcal{A}}\left(\widehat{\mathcal{A}}, \mathcal{A}\right)$. ♣

Nous donnons ici la définition des algèbres de Gorenstein comme des algèbres vérifiant une des propriétés du théorème suivant. Nous ne donnerons la preuve de l'équivalence de ces propriétés que dans le cas des algèbres de dimension zéro bien que ce résultat reste valable pour un cadre plus large (comme celui des intersections complètes). Une algèbre est dite de Gorenstein si elle vérifie une des assertions du théorème suivant :

**Théorème 4.2.5** *Les assertions suivantes sont équivalentes :*

*i) $Hom_{\mathcal{A}}\left(\widehat{\mathcal{A}}, \mathcal{A}\right)$ est un $\mathcal{A}$-module libre de rang 1, et de façon équivalente $Ann_{\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}}(\mathcal{D})$ est un $\mathcal{A}$-module libre de rang 1.*

*ii) $\mathcal{A}$ et $\widehat{\mathcal{A}}$ sont isomorphes comme $\mathcal{A}$-module.*

*iii) $\widehat{\mathcal{A}}$ est un $\mathcal{A}$-module libre de rang 1.*

*iv) Il existe une forme linéaire $\tau \in \widehat{\mathcal{A}}$ telle que la forme bilinéaire $(a,b) \in \mathcal{A}\times\mathcal{A} \to \tau(ab) \in \mathbb{K}$ est non dégénérée (i.e. $\tau(ab) = 0, \forall b \in \mathcal{A}$ implique que $a = 0$).*

*v) Il existe $\Delta = \sum_{i=1}^{D} a_i \otimes b_i \in Ann_{\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}}(\mathcal{D})$, avec $(a_i)$ et $(b_i)$ deux bases de $\mathcal{A}$ comme $\mathbb{K}$-espace vectoriel.*

*Preuve* : Nous nous référons à [39, 87, 62]. ♣

**Définition 4.2.6** *Soit $\mathcal{A}$ une $\mathbb{K}$-algèbre de Gorenstein. La forme linéaire $\tau$ est appelée résidu algébrique (ou symbole de Grothendieck) de $\mathcal{A}$ pour $\Delta$.*

**Remarque 4.2.7** *Une autre caractérisation utile d'une algèbre de Gorenstein, donné dans [35], est que son socle est simple. En reprenant les exemples de la section précédente il apparaît clairement que $\mathbb{K}[x,y]/\left(x^2,y^3\right)$ est une algèbre de Gorenstein tandis que $\mathbb{K}[x,y]/\left(x^2,xy^2,y^3\right)$ n'en est pas une. Nous reviendrons sur ce point ultérieurement.*

Dans la section suivante, nous nous intéressons à la représentation des algèbres de Gorenstein.

### 4.2.3 Représentation des algèbres de Gorenstein

Soit $\mathcal{A}$ une algèbre de Gorenstein de dimension finie $D$ comme $\mathbb{K}$-espace vectoriel. Dans la section précédente nous avons vu qu'il existe une forme bilinéaire définie comme suit :

$$\forall a \in \mathcal{A} \text{ et } b \in \mathcal{A},\ \langle a,b\rangle = \tau\left(ab\right) = \left(a\tau\right)\left(b\right) = \overline{\chi}\left(\Delta\right)^{-1}\left(a\right)\left(b\right).$$

On a alors la proposition suivante :

**Proposition 4.2.8** *Soit $\sum_{i=1}^{d'} a_i \otimes b_i$ une décomposition de $\Delta \in Ann_{\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}}\left(\mathcal{D}\right)$, où la famille $(a_i)$ est libre sur $\mathbb{K}$. Alors $D = D'$ et $(a_i)$ et $(b_i)$ sont des bases duales pour la forme bilinéaire $\langle .,.\rangle$.*

*Preuve :* Soit $(b_i)_{i\in\{1,\dots,D''\}}$ la plus grande famille libre extraite de la famille $(b_i)_{i\in\{1,\dots,D'\}}$. Quitte à réordonner les $b_i$, pour tout $i \in \{D'',\dots,D'\}$, il existe des $\alpha_{i,j} \in \mathbb{K}$ non tous nuls tels que $b_j = \sum_{j=1}^{D''} \alpha_{i,j} b_j$. Ainsi

$$\Delta = \sum_{i=1}^{D''} a_i \otimes b_i + \sum_{i=D''}^{D'} a_i \otimes \left(\sum_{j=1}^{D'} \alpha_{i,j} b_j\right) = \sum_{i=1}^{D''} a_i \otimes b_i + \sum_{j=1}^{D''} \alpha_{i,j} \sum_{i=D''}^{D'} a_i \otimes \alpha_{i,j} b_j$$

$$= \sum_{i=1}^{D''} a_i \otimes \left(b_i + \sum_{j=D''}^{D'} b_j\right) = \sum_{i=1}^{D''} a_i \otimes b_i'$$

La famille $\left(b'_j\right)_{j\in\{1,\dots,D''\}}$ est libre et engendre $\mathcal{A}$ car $\overline{\chi}(\Delta)$ est un isomorphisme entre $\widehat{\mathcal{A}}$ et $\mathcal{A}$. Donc c'est une base de $\mathcal{A}$ et finalement $D''=D'=D$ et $(a_i)$ est une autre base de $\mathcal{A}$.

Soit alors $\left(\widehat{b_j}\right)$ la base duale de $(b_j)$. Alors $\overline{\chi}(\Delta)=\sum_{i=1}^{D}\widehat{b_j}(b_i)\,a_i=a_j$ et alors $\langle a_j,b_i\rangle=\overline{\chi}(\Delta)^{-1}(a_j)(b_i)=\widehat{b_j}(b_i)=\delta_{i,j}$. Donc les bases $(a_i)$ et $(b_i)$ sont duales pour $\langle .,.\rangle$. ♣

On obtient ainsi une nouvelle expression de la formule de Cauchy pour le résidu $\tau$ :

$$\forall a\in\mathcal{A}, a=\sum_{i=1}^{D}\langle a,a_i\rangle b_i=\sum_{i=1}^{D}\langle a,b_i\rangle a_i \tag{4.1}$$

La non dégénérescence de cette forme bilinéaire, qui est associée à $\tau$, implique la formule dite de dualité :

$$a\tau=0 \text{ si et seulement si } a=0 \tag{4.2}$$

On associe à la forme bilinéaire associée à $\tau$ la forme quadratique suivante :

$$Q:\left\{\begin{array}{ccc}\mathcal{A}\times\mathcal{A} & \longrightarrow & \mathbb{K}\\ a & \longmapsto & \langle a,a\rangle=\tau\left(a^2\right)\end{array}\right.$$

La matrice de $Q$ dans la base $(b_i)$ est donnée par $\left(\langle b_i,b_j\rangle\right)_{i,j\in\{1,\dots,D\}}$. En utilisant la définition de $\Delta$ et la formule de Cauchy 4.1 on obtient : $\Delta=\sum_{i,j=1}^{D}\langle b_i,b_j\rangle a_i\otimes a_j$.

Cette forme bilinéaire $\langle .,.\rangle$ permet également de relier l'annulateur d'un idéal de $\mathcal{A}$ et l'orthogonal de cet idéal pour cette forme bilinéaire :

**Proposition 4.2.9** *Soit $J$ un idéal de $\mathcal{A}$. Alors l'orthogonal de $J$ pour la forme bilinéaire induite de $\tau$ coïncide avec $Ann_{\mathcal{A}}(J)$.*

*Preuve :* Soit $a\in\mathcal{A}$. Alors par la formule de dualité 4.2, $a\in\mathrm{Ann}_{\mathcal{A}}(J)$ si et seulement si pour tout $g\in J$, $ag=0$ ce qui équivaut à dire que pour tout $g\in J$ et $b\in\mathcal{A}$, $\langle ag,b\rangle=\langle a,gb\rangle=0$. Cela est équivalent à dire que $\forall h\in J$, $\langle a,h\rangle=0$, donc que $a\in\mathrm{Ann}_{\mathcal{A}}(J)$ si et seulement si $a$ appartient à l'orthogonal de $J$. ♣

Soit $\mathcal{I}$ un idéal zéro-dimensionnel de $\mathbb{K}[x_1,\dots,x_n]$, i.e. $\mathcal{A}=\mathbb{K}[x_1,\dots,x_n]/\mathcal{I}$ est un $\mathbb{K}$-espace vectoriel de dimension finie. Notons par $\mathbf{e}_1,\dots,e_d$ les idempotents de $\mathcal{A}$. Par les propositions 2.2.3 et 2.2.9, on a :

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

On a déjà vu que $\widehat{\mathcal{A}} = \widehat{\mathcal{A}}_1 \oplus \cdots \oplus \widehat{\mathcal{A}}_d$ au chapitre précédent. Soit $\Lambda \in \widehat{\mathcal{A}}$, la forme linéaire $\Lambda_i$ qui prend les mêmes valeurs que $\Lambda$ sur $\mathcal{A}_i$ et s'annulant partout ailleurs est donnée par $\Lambda_i = \mathbf{e}_i\Lambda$. On retrouve donc que pour tout élément $\Lambda \in \mathcal{A}$, il existe une écriture de la forme $\Lambda = \sum_{i=1}^{d} \Lambda_i = \sum_{i=1}^{d} \mathbf{e}_i\Lambda_i$.

**Proposition 4.2.10** *Soit $\Delta \in \mathcal{A} \otimes_{\mathbb{K}} \mathcal{A}$, alors $\Delta \in Ann_{\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}}(\mathcal{D})$ si et seulement si $\Delta$ se décompose sous la forme $\Delta = \Delta_1 + \cdots + \Delta_d$ où $\Delta_i = (\mathbf{e}_i \otimes \mathbf{e}_i)\,\Delta \in Ann_{\mathcal{A}_i\otimes_{\mathbb{K}}\mathcal{A}_i}(D_i)$ où $D_i$ désigne le $\mathcal{A}_i$-module de $\mathcal{A}_i \otimes_{\mathbb{K}} \mathcal{A}_i$ engendré par $\{a \otimes 1 - 1 \otimes a | a \in \mathcal{A}_i\}$.*

*Preuve :* Voir [39, 38, 87, 62]. ♣

**Corollaire 4.2.11** *Soit $\Delta = \sum_{i=1}^{d} a_i \otimes b_i \in Ann_{\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}}(\mathcal{D})$avec $(a_i)_{i\in\{1,\ldots,d\}}$ (resp. $(b_i)_{i\in\{1,\ldots,d\}}$) formant une base de $\mathcal{A}$ si et seulement si $\forall j \in \{1,\ldots,d\}$ , $\Delta_j = (\mathbf{e}_j \otimes \mathbf{e}_j)\Delta = \sum_{i=1}^{\mu_i} a_{j,i} \otimes a_{j,i} \in Ann_{\mathcal{A}_j\otimes_{\mathbb{K}}\mathcal{A}_j}(D_j)$ avec $(a_{j,i})_{i\in\{1,\ldots,mu_i\}}$ et $(b_{j,i})_{i\in\{1,\ldots,mu_i\}}$ formant des bases de $\mathcal{A}_j$.*

**Proposition 4.2.12** *Soit $\mathcal{A}$ une $\mathbb{K}$-algèbre et soit $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_d$ sa décomposition en algèbres locales, alors $\mathcal{A}$ est de Gorenstein si et seulement si $\mathcal{A}_i$ est de Gorenstein, $\forall i \in \{1,\ldots,d\}$.*

*Preuve :* Voir [39, 38, 87, 62]. ♣

**Remarque 4.2.13** *Soit $\mathcal{A}$ une algèbre de Gorenstein et soit $\Delta$ un générateur de $Ann_{\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}}(\mathcal{D})$. On a déjà vu que $\Delta^{-1}(1)$ est un générateur de $\widehat{\mathcal{A}}$ comme $\mathcal{A}$-module. Si $\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_d$ est la décomposition de $\mathcal{A}$ en algèbres locales, alors d'après la proposition précédente $\mathcal{A}_i$ est une algèbre de Gorenstein et si $\Delta = \sum_{i=1}^{d} \Delta_i$ est la décomposition correspondante de $\Delta$, alors $\Delta_i$ est un générateur de $Ann_{\mathcal{A}_i\otimes_{\mathbb{K}}\mathcal{A}_i}(D_i)$ et $\tau_i = \Delta_i^{-1}(\mathbf{e}_i) = e_i\Delta^{-1}(1)$ est un générateur de $\widehat{\mathcal{A}}_i$. On a donc $\tau = \sum_{i=1}^{d} \tau_i$. La forme linéaire $\tau$ est appelée résidu global de $\mathcal{A}$ et les $\tau_i$, $i \in \{1,\ldots,d\}$ sont appelés les résidus locaux de $\mathcal{A}$. On verra ultérieurement le lien avec le résidu analytique, mais cette propriété est le pendant algébrique de la définition analytique du résidu.*

### 4.2.4 Lien avec les systèmes inverses à la Macaulay

Nous rappelons ici le formalisme des systèmes inverses tels qu'introduits par Macaulay, puis nous relions ce formalisme à celui que nous avons introduit dans le chapitre 1.

On note $\mathbb{K}[x_1,\ldots,x_n]_d$ l'espace vectoriel des polynômes de $\mathbb{K}[x_1,\ldots,x_n]$ de degré $d$. Soit $T = \mathbb{K}[x_1^{-1},\ldots,x_n^{-1}] \subset \mathbb{K}(x_1,\ldots,x_n)$ l'anneau des polynômes en les variables $x_1^{-1},\ldots,x_n^{-1}$. On munit $T$ d'une structure de $\mathbb{K}[x_1,\ldots,x_n]$-module de la façon suivante : on considère $L \subset \mathbb{K}(x_1,\ldots,x_n)$ comme le sous-espace vectoriel de $\mathbb{K}(x_1,\ldots,x_n)$ engendré par les monômes de la forme $\mathbf{x}^\alpha\mathbf{x}^{-\beta}$, où $\alpha$ et $\beta \in \mathbb{N}^n$, qui ne sont pas dans $T$. L'espace $L$ est alors un sous-$\mathbb{K}[x_1,\ldots,x_n]$-module de $\mathbb{K}[x_1,\ldots,x_n]$. On identifie alors $T$ avec $\mathbb{K}(x_1,\ldots,x_n)/L$ par le morphisme surjectif $T \subset \mathbb{K}(x_1,\ldots,x_n) \to \mathbb{K}(x_1,\ldots,x_n)/L$. De façon plus calculatoire, si $m$ est un monôme de $\mathbb{K}[x_1,\ldots,x_n]$ et $n$ un monôme de $T$, $n.m$ est le monôme $nm$ si $nm \in T$ et 0 sinon. On dispose alors du théorème suivant :

**Théorème 4.2.14** *Avec les notations précédentes, on a une correspondance bijective renversant les inclusions entre les $\mathbb{K}[x_1,\ldots,x_n]$-modules de type fini $M$ de $T$ et les idéaux $\mathcal{I} \subset \mathbb{K}[x_1,\ldots,x_n]$ tels que $\mathcal{I} \subset (x_1,\ldots,x_n)$. Et si $\mathbb{K}[x_1,\ldots,x_n]/\mathcal{I}$ est une algèbre locale de dimension zéro, cette correspondance est donnée par :*

- $M \to \left(0 :_{\mathbb{K}[x_1,\ldots,x_n]} M\right)$*, l'annulateur de $M$ dans $\mathbb{K}[x_1,\ldots,x_n]$,*
- $\mathcal{I} \to (0 :_T \mathcal{I})$*, le sous-module de $T$ annulant $\mathcal{I}$.*

*Si $M$ et $\mathcal{I}$ se correspondent, alors $M \cong Hom_{\mathbb{K}}(\mathbb{K}[x_1,\ldots,x_n]/\mathcal{I},\mathbb{K})$ ; ainsi les anneaux quotients locaux de $\mathbb{K}[x_1,\ldots,x_n]$ qui sont de Gorenstein sont les quotients par les idéaux de la forme $\mathcal{I} = \left(0 :_{\mathbb{K}[x_1,\ldots,x_n]} \tau\right)$ pour un certain $\tau$ dans $T$. L'élément $\tau$ associé de cette manière à un anneau local de dimension zéro $\mathbb{K}[x_1,\ldots,x_n]/\mathcal{I}$ est appelé le résidu local de $\mathbb{K}[x_1,\ldots,x_n]/\mathcal{I}$.*

On se réfère à [35] pour une démonstration de ce théorème qui est une reformulation du théorème 2.3.9, comme nous allons le voir. En effet, ce formalisme est équivalent à celui que nous avons introduit au chapitre 1. Soit $\mathcal{I}$ un idéal de $\mathbb{K}[x_1,\ldots,x_n]$ tel que $\mathcal{A} = \mathbb{K}[x_1,\ldots,x_n]/\mathcal{I}$ soit une algèbre locale de dimension zéro telle que $\mathcal{I}$ définisse uniquement le point 0 dans $\mathbb{K}^n$ (cela implique que $\mathcal{I} \subset (x_1,\ldots,x_n)$). On définit alors un isomorphisme de $\mathcal{A}$-module entre $\mathbb{K}[\partial_1,\ldots,\partial_n]$ et $T$ en associant à tout $\partial^\alpha \in \mathbb{K}[\partial_1,\ldots,\partial_n]$ le monôme $(\alpha!)\mathbf{x}^{-\alpha} \in T$. Il n'est pas très difficile de constater qu'il s'agit d'un isomorphisme. Par cet isomorphisme, on associe à $\mathcal{I}^\perp$ le module $(0 :_T \mathcal{I})$. De façon analogue, si $D \subset \mathbb{K}[\partial_1,\ldots,\partial_n]$ est un sous-espace vectoriel de $\mathbb{K}[\partial_1,\ldots,\partial_n]$ stable par dérivation, alors il lui correspond le sous-module de

$T$ défini par $\left(0 :_T D^{\perp}\right) = \left(0 :_T \left(0 :_{\mathbb{K}[x_1,\ldots,x_n]} D\right)\right)$.

### 4.2.5 Suites régulières, quasi-régulières et théorème de Wiebe

Dans cette section nous introduisons les notions de suites régulières et quasi-régulières ainsi que des résultats les concernant. Nous ne donnerons cependant pas de preuves de ces résultats. Le lecteur pourra se référer à [72] ou [39] pour avoir les preuves et plus de développement sur ce sujet. Notre objectif est uniquement d'énoncer le théorème de Wiebe qui jouera un rôle important dans les calculs effectifs de résidus algébriques. On ne démontrera pas non plus ce dernier résultat.

Soit $A$ un anneau commutatif unitaire.

**Définition 4.2.15** *Une suite $\{a_1, \ldots, a_n\}$ d'éléments de $\mathcal{A}$ est régulière si et seulement si :*

*i) l'idéal $(a_1, \ldots, a_n)$ est propre,*

*ii) $a_i$ n'est pas un diviseur de zéro dans $A$ et pour tout $i \in \{1, \ldots, n\}$, $a_i$ n'est pas un diviseur de zéro dans l'anneau $A/(a_1, \ldots, a_{i-1})$.*

La manipulation des suites régulières n'est pas facile car la propriété de régularité n'est pas stable par permutation des éléments de la suite.

**Rappel 4.2.16** *Le radical de Jacobson d'un anneau $A$, noté $J(A)$, est l'intersection de tous les idéaux maximaux de cet anneau.*

**Lemme 4.2.17 (Lemme de Nakayama)** *Si $M$ est un $A$-module de type fini tel que $J(A)M = M$, alors $M = \{0\}$.*

**Lemme 4.2.18** *Soit $\{a_1, \ldots, a_n\}$ une suite régulière de $A$ contenue dans $J(A)$, alors toute permutation de $\{a_1, \ldots, a_n\}$ est aussi une suite régulière.*

**Corollaire 4.2.19** *Dans un anneau local, toute suite obtenue en permutant les éléments d'une suite régulière est elle aussi régulière.*

**Définition 4.2.20** *Une suite $\{a_1, \ldots, a_n\}$ de $A$ est dite quasi-régulière si et seulement si :*

*i) l'idéal $(a_1, \ldots, a_n)$ est propre,*

*ii) Pour tout idéal maximal $\mathbf{m}$ de $A$ contenant l'idéal $(a_1, \ldots, a_n)$, la suite $\{a_1, \ldots, a_n\}$ est régulière dans $\mathcal{A}_{\mathbf{m}}$.*

**Proposition 4.2.21** *Les polynômes $f_1, \ldots f_n$ de $\mathbb{K}[x_1, \ldots, x_n]$ forment une suite quasi-régulière si et seulement si la variété qu'ils définissent est discrète.*

Le théorème de Wiebe établit le lien entre deux suites quasi-régulières liées par une relation matricielle. Soientt $p_1, \ldots, p_n, q_1, \ldots, q_n$ des éléments de $A$ tels que $\forall i \in \{1, \ldots, n\}$, $q_i = \sum_{i=1}^{n} a_{i,j} f_j$ avec $a_{i,j} \in A$.

On suppose que $\{p_1, \ldots, p_n\}$ et $\{q_1, \ldots, q_n\}$ sont deux suites quasi-régulières. Notons $\Omega = \det\left((a_{i,j})_{i,j \in \{1,\ldots,n\}}\right)$, $P = (p_1, \ldots, p_n)$ et $Q = (q_1, \ldots, q_n)$.

**Théorème 4.2.22 (Théorème de Wiebe)** *:*

1. *La classe de $\Omega$ dans $A$ est indépendante du choix des $a_{i,j}$.*
2. *$Ann_A(\Omega A) = PA$.*
3. *$Ann_A(PA) = \Omega A$.*

*Preuve* : Le lecteur pourra se reporter à [62, 39, 38]. ♣

## 4.3 Bézoutiens

### 4.3.1 Les bézoutiens : introduction

Les bézoutiens ont probablement été introduits par Etienne Bézout et Léonard Euler dans la seconde moitié du XVIIIème siècle. Leurs travaux sur ce sujet avaient pour but d'étendre au cas des systèmes algébriques la théorie de la résolution des systèmes linéaires comme la célèbre élimination de Gauss. A partir de deux équations algébriques univariées $f$ et $g$ de degré respectivement $n$ et $m$ (on suppose $m \geq n$), E. Bézout construit une matrice de taille $m \times m$, appelé matrice bézoutienne par J. J. Sylvester et dont le déterminant est la résultante des deux polynômes $f$ et $g$, c'est-à-dire un polynôme des coefficients de $f$ et $g$ exprimant une condition pour que ces polynômes aient au moins une racine commune (c'est même un peu plus que cela). De nombreuses formulations matricielles pour le calcul de la résultante de deux polynômes ont été introduites par la suite. Mais la matrice bézoutienne présente plusieurs avantages :

- La taille de la matrice est réduite.
- Ultérieurement A. Cayley a remarqué que cette matrice est formée des coefficients du polynôme $\frac{f(x)g(y)-f(y)g(x)}{x-y}$ que nous appellerons polynôme bézoutien de $f$ et $g$, permettant ainsi d'avoir une construction simple de cette matrice. Cette formulation en termes de différences divisées permet également des constructions dans le cas de plusieurs variables que nous exposerons par la suite.

Les matrices bézoutiennes ont d'autres applications que le calcul des résultants univariés ou multivariés, comme nous le verrons dans la section suivante en expliquant ses liens avec les résidus algébriques. Les bézoutiens permettent également de calculer des relations de dépendance algébrique et se révèle être un outil efficace pour l'étude des variétés algébriques "paramétrées". De plus les bézoutiens ont souvent de très bonnes propriétés du point de vue algorithmique et permettent d'établir des bornes intéressantes pour la résolution des systèmes algébriques.

Dans cette section, après avoir rappelé la construction et les propriétés des matrices bézoutiennes dans le cas univarié, nous ferons une étude de ces constructions théoriques dans le cas des systèmes algébriques multivariés.

### 4.3.2 Cas des polynômes d'une variable

Dans toute cette section $f$ et $g$ sont deux polynômes de $\mathbb{K}[x]$ de degré respectif $n$ et $m$. On supposera que $m \geq n$.

**Définition 4.3.1** *Le polynôme bézoutien de $f$ et $g$ est l'élément de $\mathbb{K}[x,y]$ défini par :*

$$\Theta_{f,g}(x,y) = \frac{f(x)\,g(y) - g(x)\,f(x)}{x-y} = \sum_{i=0}^{m-1} \Theta_{f,g,i}(x)\,y^i = \sum_{i,j=0}^{m-1} \Theta_{i,j} x^i y^j$$

*La matrice bézoutienne de $f$ et $g$ est alors définie par $B_{f,g} = (\Theta_{i,j})_{i,j\in\{0,\ldots,m-1\}}$.*

La matrice $B_{f,g}$ est donc une matrice $m\times m$ symétrique (puisque $\Theta_{f,g}(x,y) = \Theta_{f,g}(y,x)$). Les polynômes $\Theta_{f,g,i}$, $i \in \{0,\ldots,m-1\}$, sont des polynômes de degré $m-1$.

Un cas intéressant est celui pour lequel $f = 1$, i.e. $n = 1$. Dans ce cas la matrice bézoutienne a une structure de matrice de Hankel, i.e. $\Theta_{i,j} = \Theta_{i-1,j+1}$. On note $H_{g,i}(x)$ le polynôme $\Theta_{1,g,i}(x)$. On a donc $H_{g,i}(x) = c_{1,m-i} + \cdots + c_{1,m}x^i$. Les polynômes $H_{g,i}$, $i \in \{1,\ldots,m\}$, sont appelés les polynômes de Horner associés à $g$. On a alors $\Theta_{1,g}(x,y) = \sum_{i=1}^{m} H_{g,m-i-1}(x)\,y^i$. De plus les coefficients antidiagonaux de $B_{1,g}$ (i.e. $\Theta_{m-i-1,i-1}$, $i \in \{1,\ldots,m\}$) sont égaux à $c_{1,m}$.

**Proposition 4.3.2** *Soit $\mathcal{A} = \mathbb{K}[x]/(g)$, alors les polynômes de Horner $(H_{g,i})_{i\in\{1,\ldots,m\}}$ forment une base de $\mathcal{A}$.*

*Preuve* : Les polynômes de Horner sont tous de degré différent. Ils forment donc une famille libre de $\mathcal{A}$. De plus comme $\mathrm{Dim}_{\mathbb{K}}(\mathcal{A}) = m$, ils en forment une base. ♣

**Corollaire 4.3.3** *La matrice $B_{1,g}$ est la matrice de passage de la base de Horner dans la base monomiale $\left(x^i\right)_{i\in\{0,\ldots,m-1\}}$ de $\mathcal{A}$. Elle est donc inversible.*

Ces deux résultats simples sont importants car ils permettent d'exprimer la matrice de multiplication par $f$ dans la base monomiale de $\mathcal{A}$ à l'aide des matrices de Bézout.

**Proposition 4.3.4** *La matrice de multiplication par $f$ dans la base monomiale de $\mathcal{A}$ est donnée par :*

$$M_f = B_{f,g}B_{1,g}^{-1}.$$

*Preuve* : On a

$$\Theta_{f,g} = f(x)\,\frac{g(y)-g(x)}{x-y} + g(x)\,\frac{f(x)-f(y)}{x-y}.$$

On a donc $f(x)\,\frac{g(y)-g(x)}{x-y} \equiv \Theta_{f,g}(x,y)$ dans $\mathcal{A}$. Donc on a $\forall i \in \{0,\ldots,m-1\}$, $\Theta_{f,g,i} \equiv f(x)\,\Theta_{1,g,i}$ dans $\mathcal{A}$. Cette dernière égalité signifie que $B_{f,g}$ est la matrice de multiplication par $f$ dans la base de Horner. La formule de la proposition découle directement de cette constatation. ♣

Etant donné le rôle important que jouent les matrices de multiplication dans la résolution des équations et des systèmes d'équations algébriques, on comprend l'importance de l'étude des bézoutiens.

### 4.3.3 Bézoutiens : cas multivarié

La généralisation des bézoutiens dans le cadre multivarié fait apparaître des difficultés supplémentaires. Nous verrons que la définition du bézoutien n'en donne pas de forme canonique. Si on l'exprime dans une base monomiale, son support peut d'ailleurs parfois être beaucoup plus gros qu'une base de l'algèbre quotient. Mais il a de nombreux avantages. C'est un objet très général et qui donne beaucoup d'informations sur le quotient. C'est pourquoi il représente un outil très efficace en géométrie algébrique effective. Il s'agit avant tout d'une formidable machine à fabriquer des relations algébriques. Dans toute cette section on note $R$ l'anneau $\mathbb{K}[x_1,\ldots,x_n]$ quand le contexte est clair, sinon on note $R_{\mathbf{x}}$ l'anneau $\mathbb{K}[x_1,\ldots,x_n]$ et $R_{\mathbf{y}}$ l'anneau $\mathbb{K}[y_1,\ldots,y_n]$.

**Définition des bézoutiens**

On considère $n+1$ polynômes $f_0, \ldots, f_n \in R$ et on note $X_{(0)} = (x_1, \ldots, x_n)$, $X_{(1)} = (y_1, x_2, \ldots, x_n), \ldots, X_{(n)} = (y_1, \ldots, y_n)$. Pour tout $f$ on introduit la i-ème différence divisée de $f \in R_{\mathbf{x}}$ par $\theta_i(f) = \frac{f(X_{(i)}) - f(X_{(i-1)})}{x_i - y_i}$, $\forall i \in \{1, \ldots, n\}$. On considère alors le polynôme suivant :

$$\Phi\left(f_0, f_1, \ldots, f_n\right) = \begin{vmatrix} f_0\left(X_{(0)}\right) & \theta_1\left(f_0\right) & \cdots & \theta_n\left(f_0\right) \\ \vdots & \vdots & & \vdots \\ f_n\left(X_{(0)}\right) & \theta_1\left(f_n\right) & \cdots & \theta_n\left(f_n\right) \end{vmatrix} \tag{4.3}$$

On note $\mathbf{f} = (f_1, \ldots, f_n)$, $\mathcal{I}_{\mathbf{x}}$ (resp. $\mathcal{I}_{\mathbf{y}}$) l'idéal que ces polynômes définissent dans $R_{\mathbf{x}}$ (resp. $R_{\mathbf{y}}$) et $\mathcal{A}_{\mathbf{x}} = R_{\mathbf{x}}/\mathcal{I}_{\mathbf{x}}$ (resp. $\mathcal{A}_{\mathbf{y}} = R_{\mathbf{y}}/\mathcal{I}_{\mathbf{y}}$) le quotient associé. On a alors $R_{\mathbf{x}} \otimes_{\mathbb{K}} R_{\mathbf{y}} = \mathbb{K}[y_1, \ldots, y_n]$ et $\mathcal{A} \otimes_{\mathbb{K}} \mathcal{A} \cong \mathbb{R}_{\mathbf{x}} \otimes_{\mathbb{K}} \mathbb{R}_{\mathbf{y}}/\mathcal{I}_{\mathbf{x}} \otimes_{\mathbb{K}} \mathcal{I}_{\mathbf{y}} = \mathcal{A}_{\mathbf{x}} \otimes_{\mathbb{K}} \mathcal{A}_{\mathbf{y}}$. Généralement, $\Phi(f_0, \mathbf{f}) \in \mathbb{K}[x_1, \ldots, x_n]$ n'est pas directement exprimé dans $\mathcal{A}_x \otimes_{\mathbb{K}} \mathcal{A}_{\mathbf{y}}$.

**Définition 4.3.5** *Soient $\mathbf{a} = (a_i)$ et $\mathbf{b} = (b_i)$ deux bases de $R$. On appelle polynôme bézoutien de $f_0, \mathbf{f}$ relativement aux bases $\mathbf{a}$ et $\mathbf{b}$ et on note $\Phi_{\mathbf{a},\mathbf{b}}\left(f_0, \mathbf{f}\right) = \sum_{i,j} \phi_{i,j} a_i\left(\mathbf{x}\right) b_j\left(\mathbf{y}\right)$. Cette expression a bien sûr un support fini. On appelle matrice bézoutienne de $f_0, \mathbf{f}$ dans les bases $\mathbf{a}$ et $\mathbf{b}$ la matrice $B_{\mathbf{a},\mathbf{b}}\left(f_0, \mathbf{f}\right) = \left(\phi_{i,j}\right)_{i,j}$.*

**Définition 4.3.6** *Si $\mathcal{I}$ est une intersection complète (ce qui implique que $\mathcal{A}$ est de dimension zéro), on considère alors $\mathbf{u} = (u_i)$ et $\mathbf{v} = (v_i)$ deux bases de $\mathcal{A}$. On appelle polynôme bézoutien réduit de $f_0, \mathbf{f}$ et on note $\Theta_{\mathbf{u},\mathbf{v}}\left(f_0, \mathbf{f}\right) = \sum_{i,j} \theta_{i,j} u_i\left(\mathbf{x}\right) \mathbf{v}_i\left(\mathbf{y}\right)$ la forme normale de $\Phi\left(f_0, \mathbf{f}\right)$ relativement aux bases $\mathbf{u}$ et $\mathbf{v}$. De plus, on note $\Delta_{\mathbf{f}}^{\mathbf{u},\mathbf{v}} = \Theta_{\mathbf{u},\mathbf{v}}\left(1, \mathbf{f}\right)$.*

**Définition 4.3.7** *Si $\mathcal{I}$ est une intersection complète et si $\mathbf{u}$ et $\mathbf{v}$ sont deux bases de $\mathcal{A}$, on appelle matrice bézoutienne réduite de $f_0, \mathbf{f}$ la matrice $\overline{B}_{\mathbf{u},\mathbf{v}}\left(f_0, \mathbf{f}\right) = \left(\theta_{i,j}\right)_{i,j}$.*

Dans ce qui suit on s'intéresse à quelques propriétés élémentaires des bézoutiens.

**Propriété 4.3.8** *Pour tout $f_0 \in R$, on a $\Phi\left(f_0, \mathbf{f}\right) \equiv f_0\left(\mathbf{x}\right) \Delta_{\mathbf{f}}[\mathcal{I}_{\mathbf{x}}] \equiv f_0\left(\mathbf{y}\right) \Delta_{\mathbf{f}}[\mathcal{I}_{\mathbf{y}}]$.*

*Preuve :* On développe le déterminant de la définition de $\Phi$ par rapport à la première colonne et on obtient $\Phi(f_0, \mathbf{f}) = f_0\Phi_{1,\mathbf{f}} - f_1\Phi(f_0, 1, \ldots, f_n) + (-1)^n \cdots + f_n\Phi(f_0, f_1, \ldots, 1)$, donc $\Phi(f_0, \mathbf{f}) \equiv f_0(\mathbf{x})\,\Delta_{\mathbf{f}}$. On constate alors que $\forall f_0 \in R$, on a $f_0(X_{(i)}) = f_0(X_{(0)}) + \theta_1(f_0)\,dx_1 + \cdots + \theta_i(f_0)\,dx_i$ où $dx_i = y_i - x_i$, $\forall i \in \{1, \ldots, n\}$. Ainsi on a :

$$\Phi(f_0, f_1, \ldots, f_n) = \begin{vmatrix} f_0(X_{(0)}) & \cdots & \theta_n(f_0) \\ f_1(X_{(0)}) & \cdots & \theta_n(f_1) \\ \vdots & \ddots & \vdots \\ f_n(X_{(0)}) & \cdots & \theta_n(f_n) \end{vmatrix}$$

$$= \frac{\begin{vmatrix} f_0(X_{(0)}) & \cdots & f_0(X_{(0)}) + f_0(X_{(1)})dx_1 + \cdots + f_0(X_{(n)})dx_n \\ \vdots & & \vdots \\ f_n(X_{(0)}) & \cdots & f_0(X_{(0)}) + f_n(X_{(1)})dx_1 + \cdots + f_n(X_{(n)})dx_n \end{vmatrix}}{\prod_{i=1}^{n} dx_i}$$

$$= \frac{\begin{vmatrix} f_0(X_{(0)}) & \cdots & f_0(X_{(n)}) \\ \vdots & & \vdots \\ f_n(X_{(0)}) & \cdots & f_n(X_{(n)}) \end{vmatrix}}{\prod_{i=1}^{n} dx_i}$$

De cette dernière égalité découle directement la deuxième congruence de la propriété. ♣

**Remarque 4.3.9** *La dernière congruence de la preuve de la propriété précédente donne une autre construction du bézoutien. C'est par exemple celle qui est utilisée dans SYNAPS pour le calcul du polynôme bézoutien.*

On obtient facilement la propriété suivante :

**Propriété 4.3.10** *Pour tout $f_0 \in R$, on a $(f_0(\mathbf{x}) - f_0(\mathbf{y}))\,\Delta_{\mathbf{f}} = 0 \in \mathcal{A}_{\mathbf{x}} \otimes_{\mathbb{K}} \mathcal{A}_{\mathbf{y}}$.*

**Rappel 4.3.11** *On rappelle qu'on note $\mathcal{D}$ le sous-$\mathcal{A}$-module de $\mathcal{A} \otimes_{\mathbb{K}} \mathcal{A}$ engendré par les éléments de la forme $a \otimes 1 - 1 \otimes a$, $a \in \mathcal{A}$.*

De la propriété précédente on déduit alors immédiatement la propriété suivante :

**Propriété 4.3.12** $\Delta_{\mathbf{f}} \in Ann_{\mathcal{A}\otimes_{\mathbb{K}}\mathcal{A}}(\mathcal{D})$.

### Liens entre bézoutiens et résidus algébriques

L'ensemble des propriétés précédemment établies permet de donner le lien entre les polynômes bézoutiens et les résidus dans le cadre de l'intersection complète. Nous verrons également que les bézoutiens permettent de calculer les résidus dans ce cadre. On a la proposition suivante :

**Proposition 4.3.13** *Si les polynômes $f_1, \ldots, f_n \in R$ forment une intersection complète, alors $\mathcal{A}$ est une algèbre de Gorenstein et $\overline{\chi}(\Delta_{\mathbf{f}})$ réalise un isomorphisme explicite de $\mathcal{A}$-module entre $\widehat{\mathcal{A}}$ et $\mathcal{A}$.*

*Preuve* : Voir [39, 37, 36]. ♣

Cette proposition nous permet de donner explicitement le lien entre le résidu algébrique et le bézoutien. C'est l'objet du théorème suivant :

**Théorème 4.3.14** *Le résidu algébrique de $\mathbf{f} = (f_1, \ldots, f_n)$ est l'unique forme linéaire $\tau$ de $\widehat{R}$ telle que :*

1. *$\tau$ s'annule sur $\mathcal{I} = (f_1, \ldots, f_n)$,*
2. *$\Delta_{\mathbf{f}}(\tau) = 1\,[\mathcal{I}]$.*

*Preuve* : C'est un corollaire de la proposition précédente et de la caractérisation des algèbres de Gorenstein. ♣

Nous verrons ultérieurement que ce théorème donne une méthode pour calculer les résidus algébriques. Mais nous nous concentrons préalablement sur d'autres propriétés des bézoutiens.

### D'autres propriétés des bézoutiens

**Propriété 4.3.15** *Soient $\mathbf{u}$ et $\mathbf{v}$ deux bases de $R$, la matrice $B_{\mathbf{u},\mathbf{v}}(f_0, \mathbf{f})$ est la matrice de l'application $\mathbb{K}$-linéaire $\overline{\chi}(\Phi(f_0, \mathbf{f}))$ qui à $\Lambda \in \widehat{R}$ associe $\overline{\chi}(\Phi(f_0, \mathbf{f}))(\Lambda) = \sum_{i,j} \phi_{i,j}\Lambda(u_i)v_j$ exprimée de la base $\widehat{\mathbf{u}} = (\widehat{u_i})_i$ de $\widehat{R}$ dans la base $\mathbf{v}$ de $R$.*

Soit $p \in R$, on dénote par $\overline{p}$ la classe de $p$ dans $\mathcal{A}$. On a alors le lemme suivant (Voir [39, 37, 36]) :

**Lemme 4.3.16** *Soient $\mathbf{u} = (u_i)_{i\in\mathbb{N}}$ et $\mathbf{v} = (v_i)_{i\in\mathbb{N}}$ deux bases de $R$ telles que $(\overline{u_i})_{i\in\{1,\ldots,D\}}$ et $(\overline{v_i})_{i\in\{1,\ldots,D\}}$ soient des bases de $\mathcal{A}$, ce qui implique que $u_i$ et*

*$v_i$ sont dans $\mathcal{I}$ pour $i > D$. Alors pour tout $f_0 \in R$, la matrice $B_{\mathbf{u},\mathbf{v}}(f_0, \mathbf{f})$ est de la forme :*

$$\begin{array}{cc} \begin{array}{ccccc} u_1 & \cdots & u_D & u_{D+1} & \cdots \end{array} & \\ \left(\begin{array}{ccccc} & M_{f_0} & & & \\ & & & & \\ & & & L_{f_0} & \end{array}\right) & \begin{array}{c} v_1 \\ \vdots \\ v_D \\ v_{D+1} \\ \vdots \end{array} \end{array}$$

*où $M_{f_0}$ est la matrice de multiplication par $\overline{f_0}$ dans $\mathcal{A}$ dans les bases $(\overline{u_i})_{i\in\{1,\ldots,D\}}$ et $(\overline{v_i})_{i\in\{1,\ldots,D\}}$.*

*Preuve* : Bien que la preuve faite ici ne soit pas nouvelle, nous la reprenons car elle nous servira ultérieurement. Dans un premier temps, nous nous intéressons seulement à obtenir la décomposition par blocs puis nous identifierons les blocs. On suppose que $Z(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_d\}$. On identifie alors $\widehat{\mathcal{A}}$ à $\mathcal{I}^\perp$. On considère les deux sous-espaces $E = \overline{\chi}(\Delta_{\mathbf{f}})(\mathcal{A})$ et $F = \underline{\chi}(\Delta_{\mathbf{f}})(\mathcal{A})$ de $R$. Comme $\dim_{\mathbb{K}}\left(\widehat{\mathcal{A}}\right) = D$, on en déduit que $E$ et $F$ sont deux espaces vectoriels de dimension $D$ puisque $\overline{\chi}(\Delta_{\mathbf{f}})$ et $\underline{\chi}(\Delta_{\mathbf{f}})$ sont des isomorphismes. On sait que $\mathcal{A} = \mathcal{A}_{\zeta_1} \oplus \cdots \oplus \mathcal{A}_{\zeta_d}$ où les $\mathcal{A}_{\zeta_i}$ sont les algèbres locales associées aux $\zeta_i$. On sait que ce sont des intersections complètes définies par $f_1, \ldots, f_n$. Les isomorphismes $\overline{\chi}(\Delta_{\mathbf{f}})$ et $\underline{\chi}(\Delta_{\mathbf{f}})$ induisent des isomorphismes de $\widehat{\mathcal{A}}_{\zeta_i}$ sur $\mathcal{A}_{\zeta_i}$ et on a déjà vu que $\widehat{\mathcal{A}} = \widehat{\mathcal{A}}_{\zeta_1} \oplus \cdots \oplus \widehat{\mathcal{A}}_{\zeta_d}$. On a donc $E$ et $F$ qui sont isomorphes à $\mathcal{A}$, ainsi $R_{\mathbf{x}} = E \oplus \mathcal{I}_{\mathbf{x}}$ et $R_{\mathbf{y}} = F \oplus \mathcal{I}_{\mathbf{y}}$. On en déduit que $\Delta_{\mathbf{f}} \in E \otimes_{\mathbb{K}} F \oplus \mathcal{I}_{\mathbf{x}} \otimes \mathcal{I}_{\mathbf{y}}$ puisque $\Delta_{\mathbf{f}} \in E \otimes_{\mathbb{K}} F \oplus E \otimes \mathcal{I}_{\mathbf{y}} \oplus \mathcal{I}_{\mathbf{x}} \otimes F \oplus \mathcal{I}_{\mathbf{x}} \otimes \mathcal{I}_{\mathbf{y}}$ et que $\overline{\chi}(\Delta_{\mathbf{f}})\left(\mathcal{I}^\perp\right) = E$ et que $\underline{\chi}(\Delta_{\mathbf{f}})\left(\mathcal{I}^\perp\right) = F$.

Soit $f_0 \in R$, on a $\Phi(f_0, \mathbf{f}) - f_0(\mathbf{y})\,\Delta_{\mathbf{f}} \in 1 \times_{\mathbb{K}} \mathcal{I}$. Donc $\overline{\chi}(\Phi(f_0, \mathbf{f}))\left(\widehat{\mathcal{A}}\right) = \overline{\chi}(\Delta_{\mathbf{f}})\left(f_0\widehat{\mathcal{A}}\right) \subset \overline{\chi}\left(\Delta_(\mathbf{f})\right)\left(\widehat{\mathcal{A}}\right) = E$. De même $\underline{\chi}(\Phi(f_0, \mathbf{f}))\left(\widehat{\mathcal{A}}\right) \subset \underline{\chi}(\Delta_{\mathbf{f}})\left(\widehat{\mathcal{A}}\right) = F$ et donc $\Phi(f_0, \mathbf{f}) = E \otimes_{\mathbb{K}} F \oplus \mathcal{I} \otimes_{\mathbb{K}} \mathcal{I}$. Soient $\mathbf{u} = (u_i)_{i\in\mathbb{N}}$ et $\mathbf{v} = (v_i)_{i\in\mathbb{N}}$ deux bases de $R$ telles que $(\overline{u_i})_{i\in\{1,\ldots,D\}}$ et $(\overline{v_i})_{i\in\{1,\ldots,D\}}$ soient des bases respectivement de $E$ et $F$. Ce qui donne la décomposition par blocs de $B_{\mathbf{u},\mathbf{v}}(f_0, \mathbf{f})$ du type de celle du lemme puisqu'on a la décomposition de $\Phi(f_0, \mathbf{f})$ comme élément de $E \otimes_{\mathbb{K}} F$. Nous nous intéressons maintenant à identifier les blocs.

Notons alors $C_{f_0} = (c_{i,j}(f_0))$ le bloc du haut à gauche et $M_{f_0}$ la matrice de la multiplication par $\overline{f_0}$ dans les bases $(\overline{u_i})_{i\in\{1,\ldots,D\}}$ et $(\overline{v_i})_{i\in\{1,\ldots,D\}}$. On déduit de la décomposition de $B_{\mathbf{u},\mathbf{v}}(f_0, \mathbf{f})$ que modulo $1 \otimes \mathcal{I}$, on a :

$$\sum_{i,j \in \{1,\dots,D\}} c_{i,j}(f_0)\overline{u_i} \otimes \overline{v_j} \equiv \Phi(f_0, \mathbf{f}) \equiv f_0(\mathbf{x}) \sum_{i,j \in \{1,\dots,D\}} c_{i,j}(1)\overline{u_i} \otimes \overline{v_j}$$

$$\equiv \sum_{i,j \in \{1,\dots,D\}} c_{i,j}(1) f_0(\mathbf{x})\overline{u_i} \otimes \overline{v_j} \equiv \sum_{k,j \in \{1,\dots,D\}} \left( \sum_{i=1}^{D} m_{k,j} c_{i,j}(1) \right) \overline{u_i} \otimes \overline{v_j}.$$

Ce qui implique que $C_{f_0} = M_{f_0} C_1$. On remarque alors que $C_1$ est inversible puisque c'est la matrice de $\overline{\chi}\Delta_{\mathbf{f}}$. A un changement de base près, on a donc $C_1 = Id$ ce qui achève le démonstration du lemme. ♣

### Complexité du bézoutien

On donne ici des bornes pour la taille de la matrice bézoutienne et la hauteur des coefficients de cette matrice. Ces résultats sont tirés de [38], [36], [37] ou [27]. Soient $d_i = \deg(f_i)$ et $d = \max\{d_i \,|\, i \in \{1, \dots, n\}\}$. Pour tout $\alpha$ et $\beta \in \mathbb{N}^n$, on note par $l_{\alpha,\beta}$ le nombre de tuples $(n_0, \dots, m_n)$ de monômes tels que les $m_i$ soient des monômes apparaissant dans $\Phi(m_0, m_1, \dots, m_n)$. On définit alors $l = \max\left\{ l_{\alpha,\beta \,|\, \alpha \text{ et } \beta \in \mathbb{N}^n} \right\}$. On a alors le lemme suivant :

**Lemme 4.3.17** *Soient $f_0, \dots, f_m \in \mathbf{Q}[\mathbf{x}]$ et soit $\mathbf{h} = max\{h(f_i) \,|\, i \in \{1, \dots, n\}\}$ où $h$ est la fonction de hauteur. Alors la taille de la matrice bézoutienne est bornée par $(en)^n$ et la hauteur des coefficients de $B(f_0, f_1, \dots, f_n)$ est bornée par $(n+1)(h + n\log(d+1) + n\log(n+1)$.*

### Application au calcul de relations algébriques

Cette partie est consacrée à l'utilisation des bézoutiens pour le calcul de relations de dépendance algébrique. C'est une application importante des bézoutiens. Elle joue un rôle important dans des applications comme les calculs des résidus algébriques. On considère $f_0, f_1, \dots, f_n$ des polynômes de $R$ tels que $f_1, \dots, f_n$ sont algébriquement indépendants sur $\mathbb{K}$. Alors, il existe un polynôme $P$ tel que $P(f_0, f_1, \dots, f_n) = 0$. Le but est alors de donner effectivement un tel polynôme.

**Théorème 4.3.18** *Soit $\mathbf{u} = (u_0, \dots, u_n)$ un nouveau vecteur de paramètres et on suppose que $f_1, \dots, f_n$ est une intersection complète, i.e. $\mathcal{A} = R/(f_1, \dots, f_n)$ est un $\mathbb{K}$-espace vectoriel de dimension finie $D$. Alors, tout mineur non nul $P(u_0, \dots, u_n)$ de la matrice bézoutienne des polynômes $f_0 - u_0, f_1 - u_1, \dots, f_n - u_n$ dans $\mathbb{K}[\mathbf{u}][\mathbf{x}]$ satisfait l'identité $P(f_0, f_1, \dots, f_n) = 0$.*

*Preuve :* Voir [39, 37, 38].
♣

**Lemme 4.3.19** *En reprenant les notations du lemme 4.3.17, le polynôme $P$ du théorème 4.3.18 est degré au plus $(ed)^n$ et la hauteur de ses coefficients est au plus $(n+1)\,(ed)^n\,(h+(n+1)\log(d+1)+log(n+1)+2$.*

*Preuve :* Voir [38], [36] ou [37]. ♣

Nous rappelons ici sans preuve un résultat énonçant l'unicité d'un polynôme irréductible tel que $P\,(f_0, f_1, \ldots, f_n) = 0$. Le lecteur pourra se référer à [38], [36] ou [37].

**Proposition 4.3.20** *Soient $f_0, f_1, \ldots, f_n$ des polynômes de $R$ tels que $f_1, \ldots, f_n$ sont $\mathbb{K}$-algébriquement indépendants. Alors il existe un unique polynôme $P \in \mathbb{K}[u_0, u_1, \ldots, u_n]$ irréductible (à multiplication par un scalaire inversible près) tel que $P\,(f_0, f_1, \ldots, f_n) = 0$. Si $\mathbb{K}$ est infini et si $deg(f_0) \leq inf\{deg(f_i)\,|\,i \in \{1, \ldots, n\}\}$, le degré de $P$ est majoré par :*

$$\delta = \frac{deg(f_1)\cdots deg(f_n)}{[\mathbb{K}(\mathbf{x})\ :\ \mathbb{K}(\mathbf{f})]}.$$

*De plus si les polynômes $f_1, \ldots, f_n$ n'ont pas de zéro à l'infini, alors ce degré est exactement $\delta$.*

**Remarque 4.3.21** *Tous les résultats énoncés dans cette partie ne sont en fait que des cas particuliers des résultats énoncés dans [38], [36] ou [37]. En effet, dans ces références les auteurs montrent ces résultats pour le cas des points isolés (qui sont localement intersections complètes) d'un ensemble algébrique de dimension positive. Nous avons volontairement choisi de traiter un cas moins général afin de préserver la simplicité de l'exposé.*

## 4.4 Résidus algébriques

Cette section est consacrée aux résidus algébriques et à leurs liens avec les bézoutiens.

Soient $f_1, \ldots, f_n$ des polynômes de $R$ définissant une intersection complète. On note $\mathcal{I} = (f_1, \ldots, f_n)$ l'idéal qu'ils engendrent, $\mathcal{A} = R/\mathcal{I}$ le quotient et $\mathbf{f}$ le vecteur $(f_1, \ldots, f_n)$. On rappelle la définition du résidu algébrique associé à $f_1, \ldots, f_n$ :

**Définition 4.4.1** *Le résidu $\tau_{\mathbf{f}}$ est l'unique forme linéaire sur $R$ telle que :*

1. $\tau_{\mathbf{f}}(\mathcal{I}) = 0$,
2. $\overline{\chi}(\Delta_{\mathbf{f}})\,(\tau_{\mathbf{f}}) - 1 \in \mathcal{I}$.

Dans le cadre complexe (i.e. $\mathbb{K} = \mathbb{C}$) on dispose d'une définition analytique du résidu :

$$\forall h \in R,\ \tau_{\mathbf{f}}(h) = \sum_{\zeta \in Z(\mathcal{I})} \int_{\partial C_\zeta} \frac{h(\mathbf{x})}{f_1(\mathbf{x}) \cdots f_n(\mathbf{x})} d\mathbf{x}$$

où $C_\zeta$ est un petit polydisque autour de $\zeta$, ne contenant que cette racine, n'ayant pas d'autre racine sur ses frontières, et où $\partial C_\zeta$ est la frontière de ce polydisque.

### Calcul du résidu via une forme normale

Par abus de notation, on notera aussi $\tau_{\mathbf{f}}$ la restriction de $\tau_{\mathbf{f}}$ à $\mathcal{A}$. Pour calculer explicitement $\tau_{\mathbf{f}}$, on peut utiliser le bézoutien. Si on dispose d'une forme normale $N$ dans $\mathcal{A}$ (i.e. d'une projection de $R$ sur une base $\mathbf{b} = (b_i)_{i \in \{1,\ldots,D\}}$ de $\mathcal{A}$), on procède comme suit : cn calcule $\Phi(1, \mathbf{f})$ qu'on réduit en $\mathbf{x}$ et en $\mathbf{y}$. On obtient ainsi $\Theta_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) = \sum_{i,j \in \{1,\ldots,D\}} \theta_{i,j} b_i(\mathbf{x}) b_j(\mathbf{y})$, avec $\theta_{i,j} \in \mathbb{K}$. On considère alors le vecteur $\mathbf{u}$ des coordonnées de la forme normale de 1 dans la base $\mathbf{b}$. On résout alors le système $(\theta_{i,j})_{i,j}\mathbf{t} = \mathbf{u}$ en $\mathbf{t}$. Alors pour tout $h \in \mathcal{A}$, on a $\tau_f(h) = \sum_{i=1}^{D} t_i h_i$.

Un cas particulièrement intéressant est celui où on connaît une forme normale du bézoutien dans une base monomiale. Soit $E = \{\alpha_1, \ldots, \alpha_D\} \subset \mathbb{N}^n$ tel que $\mathbf{x}^E$ soit une base de $\mathcal{A}$. Alors on a $\Theta_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) = \sum_{\alpha,\,\beta \in E} \theta_{\alpha,\beta} \mathbf{x}^\alpha \mathbf{y}^\beta = \sum_{\alpha \in E} \mathbf{x}^\alpha H_\alpha(\mathbf{y})$. La proposition 4.2.8 indique que $(H_\alpha)$ est une base de $\mathcal{A}$, duale de la base $\mathbf{x}^E$ pour le produit scalaire associé à $\tau_{\mathbf{f}}$, i.e. $\tau_{\mathbf{f}}(x^\alpha H_\alpha(y)) = \delta_{\alpha,\beta}$.

**Définition 4.4.2** *La base $(H_\alpha)$ est appelée base de Horner de $\mathcal{A}$.*

Cela reste valable pour d'autres bases que des bases monomiales, mais il est d'usage de définir les polynômes de Horner comme les duaux des monômes d'une base monomiale.

On dispose alors de la formule de Cauchy :

**Proposition 4.4.3** *Soit $E \subset \mathbb{N}^n$ tel que $\mathbf{x}^E$ soit une base monomiale de $\mathcal{A}$. Alors pour tout $f$ dans $\mathcal{A}$, on a :*

$$f = \sum_{\alpha \in E} \tau_{\mathbf{f}}(f H_\alpha) x^\alpha = \sum_{\alpha \in E} \tau_{\mathbf{f}}(f \mathbf{y}^\alpha) H_\alpha(\mathbf{x}).$$

Comme $\Theta_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) = \sum_{\alpha \in E}$, en utilisant la formule de Cauchy, on obtient :

$$\Theta_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) = \sum_{\alpha \in E} \sum_{\beta \in E} \tau_{\mathbf{f}}(H_\alpha H_\beta) \mathbf{y}^\beta \mathbf{x}^\alpha.$$

Cette formule prouve que $\theta_{\alpha,\beta} = \tau_{\mathbf{f}}(H_\alpha H_\beta)$, $\forall \alpha,\ \beta E$. On obtient alors la proposition suivante :

**Proposition 4.4.4** *La matrice du bézoutien réduit dans une base monomiale $\mathbf{x}^E$ de $\mathcal{A}$ est donnée par :*

$$\overline{B}_{\mathbf{f}} = \left(\tau_{\mathbf{f}}(H_\alpha H_\beta)\right)_{\alpha,\,\beta \in E}$$

### Résidu d'une application à variables séparées

On traite ici un cas simple, mais qui joue un rôle important dans les algorithmes de calcul du résidu, comme nous le verrons, puisqu'on se ramène toujours à ce cas-ci en utilisant la loi de transformation. On considère des polynômes $f_1(x_1), \ldots, f_n(x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ avec $f_i(x_i) = f_{i,0} x_i^{d_i} + \cdots + f_{i,d_i}$ avec $f_{i,0} \neq 0$. Le bézoutien de $\mathbf{f} = (f_1, \ldots, f_n)$ est donné par : $\Delta_{\mathbf{f}} = \delta_{f_1} \cdots \Delta_{f_n}$, avec $\Delta_{f_i} = \sum_{j=0}^{d_i - 1} H_{i, d_i - j - 1}(y_i) x_i^j$, où les $H_{i,j}$ sont les polynômes de Horner univariés en la variable $x_i$, $\forall i \in \{1, \ldots, n\}$. On a donc $\Delta_{\mathbf{f}} = \sum_{i=1}^{n} \sum_{j=0}^{d_i - 1} x_1^{j_1} \cdots x_n^{j_n} H_{1, d_i - 1 - j_1}(y_1) \cdots H_{n, d_n - 1 - j_n}$.

Une base monomiale $B$ de $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$ est donnée par :

$$B = \left\{ x_1^{i_1} \cdots x_n^{i_n} \,|\, 0 \leq i_1 < d_1, \ldots, 0 \leq i_n < d_n \right\}.$$

Une autre base de $\mathcal{A}$ est :

$$H = \{ H_{1, d_1 - 1 - i_1}(y_1) \cdots H_{n, d_n - 1 - i_n}(y_n) \,|\, 0 \leq i_1 < d_1, \ldots, 0 \leq i_n < d_n \}.$$

D'après la proposition 4.2.8, ces deux bases sont duales pour le produit scalaire $(a, b) \mapsto \tau_{\mathbf{f}}(ab)$ sur $\mathcal{A}$. Comme $\overline{\chi}(\Delta_{\mathbf{f}})(\tau_{\mathbf{f}}) - 1 \in (f_1, \ldots, f_n)$ et puisque le polynôme bézoutien se décompose uniquement avec des éléments des deux bases précédemment citées de $\mathcal{A}$ (i.e. c'est une forme normale du bézoutien dans ces bases), on en déduit les égalités suivantes :

$$\left\{ \begin{array}{c} \tau_{\mathbf{f}}(\mathbf{x}^{\alpha}) = 0 \text{ si } \mathbf{x}^{\alpha} \in B \setminus \left\{ x_1^{d_1-1} \cdots x_n^{d_n-1} \right\} \\ \tau_{\mathbf{f}}(x_1^{d_1-1} \cdots x_n^{d_n-1}) = \frac{1}{f_{1,0} \cdots f_{n,0}} \end{array} \right.$$

De façon analogue :

$$\left\{ \begin{array}{c} \tau_{\mathbf{f}}(H_{1,i_1} \cdots H_{n,i_n}) = 0 \text{ si } x_1^{i_1} \cdots x_n^{i_n} \in B \setminus \left\{ x_1^{d_1-1} \cdots x_n^{d_n-1} \right\} \\ \tau_{\mathbf{f}}(H_{1,d_1-1} \cdots H_{n,d_n-1} = 1 \end{array} \right.$$

Cela entraîne qu'on peut calculer le résidu en traitant les variables séparément, c'est-à-dire que pour tout $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $\tau_{\mathbf{f}}(\mathbf{x}^{\alpha} = \tau_{f_1}(x_1^{\alpha_1}) \cdots \tau_{f_n}(x_n^{\alpha_n})$. Par linéarité, cela permet de calculer la valeur du résidu pour tout $h \in \mathcal{A}$.

**Remarques 4.4.5**

- *Soit* $h \in \mathbb{K}[x_1, \ldots, x_n]$, *le résidu* $\tau_{(x_1^{d_1}, \ldots, x_n^{d_n})}(h)$ *est le coefficient de* $x_1^{d_1-1} \cdots x_n^{d_n-1}$ *dans* $h$. *C'est un analogue de la formule de Cauchy classique.*
- *On peut aussi voir cette dernière remarque à la lumière de la dualité locale. En effet, si on note* $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/(x_1^{d_1}, \ldots, x_n^{d_n})$, *cette algèbre est locale d'idéal maximal* $(x_1, \ldots, x_n)$. *Alors* $x_1^{d_1-1} \cdots x_n^{d_n-1}$ *est un générateur de Sommet*$(\mathcal{A})$ *(comme* $\mathcal{A}$*-module) et par conséquent son élément dual, qui à* $h \in \mathbb{K}[x_1, \ldots, x_n]$ *associe le coefficient de* $x_1^{d_1-1} \cdots x_n^{d_n-1}$ *dans* $h$ *est un générateur de Socle*$(\widehat{\mathcal{A}})$ *qui est aussi dans ce cas un générateur de* $\widehat{\mathcal{A}}$ *comme* $\mathcal{A}$*-module.*

**Déformation du cas monomial**

C'est le cas le plus facile après le cas des applications polynomiales à variables séparées. On considère une application polynomiale $\mathbf{f} = (f_1, \ldots, f_n)$ où les $f_i$ sont de la forme $f_i(\mathbf{x}) = x_i^{d_i} + g_i(\mathbf{x})$ avec $\deg(g_i) < d_i$, $\forall i \in \{1, \ldots, n\}$. Une base de $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$ est $B = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid 0 \leq \alpha_1 < d_1, \ldots, 0 \leq \alpha_n < d_n\}$. C'est la même base que dans le cas des applications à variables séparées. Pour calculer une forme normale dans cette base, il suffit de remplacer $x_i^{d_i}$ par $g_i(\mathbf{x})$ tant que faire se peut. On note par $\langle B \rangle$ le sous-espace vectoriel de $\mathbb{K}[x_1, \ldots, x_n]$ engendré par les monômes de cette base. La réduction modulo $f_1, \ldots, f_n$ qu'on vient de décrire définit une projection de $\mathbb{K}[x_1, \ldots, x_n]$ sur $\mathcal{A}$ parallèlement à $\mathcal{I} = (f_1, \ldots, f_n)$. On introduit une nouvelle variable $t$ servant à définir les polynômes $f_i^{\#}(t, \mathbf{x}) = x_i^{d_i} + g_i^{\#}(t, \mathbf{x})$ homogénéisés par $t$. On a $f_i^{\#}(0, \mathbf{x}) = x_i^{d_i}$ et $f_i^{\#}(1, \mathbf{x}) = f_i$. Si $\mathbf{f}_t$ désigne $\mathbf{f}_t = (f_1^{\#}, \ldots, f_n^{\#})$, alors :

$$\Delta_{\mathbf{f}_t} = \Delta_{x_1^{d_1}, \ldots, x_n^{d_n}} + tR_1(t, \mathbf{x}, \mathbf{y}) + \ldots + t^s R_s(t, \mathbf{x}, \mathbf{y})$$

où les $R_i$ sont des éléments de $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ de degré au plus $\sum_{i=1}^{n}(d_i - 1) = \nu - 1$. On a alors la proposition suivante :

**Proposition 4.4.6** *Le résidu de $f_1, \ldots, f_n$ est donné par :*
*i) $\tau_{\mathbf{f}} = 0$ sur $\mathcal{I}$,*
*ii) $\tau_{\mathbf{f}} = \tau_{x_1^{d_1} \cdots x_n^{d_n}}$ sur $\langle B \rangle$.*

*Preuve* : La forme linéaire $\tau$ définie dans la proposition est bien définie puisque $\mathbb{K}[x_1, \ldots, x_n] = \langle B \rangle \oplus \mathcal{I}$. Il suffit alors de vérifier que $\overline{\chi}(\Delta_{\mathbf{f}})(\tau) - 1 \in \mathcal{I}$. On a :

$$\overline{\chi}(\Delta_{\mathbf{f}})(\tau) = \overline{\chi}(\Delta_{x_1^{d_1}, \ldots, x_n^{d_n}})(\tau) + \overline{\chi}(R1)(\tau) + \ldots + \overline{\chi}(R_s)(\tau).$$

Comme $\mathbb{K}[x_1, \ldots, x_n] = \langle B \rangle \oplus \mathcal{I}$, $R_j = b_j(\mathbf{x}, \mathbf{y}) + q_j(\mathbf{x}, \mathbf{y})$ avec $b_j(\mathbf{x}, \mathbf{y}) = \sum_{\alpha} a_{j,\alpha}(\mathbf{x}) b_{j,\alpha}(\mathbf{y})$, tels que $a_{j,\alpha}$ et $b_{j,\alpha}$ sont dans $\langle B \rangle$ et de degré inférieur à $\nu$. De plus $q_i \in \mathcal{I} \otimes \mathcal{I}$ sont de degré inférieur à $\nu$. D'après la définition de $\tau$ on a :

$$\begin{aligned}
&\overline{\chi}(\Delta_{\mathbf{f}})(\tau) = \overline{\chi}(\Delta_{x_1^{d_1}, \ldots, x_n^{d_n}})(\tau) + \overline{\chi}(b_1)(\tau) + \ldots + \overline{\chi}(b_s)(\tau) \\
&= \overline{\chi}(\Delta_{x_1^{d_1}, \ldots, x_n^{d_n}})(\tau_{x_1^{d_1}, \ldots, x_n^{d_n}}) + \overline{\chi}(b_1)(\tau_{x_1^{d_1}, \ldots, x_n^{d_n}}) + \ldots + \overline{\chi}(b_s)(\tau_{x_1^{d_1}, \ldots, x_n^{d_n}}) \\
&= 1
\end{aligned}$$

. ♣

### Résidu d'une application simple

**Définition 4.4.7** *Soient $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$, on note $\mathbf{f} = (f_1, \ldots, f_n)$. L'application polynomiale $\mathbf{f}$ est dite simple si $\mathcal{Z} = Z(f_1, \ldots, f_n)$ n'est formé que de racines simples (cela revient à dire que $\forall \zeta \in \mathcal{Z}$, $Jac_{\mathbf{f}}(\zeta) \neq 0$).*

**Proposition 4.4.8** *Si $\mathbf{f}$ est une application polynomiale simple, alors $\tau_{\mathbf{f}} = \sum_{\zeta n \in \mathcal{Z}} \frac{\mathbf{1}_\zeta}{Jac_{\mathbf{f}}(\zeta)}$.*

*Preuve* : Soit $(\zeta,\xi)\in\mathcal{Z}^2$, avec $\zeta\neq\xi$. Comme $\mathbf{f}(\mathbf{x})-\mathbf{f}(\mathbf{y})=\Theta_{\mathbf{f}}(\mathbf{x},\mathbf{y})dx$, on a :

$$\Theta_{\mathbf{f}}(\mathbf{x},\mathbf{y})\begin{pmatrix}\zeta_1-\xi_1\\ \vdots\\ \zeta_n-\xi_n\end{pmatrix}=0$$

et $\Delta_{\mathbf{f}}(\zeta,\xi)=\det(\Theta_{\mathbf{f}}(\zeta,\xi))=0$. De plus si $\zeta\in\mathcal{Z}$, comme cette racine est simple on a $\Delta_{\mathbf{f}}(\zeta,\zeta)=Jac_{\mathbf{f}}(\zeta)\neq 0$. D'autre part, on sait que la famille $(\mathbf{1}_\zeta)_{\zeta\in\mathcal{Z}}$ forme une base de $\widehat{\mathcal{A}}$. Il existe donc des scalaires $(c_\zeta)_{\zeta\in\mathcal{Z}}$ tels que $\tau_{\mathbf{f}}=\sum_{\zeta\in\mathcal{Z}}c_\zeta\mathbf{1}_\zeta$ et comme $\overline{\chi}(\Delta_{\mathbf{f}})(\tau_{\mathbf{f}})-1\in(f_1,\ldots,f_n)$, pour tout $\zeta\in\mathcal{Z}$, on a $\overline{\chi}(\Delta_{\mathbf{f}})(\tau_{\mathbf{f}})-1)(\zeta)=c_\zeta Jac_{\mathbf{f}}(\zeta)-1=0$ et par suite $c_\zeta=\frac{1}{Jac_{\mathbf{f}}(\zeta)}$. ♣

Dans le cas où on connaît une forme normale du bézoutien et où l'application polynomiale est simple, cela permet de retrouver les idempotents de $\mathcal{A}=\mathbb{K}[x_1,\ldots,x_n]/(f_1,\ldots,f_n)$ :

**Proposition 4.4.9** *Soient $f_1,\ldots,f_n\in\mathbb{K}[x_1,\ldots,x_n]$ des polynômes tels que l'application $\mathbf{f}=(f_1,\ldots,f_n)$ soit simple. Soit $E\subset\mathbb{N}^n$ tel que $\mathbf{x}^E$ soit une base monomiale de $\mathcal{A}$. Soit $\Delta_{\mathbf{f}}^E(\mathbf{x},\mathbf{y})$ la forme normale du bézoutien relativement à cette base, alors si $\mathbf{e}_\zeta$ représente l'idempotent de $\mathcal{A}$ associé à $\zeta\in\mathcal{Z}$, on a $\mathbf{e}_\zeta(\mathbf{x})=\frac{1}{Jac_{\mathbf{f}}(\zeta)}\Delta_{\mathbf{f}}^E(x,\zeta)$.*

*Preuve* : Pour tout $h$ dans $\mathcal{A}$, on a $\Delta_{\mathbf{f}}^E(\mathbf{x},\zeta)h(\mathbf{x})\equiv\Delta_{\mathbf{f}}^E(\mathbf{x},\zeta)h(\zeta)$ dans $\mathcal{A}$ et donc :

$$\Delta_{\mathbf{f}}^E(\mathbf{x},\zeta)\Delta_{\mathbf{f}}^E(\mathbf{x},\zeta)\equiv\Delta_{\mathbf{f}}^E(\mathbf{x},\zeta)\Delta_{\mathbf{f}}^E(\zeta,\zeta)\equiv\Delta_{\mathbf{f}}^E(\mathbf{x},\zeta)Jac_{\mathbf{f}}(\zeta)$$

c'est-à-dire $\mathbf{e}_\zeta^2=\mathbf{e}_\zeta$. De plus, si $\xi\in\mathcal{Z}\setminus\{\zeta\}$, on a bien $\Delta_{\mathbf{f}}^E(\xi,\zeta)=0$. Cela caractérise bien les idempotents. ♣

**Remarque 4.4.10** *Les conséquences de cette proposition sont assez étonnantes. En effet, si $E=\{\alpha_1,\ldots,\alpha_d\}$ est tel que $\mathbf{x}^E$ soit une base monomiale de $\mathcal{A}$ et si $\mathcal{Z}=\{\zeta_1,\ldots,\zeta_d\}$, on note $\Delta_{\mathbf{f}}^E(\mathbf{x},\mathbf{y})$ la forme normale du bézoutien dans cette base, alors on a l'identité suivante :*

$$\Delta_{\mathbf{f}}^E(\mathbf{x},\zeta_i)=\sum_{k,l=1}^{d}\theta_{k,l}^E\mathbf{x}^{\alpha_k}\zeta_i^{\alpha_l}=Jac_{\mathbf{f}}(\zeta_i)\begin{vmatrix}\mathbf{x}^{\alpha_1}&\cdots&\mathbf{x}^{\alpha_d}\\ \zeta_1^{\alpha_1}&\cdots&\zeta_1^{\alpha_d}\\ \vdots&&\vdots\\ \zeta_{i-1}^{\alpha_1}&\cdots&\zeta_{i-1}^{\alpha_d}\\ \zeta_{i+1}^{\alpha_1}&\cdots&\zeta_{i+1}^{\alpha_d}\\ \vdots&&\vdots\\ \zeta_d^{\alpha_1}&\cdots&\zeta_d^{\alpha_d}\end{vmatrix}.$$

*Cette identité n'est pas évidente* a priori.

Dans ce qui suit, nous introduisons un outil fondamental pour les calculs des résidus.

### 4.4.1 Lois de transformation

Les lois de transformation donnent le lien entre des applications liées par une transformation matricielle. Ces lois sont la pierre angulaire du calcul effectif des résidus. Nous ne présentons ici deux lois de transformation. Mais il en existe bien d'autres (voir [39] pour un exposé exhaustif, [38]).

#### Loi de transformation usuelle

Soit $\mathbf{f} = (f_1, \ldots, f_n)$ et $\mathbf{g} = (g_1, \ldots, g_n)$ deux applications polynomiales définissant des suites quasi-régulières de $\mathbb{K}[x_1, \ldots, x_n]$. Supposons que $\forall i \in \{1, \ldots, n\}$, $g_i = \sum_{j=1}^{n} a_{i,j} f_j$ avec $a_{i,j} \in \mathbb{K}[x_1, \ldots, x_n]$. Notons $A = (a_{i,j})_{i,j \in \{1,\ldots,n\}}$ et $\tau_{\mathbf{f}}$ (resp. $\tau_{\mathbf{g}}$) le résidu de $\mathbf{f}$ (resp. $\mathbf{g}$).

**Théorème 4.4.11** *Pour tout $h \in \mathbb{K}[x_1, \ldots, x_n]$, on a :*

$$\tau_{\mathbf{f}}(h) = \tau_{\mathbf{g}}(det(A)h).$$

*Preuve* : Voir [39, 36].
♣

On peut trouver d'autres preuves de la loi de transformation basées sur des arguments de perturbation dans [57], [4] et [11]. L'intérêt de cette loi est qu'elle permet de se ramener à des calculs de résidus pour des applications à variables séparées.

On présente ici la loi de transformation généralisée pour les résidus due à C. A. Berenstein et A. Yger [12]. C'est une extension de la loi de transformation généralisée. Nous verrons ultérieurement qu'elle permet de construire un algorithme de calcul des résidus multivariés pour une application quelconque.

**Théorème 4.4.12** *Soient $\mathbf{f} = (f_0, f_1, \ldots, f_n)$ et $\mathbf{g} = (g_0, g_1, \ldots, g_n)$ avec $g_0 = h_0$, deux applications polynomiales (les coordonnées sont dans $\mathbb{K}[x_0, x_1, \ldots, x_n]$ qui définissent des ensembles algébriques discrets. Supposons qu'il existe des entiers $m_i$ positifs et des polynômes $a_{i,j}$ tels que :*

$$\forall i \in \{1, \ldots, n\}, f_0^{m_i} g_i = \sum_{j=1}^{n} a_{i,j} f_j \tag{4.4}$$

*alors* $\tau_{\mathbf{f}} = det(a_{i,j})\tau_{f_0^{m_1+\cdots+m_n+1},g_1,\ldots,g_n}$.

*Preuve :* xVoir [39, 37, 36].
♣
Dans le cas où $m_1 = \cdots = m_n = 0$ et $f_0 = x_0$ on retrouve la loi de transformation usuelle.

### 4.4.2 Résidu et résolution

Soit $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ définissant un ensemble algébrique fini $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_d\}$. On décrit ici un certain nombre d'informations sur la structure de $\mathcal{Z}$ qu'on peut tirer de la connaissance de $\tau_{\mathbf{f}}$.

#### La formule de trace

A chaque élément $a$ de $\mathcal{A}$, on associe l'opérateur de multiplication par $a$ dans $\mathcal{A}$ par $\mathcal{M}_a : b \in \mathcal{A} \to ab \in \mathcal{A}$. On définit alors sur $\mathcal{A}$ un opérateur de trace $Tr$ par $Tr(a) = \text{trace}(\mathcal{M}_a)$, pour tout $a \in \mathcal{A}$. L'application $Tr$ est donc une forme linéaire sur $\mathcal{A}$ et il existe alors un unique $p \in \mathcal{A}$ tel que $Tr = p\tau_{\mathbf{f}}$ puisque $\tau_{\mathbf{f}}$ est un générateur de $\widehat{\mathcal{A}}$ pour sa structure de $\mathcal{A}$-module. La proposition suivante indique que le facteur multiplicatif $p$ est en fait le jacobien de l'application $\mathbf{f}$ :

**Proposition 4.4.13** *On a* $Tr = Jac_{\mathbf{f}}(\mathbf{x})\tau_{\mathbf{f}}$.

*Preuve :* Soit $(a_i)_{i\in\{1,\ldots,D\}}$ et $(b_i)_{i\in\{1,\ldots,D\}}$ deux bases de $\mathcal{A}$ duales pour la forme bilinéaire associée à $\tau_{\mathbf{f}}$, on a alors $\Delta_{\mathbf{f}} = \sum_{i=1}^{D} a_i \otimes b_i$. Comme $\Delta_{\mathbf{f}}(\mathbf{x}, \mathbf{x}) = Jac_{\mathbf{f}}(\mathbf{x})$, on a $Jac_{\mathbf{f}}(\mathbf{x}) = \sum_{i=1}^{D} a_i b_i$. Soit alors $a \in \mathcal{A}$, par la formule de Cauchy, on a $ab_j = \sum_{i=1}^{D} \langle a | a_i b_j \rangle b_i$. Il en résulte que la trace de l'opérateur de multiplication par $a$ dans la base $(b_i)$ est $Tr(a) = \sum_{i=1}^{D} \langle a | a_i b_i \rangle = \sum_{i=1}^{D} \tau_{\mathbf{f}}(a a_i b_i) = \tau_{\mathbf{f}}(a Jac_{\mathbf{f}}) = (Jac_{\mathbf{f}} \tau_f f)(a)$. ♣

**Corollaire 4.4.14** *Si* $\mathbb{K}$ *est un corps de caractéristique zéro, alors* $dim_{\mathbb{K}}\mathcal{A} = \tau_{\mathbf{f}}(Jac_{\mathbf{f}})$.

*Preuve :* On a $\tau_{\mathbf{f}}(Jac_{\mathbf{f}}) = Tr(1) = \mathrm{trace}(Id) = dim_{\mathbb{K}}\mathcal{A}$. ♣

L'opérateur de trace est très lié aux fonctions symétriques des racines. On suppose que $\mathbb{K}$ est de caractéristique nulle et on choisit $i \in \{1, \ldots, n\}$. De ce qui précède on déduit facilement que $\tau_{\mathbf{f}}(Jac_{\mathbf{f}}(\mathbf{x})x_i^j) = Tr(x_i^j) = \sum_{k=1}^{D} \zeta_{k,i}^j$. On note $S_j = Tr(x_i^j)$, qui est appelée somme des puissances $j$ ou $j$-ème somme de Newton. On note $\sigma_k = \sum_{1 \leq j_1 < \cdots < j_k \leq D} \zeta_{j_1} \cdots \zeta_{j_k}$ la $k$-ème fonction symétrique élémentaire. Pour retrouver les fonctions symétriques élémentaires à partir des fonctions symétriques de Newton, on dispose des relations de Newton :

$$\sigma_k = \frac{(-1)^{k-1}}{k}\left(S_k - \sigma_1 S_{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1}S_1\right), k \in \{1, \ldots, D\}.$$

On considère le polynôme $A(T) = T^D - \sigma_1 T^{D-1} + \cdots + (-1)^D \sigma_D$ $= \sum_{j=1}^{D}(T - \zeta_{j,i})$. Le résidu permet donc de calculer les coefficient d'un polynôme univarié dont les racines sont coordonnées d'indice $i$ des racines de l'application $\mathbf{f}$. Mais il est aussi possible de construire une représentation univariée rationnelle à partir de la trace, c'est la démarche proposée dans [84]. Nous utiliserons ultérieurement la démarche consistant à calculer les fonctions symétriques dans un autre cadre.

### Matrices de multiplication

Nous nous intéressons maintenant aux liens qui peuvent exister entre les résidus, les bézoutiens et les matrices de multiplication. Le résidu permet de calculer les opérateurs de multiplication par un polynôme $a \in \mathcal{A}$, mais il permet aussi de donner le lien entre la forme normale du bézoutien dans une base et la matrice de multiplication par $\mathcal{A}$ dans sa base duale base.

Soit $E \subset \mathbb{N}^n$ tel que $\mathbf{x}^E$ soit une base de $\mathcal{A}$. On note $\overline{\Delta}_{\mathbf{f}}(\mathbf{x}, \mathbf{y}) = \sum_{\alpha,\beta \in E} \theta_{\alpha,\beta}\mathbf{x}^\alpha \mathbf{y}^\beta$ la forme normale de $\Delta_{\mathbf{f}}$ dans cette base. Soit $a \in \mathcal{A}$, on note $\overline{B}(a, \mathbf{f})$ la matrice associée à la forme normale de $\Phi(a, \mathbf{f})$ dans cette même base (i.e. dans la base $\mathbf{x}^\alpha \otimes \mathbf{y}^\beta$ de $\mathcal{A} \otimes \mathcal{A}$). On a alors la proposition suivante :

**Proposition 4.4.15** *On a $\overline{B}(a, \mathbf{f}) = (\tau_{\mathbf{f}}(aH_\alpha H_\beta))_{\alpha,\beta \in E}$, où $(H_\alpha)_{\alpha \in E}$ est la base de Horner.*

*Preuve :* On a vu que $p\Delta_{\mathbf{f}} \equiv \Phi(a, \mathbf{f})$ dans $\mathcal{A}$. On a également vu que $\Delta_{\mathbf{f}} = \sum_{\alpha} \mathbf{x}^{\alpha} H_{\alpha}(\mathbf{y})$. On a donc :

$$p\Delta_{\mathbf{f}} \equiv \mathbf{x}^{\alpha}(p(y)H_{\alpha}(\mathbf{y})).$$

D'où en utilisant la formule de Cauchy :

$$\begin{aligned} p\Delta_{\mathbf{f}} &\equiv \sum_{\alpha \in E} \mathbf{x}^{\alpha} \sum_{\beta \in E} \tau_{\mathbf{f}}(pH_{\alpha}H_{\beta})\mathbf{y}^{\beta} \\ &\equiv \sum_{\alpha \in E} \sum_{\beta \in E} \tau_{\mathbf{f}}(pH_{\alpha}H_{\beta})\mathbf{x}^{\alpha}\mathbf{y}^{\beta} \end{aligned}$$

Par définition de la matrice bézoutienne, on $\overline{B}(a, \mathbf{f}) = (\tau_{\mathbf{f}}(aH_{\alpha}H_{\beta}))_{\alpha,\, \beta \in E}$. ♣

On suppose que $E \subset \mathbb{N}^n$ est tel que $\mathbf{x}^E$ est une base de $\mathcal{A}$ et on note $(H_{\alpha})_{\alpha \in E}$ la base de Horner associée. Soit $a \in \mathcal{A}$, alors $a = \tilde{a}_{\alpha} H_{\alpha}(\mathbf{x})$ avec $\tilde{a}_{\alpha} \in \mathbb{K}$, $\forall \alpha \in E$. Cela nous amène à considérer l'opérateur de multiplication $\mathcal{M}_{H_{\alpha}}$ pour étudier l'opérateur de multiplication par $a$ puisque celui-ci est donné par $\mathcal{M}_a = \sum_{\alpha} \tilde{a}_{\alpha} \mathcal{M}_{H_{\alpha}}$. On note $M_{H_{\alpha}}$ la matrice de $\mathcal{M}_{H_{\alpha}}$ dans la base $\mathbf{x}^E$. On a $\mathcal{M}_{H_{\alpha}} = \left(m^{\alpha}_{\beta,\gamma}\right)_{\beta,\, \gamma \in E}$. Comme, par la formule de Cauchy, $H_{\alpha}\mathbf{x}^{\gamma} = \sum_{\beta \in E} \tau_{\mathbf{f}}(H_{\alpha}\mathbf{x}^{\gamma}H_{\beta})\mathbf{x}^{\beta}$, on en déduit que $m^{\alpha}_{\beta,\gamma} = \tau_{\mathbf{f}}(H_{\alpha}\mathbf{x}^{\gamma}H_{\beta})$. D'autre part, on a $\overline{B}(x^{\gamma}, \mathbf{f}) = (\tau_{\mathbf{f}}(x^{\gamma}H_{\alpha}H_{\beta}))_{\alpha,\, \beta \in E}$, on en déduit la proposition suivante :

**Proposition 4.4.16** *Tous les coefficients des matrices de multiplication dans la base de Horner s'écrivent comme combinaisons linéaires de coefficients des bézoutiens réduits dans la base monomiale.*

*Preuve :* Soit $a \in \mathcal{A}$, comme $M_a = \sum_{\alpha \in \mathcal{A}} \tilde{a}_{\alpha} M_{H_{\alpha}}$ et que $M_{H_{\alpha}} = \left(m^{\alpha}_{\beta,\gamma}\right)_{\beta,\, \gamma \in E}$, si on fixe $\beta$ et $\gamma$, le coefficient indexé par $\beta$ et $\gamma$ dans $M_a$ qui s'écrit $\sum_{\alpha_i n E} m^{\alpha}_{\beta,\gamma} = \sum_{\alpha \in E} \tilde{a}_{\alpha} \tau_{\mathbf{f}}(H_{\alpha}\mathbf{x}^{\gamma}H_{\beta}) = \sum_{\alpha \in E} \tilde{a}_{\alpha} \overline{B}(\mathbf{x}^{\gamma}, \mathbf{f})_{\alpha,\beta}$, où $\overline{B}(\mathbf{x}^{\gamma}, \mathbf{f})_{\alpha,\beta}$ désigne le coefficient indexé par $\alpha$ et $\beta$ dans $\overline{B}(\mathbf{x}^{\gamma}, \mathbf{f})$ dans la base $\mathbf{x}^E$. ♣

La proposition suivante explicite un lien important entre les bézoutiens et les opérateurs de multiplication dans l'anneau des coordonnées :

**Proposition 4.4.17** *Soient* $\mathbf{v} = (v_i)_{i\in\{1,\ldots,d\}}$ *et* $\mathbf{u} = (u_i)_{i\in\{1,\ldots,d\}}$ *deux bases de* $\mathcal{A}$*. Soient* $\overline{B}_{\mathbf{u},\mathbf{v}}(1,\mathbf{f})$ *et* $\overline{B}_{\mathbf{u},\mathbf{v}}(x_l,\mathbf{f})$ *les matrices associées aux formes normales de* $\Phi(1,\mathbf{f})$ *et* $\Phi(x_l,\mathbf{f})$ *dans les bases* $\mathbf{u}$ *et* $\mathbf{v}$*,* $\forall l \in \{1,\ldots,n\}$*. Si* $M_{x_l}$ *désigne la matrice de multiplication par* $x_l$ *dans les bases* $\mathbf{u}$ *et* $\mathbf{v}$*, alors on a* $M_{x_l} = \overline{B}_{\mathbf{u},\mathbf{v}}(x_l,\mathbf{f})\overline{B}_{\mathbf{u},\mathbf{v}}(1,\mathbf{f})^{-1}$.

*Preuve* : C'est simplement un corollaire du fait que $\Phi(x_l,\mathbf{f}) \equiv x_l\Phi(1,\mathbf{f})$ dans $\mathcal{A}$ donc que $\overline{B}_{\mathbf{u},\mathbf{v}}(x_l,\mathbf{f}) = M_{x_l}\overline{B}_{\mathbf{u},\mathbf{v}}(1,\mathbf{f})$, la proposition découle directement de cette dernière égalité. ♣

### 4.4.3 Bézoutiens, systèmes inverses, résidus et formes normales

Cette sous-section reprend des résultats exposés dans [27]. On va notamment retrouver de nouveau les systèmes inverses. Un autre point de vu est exposé dans [7] sur le lien entre résidu et bézoutien ainsi que certaines applications ; mais la terminologie diffère entre le point de vu exposé ici et celui de l'article cité. Par exemple les algèbres de Gorenstein y sont appelées algèbres de Kronecker et le résidu y est appelé symbole de Kronecker. Nous avons déjà vu une égalité connue de Kronecker pour les intersections complètes projectives et qui justifie les notations de [7]. Néanmoins, nous avons préféré les notations les plus largement répendues.

#### Bézoutiens, systèmes inverses et résidus locaux

On considère $f_1,\ldots,f_n \in \mathbb{K}[x_1,\ldots,x_n]$, $\mathcal{Z} = Z(f_1,\ldots,f_n)$ l'ensemble algébrique associé qu'on suppose fini (i.e. les $f_i$ forment une intersection complète) et on note $\mathbf{f} = (f_1,\ldots,f_n)$ l'application polynomiale associée. Soit $\zeta \in \mathcal{Z}$, on note alors $\mathcal{A}_\zeta$ l'algèbre locale de $\mathcal{A}$ associée à $\zeta$. Comme $f_1,\ldots,f_n$ forment une intersection complète, ils sont encore en intersection complète dans le localisé en $\zeta$, ce qui implique que $\mathcal{A}_\zeta$ est une algèbre locale de Gorenstein. Son espace dual $\widehat{\mathcal{A}}_\zeta$ est donc un $\mathcal{A}_\zeta$-module libre de rang 1 engendré par le socle de $\widehat{\mathcal{A}}_\zeta$ (et cela même comme $\mathcal{A}$-module).

**Proposition 4.4.18** *Avec les notations et hypothèses précédentes, si* $m_\zeta(\mathbf{x})$ *désigne le générateur du sommet de* $\mathcal{A}_\zeta$*, alors on a* $\tau_\zeta = \langle m_\zeta(\partial), .\rangle_\zeta$ *qui est le générateur du socle de* $\widehat{\mathcal{A}}_\zeta$ *et par conséquent de* $\widehat{\mathcal{A}}_\zeta$*.*

On remarque que comme $(x_l - \zeta_l)$ agit comme $\partial_{\partial_i}$ dans $\widehat{\mathcal{A}}_\zeta$, toutes les autres formes linéaires sont obtenues comme des dérivées par rapport aux variables $\partial_1,\ldots,\partial_n$.

**Proposition 4.4.19** *On suppose que* $\{\zeta_1, \ldots, \zeta_d\}$*. Pour chaque* $i \in \{1, \ldots, d\}$*, on note* $m_i(\mathbf{x})$ *le générateur de* $Sommet(\mathcal{A}_{\zeta_i})$ *on a alors* $\tau_{\mathbf{f}} = \sum_{i=1}^{d} \langle m_i(\partial), .\rangle_{\zeta_i}$*.*

Soit $\Lambda \in \widehat{\mathcal{A}}$, on rappelle que si $p(x,y) = \sum_{\alpha,\, \beta \in \mathbb{N}^n} p_{\alpha,\beta}\mathbf{x}^\alpha \mathbf{y}^\beta$, on note $\overline{\chi}(p)(\Lambda) = \sum_{\alpha,\, \beta \in \mathbb{N}^n} p_{\alpha,\beta}\mathbf{x}^\alpha \Lambda(\mathbf{x}^\beta)$. On dispose alors de la proposition suivante :

**Proposition 4.4.20** *Soit* $\xi = (\xi_1, \ldots, \xi_n) \in \mathcal{Z}$ *et* $l \in \{1, \ldots, n\}$*. L'espace propre de l'opérateur de multiplication par* $x_l$ *associé à la valeur propre* $\xi_l$ *est* $\overline{\chi}(\Delta_{\mathbf{f}})(\widehat{\mathcal{A}}_\xi)$*.*

*Preuve* : Soit $\Lambda \in \widehat{\mathcal{A}}_\xi = Q_\xi^\perp$ où $Q_\xi$ est la composante $\mathbf{m}_\xi$-primaire de $\mathcal{I}$. On a alors $\overline{\chi}(\Phi(x_l, \mathbf{f}))(\Lambda) = \xi_l \overline{\chi}(\Phi(1,\mathbf{f}))(\Lambda) + \overline{\chi}(\Phi(1,\mathbf{f}))(\partial_{\partial_l}\Lambda)$, comme $\partial_{\partial_l}\Lambda \in \widehat{\mathcal{A}}_\xi$, on en déduit que $\overline{B}(x_l,\mathbf{f})\overline{B}(1,\mathbf{f})^{-1}\overline{B}(1,\mathbf{f})\Lambda = \xi_l \overline{\chi}(\Phi(1,\mathbf{f}))(\Lambda) + \overline{\chi}(\Phi(1,\mathbf{f}))(\partial_{\partial_l}\Lambda)$. Comme $\overline{B}(x_l,\mathbf{f})\overline{B}(1,\mathbf{f})^{-1} = M_{x_l}$, on a $(M_{x_l} - \zeta_l Id)\,(\overline{B}(1,\mathbf{f})\Lambda) = \overline{B}(1,\mathbf{f})(\partial_{\partial_l}\Lambda)$, on en tire que $\overline{B}(1,\mathbf{f})\left(\widehat{\mathcal{A}}_{\zeta_i}\right)$ est inclus dans l'espace propre de $M_{x_l}$. De plus comme ces espaces ont la même dimension, ils sont égaux. ♣

Le théorème suivant raffine la proposition que nous venons de démontrer :

**Théorème 4.4.21** *Les espaces de Jordan des opérateurs de multiplication par* $x_l$ *pour les valeurs propres* $\xi_l$ *sont les images par* $\overline{\chi}(\Delta_{\mathbf{f}})$ *du résidu* $\tau_{\xi_l}$ *et de ses dérivées* $\partial^i_{\partial_l}$*,* $i \in \{1, \ldots, \mu_\xi\}$*, où* $\mu_\xi$ *est la multiplicité de* $\xi$*.*

*Preuve* : Soit $\tau_\xi(\partial)$ le résidu local associé à $\xi$, alors les polynômes différentiels $\tau_\xi, \partial_{\partial_k}\tau_\xi, \ldots, \partial^k_{\partial_l}\tau_\xi$ sont indépendants, pour $k$ tel que $\partial^{k+1}_{\partial_k}\tau_\xi = 0$. On a $\overline{\chi}(\mathbf{x}_l\Delta_{\mathbf{f}})(\Lambda) = \zeta_l\overline{\chi}(\Delta)(\lambda) + \overline{\chi}(\Delta_{\mathbf{f}})(\partial_{\partial_l}\Lambda)$, $\forall \lambda \in \widehat{\mathcal{A}}_\xi$. Ainsi la matrice de multiplication par $x_l$, restreinte à l'espace vectoriel engendré par $\tau_\xi, \partial_{\partial_k}\tau_\xi, \ldots, \partial^k_{\partial_l}\tau_\xi$, et dans cette base, s'écrit :

$$\begin{pmatrix} \zeta_l & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \ddots & 1 \\ 0 & \cdots & \cdots & \zeta_l \end{pmatrix}.$$

Réciproquement, si une matrice, dans chacun des facteurs locaux, peut être décomposée sous cette forme dans un sous-espace engendré par le résidu local et ses dérivées par rapport à une des variables différentielles, alors il s'agit d'une matrice de multiplication par rapport à la variable de même indice que la variable différentielle par rapport à laquelle on dérive dans chacun des locaux. ♣

## 4.5 Calcul des résidus

Le but de cette section est d'exposer l'algorithme de calcul des résidus dû à M. Elkadi et B. Mourrain, qui permet de calculer les résidus pour des intersections complètes. Nous ne reprenons pas les applications proposées originalement dans [38]. Nous proposons comme application un travail que nous avons mené en commun avec ces deux auteurs, qui concerne l'implicitisation des surfaces rationnelles.

### 4.5.1 Algorithme de calcul des résidus dans un cas simple

On expose ici un algorithme de calcul de résidus pour un cas simple mais néanmoins assez général. La condition de validité est donnée dans la proposition suivante :

**Proposition 4.5.1** *Soient $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ des polynômes définissant un ensemble algébrique de dimension zéro. Soit $\mathbf{u} = (u_0, \ldots, u_n)$ un vecteur des nouvelles variables. Pour tout $i_i n \{1, \ldots, n\}$ on note $P_i(u_0, \ldots, u_n)$ le polynôme calculé à partir d'un mineur maximal de $B(x_i - u_0, f_1 - u_1, \ldots, f_n - u_n)$ qui est bien une relation de dépendance algébrique (voir le théorème 4.3.18). On a :*

$$P_i(u_0, u_1, \ldots, u_n) = a_{i,0} u_0^{m_i} + \cdots + a_{i,m_i}, \forall i \in \{1, \ldots, n\}.$$

*Si pour chaque $i \in \{1, \ldots, n\}$, il existe $j_i \in \{0, \ldots, m_i\}$ tel que $a_{i,j_i}(0) \neq 0$, alors pour tout $h \in \mathbb{K}[x_1, \ldots, x_n]$ le calcul du résidu $\tau_{\mathbf{f}}(h)$ se ramène à un calcul de résidu à variables séparées.*

*Preuve :* Pour tout $i \in \{1, \ldots, n\}$, soit $j_i = \min\{k | a_{i,k} \neq 0\}$. On a :

$$\begin{aligned} g_i(x_i) &= a_{i,j_i}(0) x_i^{m_i - j_i} + \cdots + a_{i,m_i} \\ &= \sum_{j=1}^{n} A_{i,j}(\mathbf{x}) f_j \text{ avec } A_{i,j} \in \mathbb{K}[x_1, \ldots, x_n]. \end{aligned}$$

Si on pose $\mathbf{g}(\mathbf{x}) = (g_1(\mathbf{x}_1), \ldots, g_n(x_n))$, en utilisant la loi de transformation usuelle, on a :

$$\tau_{\mathbf{f}}(h) = \tau_{\mathbf{g}}\left(\det\left(A_{i,j}\right) h\right)$$

qui se ramène facilement à un calcul de résidu à variables séparées. ♣

Cela nous conduit à l'algorithme suivant :

**Algorithme 4.5.2**

*Entrée :* *L'application polynomiale* $\mathbf{f} = (f_1, \ldots, f_n)$ *et le polynôme* $h \in \mathbb{K}[x_1, \ldots, x_n]$ *dont on veut calculer le résidu.*

- *Pour* $i$ *allant de* 1 *à* $n$*, calculer un mineur maximal* $P_i(u_0, \ldots, u_n)$ *du bézoutien* $B(x_i - u_0, f_1 - u_1, \ldots, f_n - u_n)$ *en utilisant l'algorithme de Bareiss par exemple.*
- *Pour* $i$ *allant de* 1 *à* $n$ *calculer* $g_i(x_i) = P_i(x_i, 0, \ldots, 0)$.
- *Calcul de la matrice de transformation :*
  *Pour* $i$ *allant de* 1 *de* 1 *à* $n$ *faire*
  - $A_{i,0} = P_i(u_0, 0, \ldots, 0) - P_i(0, 0, \ldots, 0)$
  - $A_{i,1} = A_{i,0}(u_1, 0, \ldots, 0)/u_1$
  - $A_{i,2} = (A_{i,0} - u_1 * A_{i,1})(u_2, 0, \ldots, 0)/u_2$
  - $A_{i,3} = (A_{i,0} - u_1 * A_{i,1} - u_2 * A_{i,2})(u_3, 0, \ldots, 0)/u_3$
  - ...
  - $A_{i,n} = (A_{i,0} - u_1 * A_{i,1} - \cdots - u_{n-1}A_{i,n-1})(u_n)/u_n$

  *Fin du faire.*
- *On récupère la matrice* $A = (A_{i,j}(x_i, f_1, \ldots, f_n))_{i,j \in \{1,\ldots,n\}}$.
- *On calcule* $c$ *qui est le produit des coefficients dominants des* $g_i$.
- $Res = h * det(A)/c$
- *Pour* $i$ *allant de* 1 *à* $n$*, Res reçoit le reste de la division euclidienne de Res par* $g_i$.

*Sortie :* *La valeur de Res.*

**Remarque 4.5.3** *En pratique, pour diminuer la complexité de cet algorithme, on réalise les procédés d'élimination sur les matrices spécialisées, on récupère alors avec une bonne probabilité de succès les indices de lignes et de colonnes d'un mineur maximal, et c'est seulement ce mineur qu'on calcule. Les divisions euclidiennes sont effectuées à partir d'un algorithme de division basé sur un algorithme de Newton (voir [97]).*

Il reste à traiter le cas où tous les $a_{i,j}(0) = 0$. Dans ce cas, une solution existe, utilisant la loi de transformation généralisée. C'est l'objet de ce qui suit.

### 4.5.2 Algorithme de calcul des résidus multivariés

Cet algorithme repose sur la loi de transformation généralisée et sur la génération de relations de dépendance algébrique par le bézoutien qui permet de se ramener à des systèmes à variables séparées.

Soient $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ des polynômes définissant un ensemble algébrique $\mathcal{Z} = \mathcal{Z}(f_1, \ldots, f_n)$ de dimension zéro. On note $\mathbf{f} = (f_1, \ldots, f_n)$ l'application polynomiale associée. Pour tout $i \in \{1, \ldots, n\}$, $A_1(u_0, u_1, \ldots, u_n)$ désigne une relation de dépendance algébrique entre $x_i, f_1, \ldots, f_n$.

Posons $Q_i(\mathbf{u}; x_i) = A_i(x_i, u_1, \ldots, u_n) = \displaystyle\sum_{j=1}^{n} a_{i,j}(\mathbf{u}, \mathbf{f}, x_i)(f_j - u_i)$. Soit $\xi = (\xi_1, \ldots, \xi_n) \in \mathbb{K}^n$ un vecteur générique. On définit un multi-indice $m = (m_1, \ldots, m_n)$ et des applications $\mathbf{R} = (R_1, \ldots, R_n)$ et $\mathbf{S} = (S_1, \ldots, S_n)$ de la façon suivante : si $t$ est une nouvelle variable, pour tout $i_in \{1, \ldots, n\}$, on note

$$Q_i(t\xi_1, \ldots, t\xi_n; x_i) = t^{m_i}\left(R_1(x_i) - tS_i(t, x_i)\right).$$

On dispose alors du théorème suivant :

**Théorème 4.5.4** *Avec les hypothèses précédentes et pour tout* $h \in \mathbb{K}[x_1, \ldots, x_n]$, *si on note* $D = det\big((a_{i,j}(t\xi_1, \ldots, t\xi_n, x_i))_{i,\, j \in \{1,\ldots,n\}}\big)$, *alors :*

$$\begin{aligned}\tau_{\mathbf{f}}(h) &= \tau_{(t^{|m|+1}, R_1(x_1) - tS_1(x_1), \ldots, R_n(x_n) - tS_n(x_n))}(Dh)\\ &= \sum_{k \in \mathbb{N}^n, |k| \leq |m|} \tau_{(t^{|m|+1}, R_1(x_1)^{k_1+1}, \ldots, R_n(x_n)^{k_n+1})}\left(hDS_1^{k_1}\cdots S_n^{k_n}\right)\end{aligned}$$

*Preuve* : La loi de transformation généralisée appliquée aux applications $(t, f_1 - t\xi_1, \ldots, f_n - t\xi_n)$ et $(t, R_1 - tS_1, \ldots, R_n - tS_n)$ fournit

$$\tau_{(t, f_1 - t\xi_1, \ldots, f_n - t\xi_n)}(h) = \tau_{(t^{|m|+1}, R_1 - tS_1, \ldots, R_n - tS_n)}(Dh) \tag{4.5}$$

Puis la loi de transformation usuelle appliquée aux identités

$$R_i^{|m|+1} - (tS_i)^{|m|+1} = (R_i - tS_i)\sum_{k_i=0}^{|m|} R_i^{|m|+k_i}(tS_i)^{k_i}$$

implique que le second membre de 4.5 est égal à

$$\begin{aligned}&\tau_{(t^{|m|+1}, R_1^{|m|+1}, \ldots, R_n^{|m|+1})}(hD\prod_{j=1}^{n}\sum_{k_j=0}^{|m|}(tS_i)^{k_j}R_i^{|m|-k_j})\\ =& \sum_{k \in \mathbb{N}^n, |k| \leq |m|} \tau_{(t^{|m|+1}, R_1(x_1)^{k_1+1}, \ldots, R_n(x_n)^{k_n+1})}\left(hDS_1^{k_1}\cdots S_n^{k_n}\right).\end{aligned}$$

Le théorème découle alors de l'égalité

$$\tau\mathbf{f}(h) = \tau_{(t, f_1, \ldots, f_n)}(h) = \tau_{(t, f_1 - t\xi_1, \ldots, f_n - t\xi_n)}$$

et de ce qui précède. ♣

Cela nous conduit à l'algorithme suivant :

**Algorithme 4.5.5**

<u>Entrée</u> : *L'application polynomiale* $\mathbf{f} = (f_1, \ldots, f_n)$ *et le polynôme* $h \in \mathbb{K}[x_1, \ldots, x_n]$ *dont on veut calculer le résidu.*

- *Pour* $i$ *allant de* $1$ *à* $n$, *on calcule les relations de dépendance algébrique entre* $x_i, f_1, \ldots, f_n$ *par le biais d'un mineur maximal de* $B(x_i - u_0, f_1 - u_1, \ldots, f_n - u_n)$.
- *On choisit un vecteur* $(\mathbf{x}_1, \ldots, \xi_n)$ *de* $\mathbb{K}^n$ *générique et on détermine les entiers* $m_i$, *les polynômes* $R_i$ *et* $S_i$ *et le déterminant* $D = det(a_{i,j}(t\xi_1, \ldots, t\xi_n, \mathbf{f}, x_i))$ *donné dans 4.5.*
- *Pour chaque* $k = (k_1, \ldots, k_n) \in \mathbb{N}^n$ *tel que* $|k| \leq |m|$, *on calcule le coefficient* $c_{k,0}(x_1, \ldots, x_n)$ *de* $t^{|m|-|k|}$ *dans* $hDS_1^{k_1} \cdots S_n^{k_n}$, *et par induction le coefficient* $c_{k,i}(x_{i+1}, \ldots, x_n)$ *de* $x_i^{(k_i+1)deg(R_i)-1}$ *dans la division euclidienne de* $c_{k,i-1}(x_i, \ldots, x_n)$ *par* $R_i^{k_i+1}(x_i)$, *pour* $i_in \{1, \ldots, n\}$.

<u>Sortie</u> : $\tau_{\mathbf{f}}(h) = \sum_{k \in \mathbb{N}^n, |k| \leq |m|} c_{k,n}$.

### 4.5.3 Application à l'implicitisation

On donne maintenant une application du calcul du bézoutien à l'implicitisation des surfaces rationnelles. On se restreint au cas des surfaces paramétrées dans $\mathbb{K}^3$, bien que cet algorithme s'adapte pour toutes les hypersurfaces paramétrées de $\mathbb{K}^n$. Nous commençons par rappeler le problème de l'implicitisation, puis nous montrons comment le résidu donne une solution à ce problème.

Une surface rationnelle de $\mathbb{K}^3$ est donnée soit par sa représentation paramétrique :

$$(S) : \begin{cases} x = f_1(s,t)/f_4(s,t) \\ y = f_2(s,t)/f_4(s,t) \\ z = f_3(s,t)/f_4(s,t) \end{cases}$$

où $f_1, f_2, f_3$ et $f_4 \in \mathbb{K}[s,t]$, soit par une équation implicite (i.e. un polynôme $P \in \mathbb{K}[x,y,z]$ de degré minimal satisfaisant $P(x,y,z) = 0$ pour tout $(x,y,z) \in S$). Ces deux représentations sont importantes. En effet, la représentation paramétrique permet de donner facilement des points de la surface tandis que l'équation implicite permet de calculer plus facilement des intersections avec d'autres objets géométriques, ce qui est important pour des applications comme le lancer de rayon (ray-tracing).

Le problème de l'implicitisation consiste à trouver l'équation implicite d'une surface rationnelle donnée par sa représentation paramétrique.

Plusieurs approches ont été proposées pour traiter ce problème, mais beaucoup d'entre elles échouent en présence de points de base (i.e. $\mathcal{Z}(f_1, f_2, f_3, f_4) \neq \emptyset$). Les différentes approches peuvent être classées comme suit :

- Les approches par résultants : ces méthodes sont très efficaces, mais elles échouent généralement en présence de points de base. Une solution a été proposée dans [71], basée sur des techniques de perturbation, mais elle a une très grande complexité en pratique. Une autre solution, basée sur la notion de résultant résiduel, a été proposée dans [21], mais il y a des conditions sur la géométrie des points de base. Une nouvelle méthode, proposée dans [3], traite efficacement le cas sans point de base, mais une éventuelle extension au cas des points de base n'est pas encore connue.
- Les approches par les bézoutiens : cette méthode est très générale, mais elle donne généralement un multiple de l'équation implicite et nécessite donc une factorisation qui peut s'avérer coûteuse. Des variantes, basées sur des calculs de résidu ont été proposées dans [55] et [54]. Ces algorithmes ne sont cependant pas assez généraux. L'algorithme proposé ici est une extension de ces idées.
- Les approches par les bases de Gröbner : c'est une solution qui a été très étudiée et qui est présentée dans [59] par exemple. Une approche un peu trop naïve des bases de Gröbner est très coûteuse en pratique, et ce, même pour des problèmes de petits degrés. En collaboration avec P. Trébuchet, nous avons proposé une méthode générale, basée sur des changements d'ordres, du calcul modulaire et de l'interpolation multivariée. Cette méthode traite le cas des points de base. C'est une extension du travail initié par Sandra Liccardi et Teo Mora dans [68].
- L'approche par surfaces mobiles : c'est une approche prometteuse et qui fonctionne bien sans point de base. Récemment, sa validité dans le cas de certains points de base a été démontrée. Voir [32] et [31].
- L'approche numérique : c'est une approche efficace, voir [34], mais elle introduit d'autres problèmes comme la certification et la robustesse.

Nous proposons ici une méthode basée sur des calculs de résidus. Ce travail a été effectué en collaboration avec Mohamed Elkadi et Bernard Mourrain.

**Théorie des idéaux et implicitisation**

Soit une surface rationnelle donnée par sa représentation paramétrique :

$$(S) : \begin{cases} x = f_1(s,t)/f_4(s,t) \\ y = f_2(s,t)/f_4(s,t) \\ z = f_3(s,t)/f_4(s,t) \end{cases}$$

On cherche une relation de dépendance algébrique minimale entre $x, y$ et $z$. On note $H_1(x,s,t) = f_4(s,t)x - f_1(s,t)$, $H_2(y,s,t) = f_4(s,t)y - f_2(s,t)$, $H_3(z,s,t) = f_4(s,t)z - f_3(s,t)$. L'approche classique, quand il n'y a pas de point de base, consiste à considérer l'idéal $\mathcal{I} = (H_1, H_2, H_3) \subset \mathbb{K}[x,y,z,s,t]$ et à éliminer $s$ et $t$ pour trouver un générateur de $\mathcal{I} \cap \mathbb{K}[x,y,z]$. Mais auparavant, on explique pourquoi un tel générateur existe. On considère l'application rationnelle $\Psi$ de $\mathbb{K}^2$ dans $\mathbb{K}^3$ définie par $(s,t) \mapsto (\frac{f_1(s,t)}{f_4(s,t)}, \frac{f_2(s,t)}{f_4(s,t)}, \frac{f_3(s,t)}{f_4(s,t)})$. Puisqu'il n'y a pas de point de base, l'image de la restriction de $\Psi$ à $\mathbb{K}^2 \setminus \mathcal{Z}(f_4)$ est une variété algébrique $S$ de codimension 1 (i.e. c'est une surface dans $\mathbb{K}^3$). On considère alors l'application $\Phi : \mathbb{K}^2 \to \mathbb{K}^5$ définie par $(s,t) \mapsto (\frac{f_1(s,t)}{f_4(s,t)}, \frac{f_2(s,t)}{f_4(s,t)}, \frac{f_3(s,t)}{f_4(s,t)}, s, t)$. L'image de $\Phi$ est une variété algébrique $Y$ (quelquefois appelée graphe de $\Psi$). On voit facilement que $Y = \mathcal{Z}(\mathcal{I})$. On note $\Lambda : \mathbb{K}^5 \to \mathbb{K}^3$ la projection $(x,y,z,s,t) \mapsto (x,y,z)$. La clôture de Zariski de l'image de $Y$ par $\Lambda$ est $S$. Ainsi l'idéal associé à $S$ est $\mathcal{I} \cap \mathbb{K}[x,y,z]$ qui est principal puisqu'il est de codimension 1. Le générateur (défini à un scalaire près) est donc la relation algébrique cherchée entre $x, y$ et $z$, c'est-à-dire que c'est l'équation implicite de $S$.

Quand il y a des points de base, la situation est un peu plus compliquée. En effet, comme $\mathcal{Z}(f_1, f_2, f_3, f_4) \neq \emptyset$, on considère $(s,t) \in \mathcal{Z}(f_1, f_2, f_3, f_4)$. Alors, pour tout $(x,y,z) \in \mathbb{K}^3$ on a $H_1(x,s,t) = 0$, $H_2(y,s,t) = 0$ et $H_3(z,s,t) = 0$. Donc $\mathcal{I} \cap \mathbb{K}[x,y,z] = \mathbb{K}[x,y,z]$ qui définit l'ensemble algébrique vide. Cela se traduit aussi par le fait que l'image de l'application rationnelle $\Psi$ n'est pas un morphisme de variétés algébriques. Pour contourner cette difficulté, on ne regarde que les points pour lesquels $f_4$ ne s'annule pas. Algébriquement cela revient à localiser par rapport à $(f_4)$ (on se réfère au premier chapitre de [35]). Pour ce faire, on considère l'idéal $\tilde{\mathcal{I}} = (H_1, H_2, H_3, H_4) \subset \mathbb{K}[x,y,z,w,s,t]$ où $H_1$, $H_2$ et $H_3$ sont les mêmes polynômes que dans la section précédente et $H_4(w,s,t) = f_4(s,t)w - 1$. On considère alors l'application rationnelle $\Omega : \mathbb{K}^2 \to \mathbb{K}^6$ définie par $(s,t) \mapsto (\frac{f_1(s,t)}{f_4(s,t)}, \frac{f_2(s,t)}{f_4(s,t)}, \frac{f_3(s,t)}{f_4(s,t)}, \frac{1}{f_4(s,t)}, s, t)$ qui définit un ensemble $U$ dans $\mathbb{K}^6$. On note alors $\overline{U}$ la clôture de Zariski de $U$. Il est facile de constater que $\overline{U} = \mathcal{Z}(\tilde{\mathcal{I}})$. On considère la projection $\Theta : \mathbb{K}^6 \to \mathbb{K}^3$ définie par

$(x, y, z, w, s, t) \mapsto (x, y, z)$. La clôture de Zariski de la projection de $\overline{U}$ est $\overline{\Theta(\overline{U})} = S$, qui est associée à l'idéal $\tilde{\mathcal{I}} \cap \mathbb{K}[x, y, z]$. Puisque cet idéal est de codimension 1, pour les mêmes raisons que précédemment, il est principal.

### Un cas simple

On se place ici dans un cas simple où on peut directement utiliser un calcul de résidu pour calculer l'équation implicite. On considère une surface rationnelle donnée par une représentation paramétrique :

$$\begin{cases} x = f_1(s,t)/f_4(s,t) \\ y = f_2(s,t)/f_4(s,t) \\ z = f_3(s,t)/f_4(s,t) \end{cases}$$

telle que $f_1$ et $f_4$ n'ont pas de zéro commun. Cela implique que la paramétrisation est sans point de base. On suppose qu'un des numérateurs n'a pas de zéro en commun avec le dénominateur et on se ramène au cas traité ici par renommage de $x, y$ et $z$ et renumérotation des équations. Nous allons voir dans ce cas qu'un calcul de résidu permettait de trouver l'équation implicite de la surface $S$. On note $H_1(s,t) = f_4(s,t)x - f_1(s,t)$, $H_2(s,t) = f_4(s,t)y - f_2(s,t)$ et $H_3(s,t) = f_4(s,t)z - f_3(s,t)$. On note $\mathcal{Z} = \Big\{(s,t) \in \overline{\mathbb{K}(y,z)}^2 \mid H_2(s,t) = H_3(s,t) = 0\Big\}$. Si $\mathcal{Z}$ est un ensemble fini on considère l'élément de $\mathbb{K}(y,z)[x]$ suivant :

$$\begin{aligned} P(x,y,z) &= \prod_{(s,t)\in\mathcal{Z}} H_1(s,t) \\ &= \left(\prod_{(s,t)\in\mathcal{Z}} f_4(s,t)\right)\left(\prod_{(s,t)\in\mathcal{Z}}\left(x - \frac{f_1(s,t)}{f_4(s,t)}\right)\right) \\ &= \left(\prod_{(s,t)\in\mathcal{Z}} f_4(s,t)\right)\left(x^m - \sigma_1(y,z)x^{m-1} + \cdots + \sigma_m(y,z)\right) \end{aligned} \tag{4.6}$$

où $\sigma_i(y,z) = \sigma_i(\frac{f_1(s,t)}{f_4(s,t)} \mid (s,t) \in \mathcal{Z})$ est la $i$-ème fonction symétrique élémentaire de l'ensemble $\left\{\frac{f_1(s,t)}{f_4(s,t)} \mid (s,t) \in \mathcal{Z}\right\}$.

Si on ne sait pas calculer les fonctions symétriques élémentaires *a priori*, on a vu que le résidu permet de calculer les sommes de Newton. En effet, si on note $S_i(y,z) = \sum_{(s,t)\in\mathcal{Z}} \left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i$, on a :

$$S_i(y,z) = \tau_{(H_2,H_3)}\left(Jac_{(H_2,H_3)}(s,t)\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i\right). \tag{4.7}$$

Si on sait calculer les résidus $\tau_{(H_2,H_3)}\left(Jac_{(H_2,H_3)}(s,t)\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i\right)$, pour tout $i \in \{1,\ldots,m\}$, alors on saura calculer les fonctions symétriques élémentaires grâce aux relations de Newton, et par suite on sera en mesure de calculer l'équation implicite à partir de 4.6.

**Remarque 4.5.6** *Le degré de l'équation $P$ est donné par* $m = \tau_{(H_2,H_3)}\left(Jac_{(H_2,H_3)}(s,t)\right)$.

**Théorème 4.5.7** *L'équation implicite de la surface $S$ est donnée par la partie sans carré du numérateur de* $\frac{P(x,y,z)}{\prod_{(s,t)\in\mathcal{Z}} f_4(s,t)} \in \mathbb{K}(y,z)[x]$.

Cela nous conduit donc à l'algorithme suivant dans le cas où $f_1$ et $f_4$ n'ont pas de zéro commun et où la loi de transformation usuelle suffit (sinon il faut utiliser la loi de transformation généralisée) :

**Algorithme 4.5.8**

*<u>Entrée</u> : Les polynômes $f_1, f_2, f_3$ et $f_4$.*
*Etape 1 : On se ramène au cas des variables séparées.*

- *On calcule $H_2(s,t) = f_4(s,t)y - f_2(s,t)$ et $H_3(s,t) = f_4(s,t)z - f_3(s,t)$.*
- *On calcule une relation de dépendance algébrique $A_s$ entre $s, H_2$ et $H_3$ (cela peut se faire par le calcul d'un mineur maximal d'un bézoutien par exemple). De la même façon on calcule une relation de dépendance algébrique $A_t$ entre $t, H_2$ et $H_3$.*
- *On calcule le déterminant $D$ de la matrice $T$ telle que $T\begin{pmatrix} A_s \\ A_t \end{pmatrix} = \begin{pmatrix} H_2 \\ H_3 \end{pmatrix}$.*
- *On calcule le jacobien de $\begin{pmatrix} H_2 \\ H_3 \end{pmatrix}$ par rapport aux variables $s$ et $t$.*
- *Soit $a$ le coefficient du monôme de plus haut degré (noté $d_s$) en $s$ de $A_s$ et $b$ celui de plus haut degré (noté $d_t$) en $t$ de $A_t$. On note $d = ab$.*

*Etape 2 :* *Calcul du résidu.*

- *On calcule le coefficient de $s^{d_s}t^{d_t}$ dans le reste des divisions euclidiennes successives de $DJac_{(H_2,H_3)}$ par $A_s$ puis $A_t$ qu'on divise par d. On obtient ainsi l'entier m.*
- *Pour i allant de 1 à m faire :*
  *On calcule le coefficient de $s^{d_s}t^{d_t}$ dans le reste des divisions euclidiennes successives de $DJac_{(H_2,H_3)}\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i$ par $A_s$ puis $A_t$ qu'on divise par d. On obtient ainsi $S_i(y,z)$, la i-ème somme de Newton.*

– *Etape 3 :* *Calcul des fonctions symétriques élémentaires.*
*Utiliser les relations de Newton pour calculer les fonctions symétriques élémentaires $\sigma_i(y,z)$ à partir des sommes de Newton $S_i(y,z)$.*

– *Sortie : Retourner la partie sans carré de $P(x,y,z) = x^m+\sigma_1(y,z)x^{m-1}+\cdots+\sigma_m(y,z)$.*

### Cas général

On traite maintenant le cas où la paramétrisation peut avoir des points de base (i.e. $\mathcal{Z}(f_1,f_2,f_3,f_4) \neq \emptyset$ dans $\overline{\mathbb{K}}^3$). On utilise comme nous l'avons suggéré précédemment le procédé de localisation consistant à rendre le dénominateur inversible. On considère l'application suivante :

$$\left\{\begin{array}{c} H_1(s,t) = f_4(s,t)x - f_1(s,t) \\ H_2(s,t) = f_4(s,t)y - f_2(s,t) \\ H_3(s,t,w) = f_4(s,t)w - 1 \end{array}\right.$$

On note $\mathcal{Z} = \left\{(s,t,w) \in \overline{\mathbb{K}(y,z)}^3 \mid H_2(s,t) = H_3(s,t) = H_4(s,t,w) = 0\right\}$ et $X = \left\{(s,t) \in \overline{\mathbb{K}(y,z)}^2 \mid H_2(s,t) = H_3(s,t) = 0\right\}$. On a $X = X_1 \cup X_2$ où $X_1 = X \cap Z(f_4)$ et $X_2 = X \setminus X_1$. On définit la projection suivante :

$$\Pi : \left\{\begin{array}{ccc} \overline{\mathbb{K}(y,z)}^3 & \longrightarrow & \overline{\mathbb{K}(y,z)}^2 \\ (s,t,w) & \longmapsto & (s,t) \end{array}\right.$$

On dispose alors de la proposition suivante :

**Proposition 4.5.9** *On a $\Pi(\mathcal{Z}) = X_2$.*

*Preuve* : On remarque que $H_2$ et $H_3$ sont indépendants de $w$. Si $(s,t,w) \in \mathcal{Z}$ alors $H_2(s,t) = H_3(s,t) = 0$ et $f_4(s,t) \neq 0$. Donc $\Pi(\mathcal{Z}) \subset X_2$. Réciproquement, si $(s,t) \in X_2$, alors $f_4(s,t) \neq 0$, donc $(s,t,\frac{1}{f_4(s,t)}) \in \mathcal{Z}$ et par suite $\Pi(s,t,\frac{1}{f_4(s,t)}) = (s,t) \in X_2$ et finalement $\Pi(\mathcal{Z}) = X_2$. ♣

Clairement l'ensemble des points de base est inclus dans $X_1$. On note $X_0'$ l'ensemble des points de base, on note $X_1 = X_0' \cup X_1'$ avec $X_1' = X_1 \setminus X_0'$.

Si $X_2$ est un ensemble fini, on peut appliquer la même méthodologie que dans le cas simple. On considère $P(x,y,z) \in \mathbb{K}(y,z)[x]$ défini par :

$$\begin{aligned} P(x,y,z) &= \prod_{(s,t)\in X_2} H_1(s,t) \\ &= \left( \prod_{(s,t)\in X_2} f_4(s,t) \right) \left( x^m + \sigma_1(y,z)x^{m-1} + \cdots + \sigma_m(y,z) \right) \end{aligned}$$

où $\sigma_i(y,z)$ désigne la $i$-ème fonction symétrique élémentaire de l'ensemble $\left\{ \frac{f_1(s,t)}{f_4(s,t)} \,|\, (s,t) \in X_2 \right\}$, $\forall i \in \{1,\ldots,m\}$.

Comme nous l'avons fait précédemment, on peut utiliser les formules de Newton pour calculer les fonctions symétriques élémentaires à partir des sommes de Newton qui sont données par :

$$\begin{aligned} S_i(y,z) &= \sum_{(s,t)\in X_2} \left( \frac{f_1(s,t)}{f_4(s,t)} \right)^i \\ &= \tau_{(H_2,H_3)\setminus(f_4)} \left( Jac_{(H_2,H_3}(s,t) \left( \frac{f_1(s,t)}{f_4(s,t)} \right)^i \right) \end{aligned}$$

où $\tau_{(H_2,H_3)\setminus(f_4)}$ désigne la somme des résidus locaux aux points de $X_2$.

On remarque qu'il n'y a plus de problème avec les points de base puisqu'ils sont inclus dans $X_1$.

Le théorème suivant nous fournit un moyen de calculer les sommes de Newton :

**Théorème 4.5.10** *On a :*

$$\begin{gathered} \tau_{(H_2,H_3)\setminus(f_4)} \left( Jac_{(H_2,H_3)}(s,t) \left( \tfrac{f_1(s,t)}{f_4(s,t)} \right)^i \right) \\ = \\ \tau_{(H_2,H_3,H_4)} \left( Jac_{(H_2,H_3,H_4)}(s,t,w) \left( \tfrac{f_1(s,t)}{f_4(s,t)} \right)^i \right) \end{gathered} \tag{4.8}$$

*Preuve :* L'idée est de décomposer en termes de résidus locaux. On a :

$$\tau_{(H_2,H_3)\backslash(f_4)}\left(Jac_{(H_2,H_3)}(s,t)\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i\right)$$
$$=$$
$$\sum_{(s,t)\in X_2}\frac{Jac_{(H_2,H_3)}(s,t)\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i}{Jac_{(H_2,H_3)}(s,t)}\quad .$$
$$=$$
$$\sum_{(s,t)\in X_2}\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i$$

D'autre part, on a :

$$\tau_{(H_2,H_3,H_4)}\left(Jac_{(H_2,H_3,H_4)}(s,t,w)\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i\right)$$
$$=$$
$$\sum_{(s,t,w)\in\mathcal{Z}}\frac{Jac_{(H_2,H_3,H_4)}(s,t,w)\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i}{Jac_{(H_2,H_3,H_4)}(s,t,w)}\quad .$$
$$=$$
$$\sum_{(s,t,w)\in\mathcal{Z}}\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i$$

Or $\sum_{(s,t)\in X_2}\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i = \sum_{(s,t,w)\in\mathcal{Z}}\left(\frac{f_1(s,t)}{f_4(s,t)}\right)^i$ puisque $\Pi(\mathcal{Z}) = X_2$ et le théorème est prouvé. ♣

En corollaire on a :

**Corollaire 4.5.11** *L'équation implicite de la surface $S$ est la partie sans carré du numérateur de* $\frac{P(x,y,z)}{\prod_{(s,t)} f_4(s,t)} \in \mathbb{K}(y,z)[X]$.

*Preuve :* Ce résultat découle directement de ce que $S = Z(\tilde{\mathcal{I}} \cap \mathbb{K}[x,y,z])$ et de ce que nous calculons le polynôme caractéristique de $x$ dans $\mathbb{K}[x,y,z]/(\tilde{\mathcal{I}} \cap \mathbb{K}[x,y,z])$. ♣

### Exemple

Nous présentons ici un exemple très simple de calcul d'équation implicite pour une surface dont la parametrisation présente un point de base. Cet exemple est simple dans le sens où il ne demande l'utilisation que de la loi de transformation usuelle. Les équations paramétriques de la surface sont :

$$\begin{cases} x = h1(s,t)/h_0(s,t) = \frac{s+t}{st} \\ y = h_2(s,t)/h_0(s,t) = \frac{s^2+t^2}{st} \\ z = h_3(s,t)/h_0(s,t) = \frac{s-t}{st} \end{cases}$$

La trace est alors $\sigma_0 = S_0 = 2$. Ce qui nous permet de savoir que l'équation implicite est de degré 2. Les sommes de Newton calculées sont :

$$S_1 = 0$$
$$S_2 = \frac{2*(y+2)*z^2}{y-2}$$

En utilisant les relations de Newton on obtient les fonctions symétriques :

$$\sigma_1 = 0$$
$$\sigma_2 = \frac{-(y+2)*z^2}{y-2}$$

Ce qui donne comme numérateur de $x^2 - \sigma_1 x + \sigma_2$ l'équation implicite $P(x,y,z) = x^2 * y - 2 * x^2 - z^2 * y - 2 * z^2$, qui est bien l'équation cherchée.

## 4.6 Application du bézoutien à l'implicitisation de surfaces rationnelles

Dans cette section nous exposons une application des matrices bézoutiennes à l'implicitisation. Il est connu qu'un mineur maximal d'une matrice bézoutienne convenable donnent un multiple de l'équation implicite d'une hypersurface rationnelle donnée par une représentation paramétrique. C'est un cas particulier des techniques de résultants résiduels introduites par L. Busé, M. Elkadi et B. Mourrain dans [22] dans le cadre des variétés unirationnelles. Nous nous limiterons au cas des hypersurfaces rationnelles données par des représentations paramétriques. On considère l'hypersurface suivante :

$$S : \begin{cases} x_1 = f_1(\mathbf{t})/f_0(\mathbf{t}) \\ \vdots \\ x_n = f_n(\mathbf{t})/f_0(\mathbf{t}) \end{cases}$$

où $f_0, f_1, \ldots, f_n \in \mathbb{K}[\mathbf{t}] = \mathbb{K}[t_1, \ldots, t_{n-1}]$. On définit $h_i(\mathbf{t}) = f_0(\mathbf{t})x_i - f_i(\mathbf{t})$, $\forall i \in \{1, \ldots, n\}$. Ce sont des polynômes de $\mathbb{K}[\mathbf{x}][\mathbf{t}]$. Remarquons alors que ces polynômes définissent un ensemble algébrique dans $\mathbb{K}^{n-1} \times \mathbb{K}^n$ que

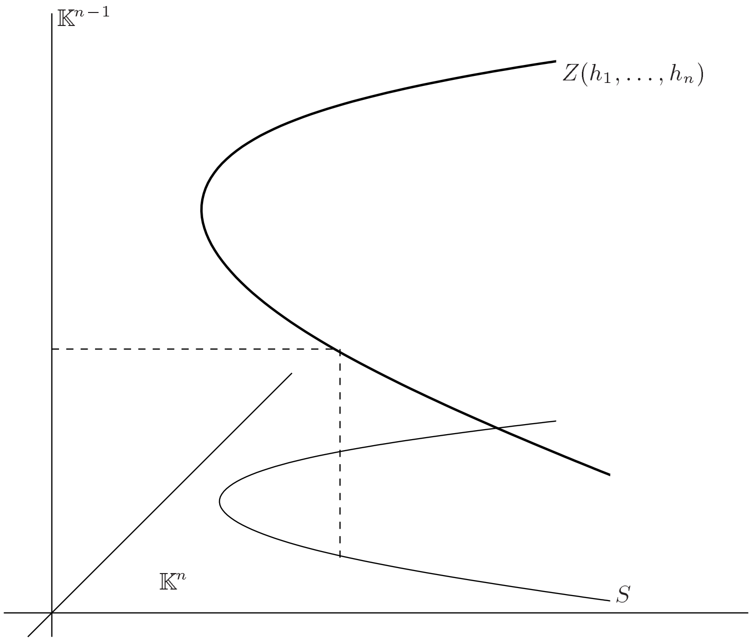


FIG. 4.1 – Graphe de $S$.

nous appellerons graphe de $S$ (bien que ce soit en réalité le graphe de l'application rationnelle $(f_1/f_0,\ldots,f_n/f_0)$).

On note $\mathcal{I}$ l'idéal $(h_2,\ldots,h_n)$ et $B_{h_1}=B(h_1,\ldots,h_n)$. Pour tout $\mathbf{z}\in\mathbb{K}^n$, on note $H_{i,\mathbf{z}}(\mathbf{t})=f_0(\mathbf{t})z_i-f_i(\mathbf{t})$, $\forall i\in\{1,\ldots,n\}$ et $H_{\mathbf{z}}(\mathbf{t})=(H_{2,\mathbf{z}},\ldots,H_{n,\mathbf{z}})$. On note alors $B_{h_1}(\mathbf{z})$ la matrice $B_{h_1}$ dont on a spécialisé les variables $x_i$ avec les valeurs $z_i$, $\forall i\in\{1,\ldots,n\}$. Pour tout $\mathbf{z}\in\mathbb{K}^n$, $H_{\mathbf{z}}$ définit un idéal $(H_{\mathbf{z}})$ dans $\mathbb{K}[\mathbf{t}]$, on note alors $\mathcal{A}_{\mathbf{z}}=\mathbb{K}[\mathbf{t}]/(H_{\mathbf{z}})$. On note $X_{\mathbf{z}}=Z((H_{\mathbf{z}}))=\left\{\mathbf{t}\in\mathbb{K}^{n-1}\mid H_{2,\mathbf{z}}(\mathbf{t})=\cdots=H_{n,\mathbf{z}}(\mathbf{t})=0\right\}$. On a alors la proposition suivante :

**Proposition 4.6.1** *Tout mineur maximal non nul de $B_{h_1}$ est un multiple de l'équation implicite de $S$.*

*Preuve* : On sait que pour $\mathbf{z}$ pris dans un ouvert dense de $\mathbb{K}^n$, la dimension de $\mathcal{A}_{\mathbf{z}}$ est constante. On note $D_g$ cette dimension. Alors pour presque tout $\mathbf{z}$, on a $X_{\mathbf{z}}=\left\{\zeta_1(\mathbf{z}),\ldots,\zeta_{D_g}(\mathbf{z})\right\}$. On considère alors $\mathcal{M}_{H_{1,\mathbf{z}}}$, l'opérateur de multiplication par $H_{1,\mathbf{z}}$ dans $\mathcal{A}_{\mathbf{z}}$. Les valeurs propres de cet opérateur sont $H_{1,\mathbf{z}}(\zeta(\mathbf{z}))$, pour $\zeta\in X_f$. Le rang de cette application est constant pour $\mathbf{z}$ pris dans un ouvert dense de $\mathbb{K}^n$ puisqu'il est égal à $D_g$ moins le nombre de racine commune de $H_{1,\mathbf{z}}$ avec $H_{2,\mathbf{z}},\ldots,H_{n,\mathbf{z}}$ et que génériquement $H_{1,\mathbf{z}}$ n'a pas de racines communes avec $H_{2,\mathbf{z}}, \ldots, H_{n,\mathbf{z}}$ en dehors des points de base de la paramétrisation. Le rang générique de cette application, noté $R_g$, est donc égal à $D_g$ moins le nombre de points de base. De plus ce rang chute si et seulement si $H_{1,\mathbf{z}}$ a une racine commune avec $H_{2,\mathbf{z}}, \ldots, H_{n,\mathbf{z}}$, ce qui signifie que le point $\mathbf{z}$ est un point de la surface $S$.

On sait que pour $\mathbf{z}$ pris dans un ouvert dense de $\mathbb{K}^n$, le rang de la matrice $B_{h_1}(\mathbf{z})$ est constant et égale au rang de $B_{h_1}$. On note $r_g$ ce rang générique. D'après la proposition 4.3.16, on sait que pour tout $\mathbf{z} \in \mathbb{K}^n$, la matrice $B_{h_1}(\mathbf{z})$ se décompose de façon çe que :

$$\operatorname{rang}(B_{h_1}(\mathbf{z})) = \operatorname{rang}(\mathcal{M}_{H_{1,\mathbf{z}}}) + \operatorname{rang}(L_{H_{1,\mathbf{z}}}).$$

Soit $\mathbf{z}$ tel que $H_{1,\mathbf{z}}$ ait une racine commune avec $H_{2,\mathbf{z}}, \ldots, H_{n,\mathbf{z}}$ en dehors des points de base. Alors $\operatorname{rang}(\mathcal{M}_{H_{1,\mathbf{z}}}) < R_g$ et le rang de $L_{H_{1,z}}$ ne peut excéder son rang générique. Donc, tout mineur $r_g \times r_g$ de $B_{h_1}(\mathbf{z})$ est nul. Ainsi tous les mineurs maximaux $r_g \times r_g$ de $B_{h_1}$ s'annulent pour des valeurs de $\mathbf{z}$ prises sur l'hypersurface $S$ et par conséquent sont des multiples de l'équation implicite de $S$. ♣

Ce résultat peut être obtenu comme conséquence d'un énoncé de [22].

# Chapitre 5

# Matrices structurées et dualité

## 5.1 Introduction

Les matrices structurées sont au cœur de beaucoup de branches des mathématiques et de l'informatique. En allant du calcul scientifique jusqu'à la combinatoire en passant par l'interpolation rationnelle, aussi bien qu'en traitement du signal, en théorie des files d'attente et jusqu'à la théorie des automates. Elles rendent compte de structures pour lesquelles seule une partie des coefficients de la matrice code de l'information nouvelle. Ainsi les matrices creuses sont celles qui ont peu de coefficients non nuls et pour lesquelles il est préférable de ne stocker que les coefficients non nuls. En calcul scientifique, les schémas de discrétisation conduisent souvent à des matrices structurées de type Toeplitz ou Hankel qui trouvent une interprétation naturelle comme application sur des espaces de polynômes univariés et qui permettent d'obtenir des algorithmes rapides de multiplication d'une matrice par un vecteur ou de résolution de systèmes linéaires. D'autres structures ont été exploitées dans ce cadre et sont l'objet d'une branche importante de l'algèbre linéaire : l'algèbre linéaire structurée. Comme c'est souvent par des interprétations en termes d'algèbre linéaire sur des espaces de polynômes qu'on abouti à des algorithmes efficaces pour manipuler des matrices structurées, il n'y a rien d'étonnant à ce qu'on retrouve ces notions dans des algorithmes de résolution d'équations algébriques.

Nous donnons un exemple de conception d'algorithme de multiplication rapide par une matrice de Toeplitz. Une matrice $M = (m_{i,j})$ telle que $m_{i,j} = m_{i+1,j+1}$ est dite de Toeplitz. C'est-à-dire que c'est une matrice de la forme :

$$\begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & \cdots & m_{1,n} \\ m_{2,1} & m_{1,1} & \ddots & & \vdots \\ m_{3,1} & m_{2,1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & m_{1,2} \\ m_{n,1} & & m_{3,1} & m_{2,1} & m_{1,1} \end{pmatrix}$$

On remarque alors que toute l'information nécessaire pour coder cette matrice est contenue dans la première ligne et la première colonne. On considère l'espace $\mathbb{K}[x]$ des polynômes de la variable $x$. On considère alors le polynôme $P_m(x) = \sum_{i=1}^{n} m_{1,i} x^{n-i} + \sum_{i=1} m_{i,1} x^{i+n-1}$. La matrice de multiplication par $P_m(x)$ dans $\mathbb{K}[x]$ muni de la base monomiale est alors de la forme suivante :

$$\begin{array}{c} \\ 1 \\ \vdots \\ x^n \\ \vdots \\ x^{2n} \\ \vdots \\ \\ \\ \end{array} \begin{pmatrix} \ddots & \vdots & \vdots & \vdots & \vdots \\ \cdots & m_{1,n} & & 0 & \cdots \\ \cdots & \vdots & \ddots & & \cdots \\ \cdots & m_{1,1} & & m_{1,n} & \cdots \\ \cdots & \vdots & \ddots & \vdots & \cdots \\ \cdots & m_{n,1} & & m_{1,1} & \cdots \\ \cdots & & \cdots & \vdots & \cdots \\ \cdots & 0 & & m_{n,1} & \cdots \\ \cdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Ainsi une matrice de Toeplitz $n \times n$ peut-elle toujours être interprétée comme la matrice de multiplication par un vecteur dans $\mathbb{K}[x]$. On note par $\mathcal{M}_{P_m}$ l'application linéaire de multiplication par $P_m$ dans $\mathbb{K}[x]$. On définit $E = \langle 1, \ldots, x^d \rangle$, $F = \langle x^d, \ldots, x^{2n} \rangle$ et $\Pi_E$ (resp. $\Pi_F$) la projection de $\mathbb{K}[x]$ dans $E$ (resp. $F$). Ainsi $M$ est la matrice de l'application linéaire suivante :

$$T_m = \Pi_F \circ \mathcal{M}_{P_m} \circ \Pi_E$$

Ainsi la multiplication d'une matrice Toeplitz par un vecteur peut se ramener à la multiplication de deux polynômes. Cela conduit à un algorithme de plus basse complexité que la multiplication classique d'une matrice par un polynôme. On peut dès lors comprendre l'intérêt de l'exploitation de ces structures dans le cadre de la résolution des équations algébriques.

De la même façon, une matrice de Hankel $H$ s'interprète comme la multiplication par un polynôme différentiel $P_H(\partial)$, où $\partial = \frac{d}{dx}$, dans l'anneau des polynômes. Nous reviendrons plus en détail sur ces structures dans la section suivante. Nous disposons d'une interprétation de même nature pour les matrices bézoutienne univariées que nous avons rencontrées au chapitre 4. Or, on a vu dans ce même chapitre que les opérateurs de multiplication dans une algèbre quotient se décomposent en termes de bézoutien et de résidu (qui est un polynôme différentiel). Cela permet de mettre en place des méthodes itératives comme la méthode des puissances, connues en analyse matricielle, mais pour une matrice de multiplication dans une algèbre quotient. L'analogue de la méthode des puissances permet d'obtenir une méthode itérative rapide pour le calcul d'une racine d'une équation algébrique : la méthode de Sebastio e Silva. Cette méthode a été étudiée par Jean-Paul Cardinal dans [25, 26]. La possibilité d'utiliser des méthodes itératives dans le cadre de la résolution des équations algébriques est une perspective intéressante. On peut en effet attendre une meilleure analyse du comportement numérique et de pouvoir sélectionner une ou plusieurs racines ayant des propriétés particulières.

Dans ce chapitre, nous nous intéressons à l'utilisation des matrices structurées dans le contexte de la résolution des équations algébriques et surtout des généralisations dans le cadre multivarié qui sont apparues récemment dans les travaux de Bernard Mourrain et Victor Pan et de leurs coauteurs [76, 75, 18, 77, 78, 19, 79]. Dans une première section, nous exposons des éléments de la théorie des matrices structurées. Dans une deuxième section nous exposons les généralisations des structures classiques dans le cadre multivarié. Dans une troisième section nous utiliserons ces structures pour la conception de méthodes itératives pour la résolution de systèmes algèbriques.

Nous travaillerons principalement sur le corps des nombres complexes. Le produit de deux polynômes à coefficients complexes, dont les degrés sont majorés par $d$, peut être réalisé en $\mathcal{O}(d\log(d))$ opérations arithmétiques. Néanmoins des algorithmes de produit rapide de polynômes existent sur tous les corps, mais la complexité est généralement en $\mathcal{O}(d\log(d)\log(\log(d)))$opérations arithmétiques et parfois d'autres termes composés de logarithmes itérés interviennent. On résume ce fait en notant
$\log^*(d) = \log(d)\log(\log(d))^{i_1}\log(\log(\log(d)))^{i_2}\cdots$, où le nombre de termes logarithmiques supplémentaires dépend du corps de base.

## 5.2 Matrices structurées usuelles

### 5.2.1 Introduction

Dans cette section, nous exposons des éléments de la théorie des matrices structurées. Il serait prétentieux de vouloir être exhaustif sur ce sujet tant il apparaît dans de nombreux domaines ayant donné lieu à de nombreux développements présentant chacun des intérêts différents [60, 63, 92, 15, 47]. Nous exposons ici quelques notions courantes qui nous seront utiles par la suite. Nous choisissons un point de vue proche de celui de Furhmann dans [47] ou de Dario Bini et Victor Pan dans [15]. Nous donnerons ensuite des applications des algorithmes de manipulations rapides de ces matrices dans le cadre de la résolution des équations algébriques.

### 5.2.2 Structures classiques

#### Notations

Dans la suite, $\mathbb{K}$ est un corps (sous-corps de $\mathbb{C}$ effectif), $R = \mathbb{K}[x]$ est l'anneau des polynômes en la variable $x$ et $L = \mathbb{K}[x^{-1}, x]$ est l'anneau des polynômes de Laurent. On note $\partial = \frac{d}{dx}$ et $\partial^i = \frac{1}{i!}\frac{d^i}{dx^i}$, $B = \mathbb{K}[\partial]$ est l'anneau des polynômes et $S = \mathbb{K}[[\partial]]$ l'anneau des séries formelles en la variable $\partial$.

#### Matrices de Toeplitz

On considère le polynôme $p(x) = \sum_{i=0}^{2d} p_i x^i$ de $R$ auquel on associe l'opérateur $\mathcal{M}_p$ de multiplication par $p$ dans $R$ défini comme suit :

$$\mathcal{M}_p : \left\{ \begin{array}{ccc} R & \longrightarrow & R \\ f & \longmapsto & pf \end{array} \right.$$

La matrice $M_p$ de l'opérateur $\mathcal{M}_p$ dans la base monomiale est de la forme :

$$\begin{array}{c} \\ 1 \\ \vdots \\ x^d \\ \vdots \\ x^{2d} \\ \vdots \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & \cdots & x^d & \cdots & \cdots \end{array} \\ \begin{pmatrix} p_0 & & \mathbf{0} & & \cdots \\ \vdots & \ddots & & & \cdots \\ p_d & & p_0 & & \cdots \\ \vdots & \ddots & \vdots & \ddots & \cdots \\ p_{2d} & & p_d & & \cdots \\ \vdots & \ddots & \vdots & \ddots & \cdots \\ \mathbf{0} & & p_{2d} & & \cdots \end{pmatrix} \end{array} \tag{5.1}$$

C'est une matrice bande infinie. Le coefficient d'indices $(i, j)$ de $M_p$ est le coefficient de $x^i$ dans $px^j$. Les coefficients sont égaux le long des parallèles à la diagonale. C'est une caractérisation des matrices de Toeplitz, dont nous donnons la définition précise ci-après :

**Définition 5.2.1** *Une matrice $T = (t_{i,j})_{i,j}$ est une matrice de Toeplitz si $t_{i+1,j+1} = t_{i,j}$, c'est-à-dire si le coefficient $t_{i,j}$ ne dépend que de $i - j$.*

**Remarque 5.2.2** *On peut considérer l'opérateur de multiplication par $p$ dans $L$, ce qui ferait de la matrice obtenue dans la base monomiale une matrice bande bi-infinie.*

Soit $T$ une matrice de Toeplitz $k \times h$ :

$$T = \begin{pmatrix} t_{1,1} & \cdots & t_{1,k} \\ \vdots & & \vdots \\ t_{h,1} & & t_{h,k} \end{pmatrix}.$$

Cette matrice peut être vue comme une sous-matrice de la matrice associée à l'opérateur de multiplication par un polynôme dans $R$. On considère le polynôme $p(x) = \sum_{i=0}^{k+h} p_i x^i$ avec $p_i = t_{1,k-i}$ pour $i \in \{0, \ldots, k-1\}$ et $p_{k+i-1} = t_{i,1}$ pour $i \in \{2, \ldots, h\}$. Dès lors, on note :

$$\widetilde{M_p} = \begin{pmatrix} p_k & \cdots & p_0 \\ \vdots & & \vdots \\ p_{k+h} & \cdots & p_{|k-h|} \end{pmatrix}$$

on a $T = \widetilde{M_p}$ qui est la matrice associée à l'application définie comme suit : on note $E = \langle 1, \ldots, x^k \rangle$, $F = \langle x^k, \ldots, x^{k+h} \rangle$ et $\Pi_E$ (resp. $\Pi_F$) la projection de $R$ dans $E$ (resp. $F$). Alors $\widetilde{M_p}$ est la matrice de :

$$\Pi_F \circ \mathcal{M}_p \circ \Pi_E$$

dans les bases décrites dans les définitions de $E$ et $F$. Cela nous permet d'obtenir facilement la proposition suivante :

**Proposition 5.2.3** *Un opérateur de Toeplitz (associé à une matrice de Toeplitz) peut toujours être interprété comme la restriction (sur le but et l'image) d'un opérateur de multiplication par un polynôme déterminé par la première ligne et la première colonne de la matrice associée à cet opérateur.*

L'intérêt algorithmique d'une telle approche est donné par la proposition suivante :

**Proposition 5.2.4** *Soit $T$ une matrice de Toeplitz $h \times k$ et soit $d = max\{h,k\}$, alors le produit de $T$ avec un vecteur $v \in \mathbb{K}^k$ peut se faire en $\mathcal{O}(d \log^*(d))$ opérations arithmétiques.*

*Preuve* : Soit $v = (v_1, \ldots, v_k) \in \mathbb{K}^k$, on considère alors le polynôme $V(x) = \sum_{i=0}^{k} v_k x^{i-1}$ et $p(x) = \sum_{i=0}^{h+k} p_i x^i$ avec $p_i = t_{1,k-i}$ pour $i \in \{0, \ldots, k\}$ et $p_i = t_{i,1}$ pour $i \in \{2, \ldots, h\}$. On considère alors le polynôme $W(x) = \Pi_F(p(x)V(x)) = \sum_{i=1}^{h} w_i x^{i-1}$. On note $w = (w_1, \ldots, w_h)$. On a $w = Tv$. La proposition découle alors du fait que la multiplication de $p$ par $V$ peut se faire en $\mathcal{O}(d \log^*(d))$ opérations arithmétiques par un produit rapide de polynômes univariés. ♣

Ce résultat confère aux matrices de Toeplitz des propriétés algorithmiques remarquable. Le fait que la multiplication d'une matrice de Toeplitz $d \times d$ avec un vecteur ne nécessite que $\mathcal{O}(d \log^*(d))$ opérations arithmétiques au lieu des $\mathcal{O}(d^2)$ opérations n'est pas la seule propriété remarquable de ces matrices. Nous en rencontrerons d'autres dans la suite de ce texte. On peut aussi retrouver les matrices de Toeplitz de la façon suivante : soit $p(x) = \sum_{i=0}^{2d} p_i x^i \in R$, on associe à $p$ l'application linéaire suivante :

$$\mathcal{M}_p^t : \left\{ \begin{array}{ccc} S & \longrightarrow & S \\ q(\partial) & \longmapsto & \pi_+(p(\partial^{-1})q(\partial)) \end{array} \right.$$

où $\pi_+$ est la projection sur les monômes d'exposants positifs. La matrice $M_p^t$ de $\mathcal{M}_p^t$ dans la base $\left(\partial^i\right)_{i\in\mathbb{N}}$ est alors :

$$\begin{array}{c} \\ 1 \\ \vdots \\ \partial^d \\ \vdots \end{array}
\begin{array}{c} \begin{array}{ccccccccc} 1 & \cdots & \partial^d & \cdots & \partial^{2d} & \cdots & & & \end{array} \\
\begin{pmatrix} p_0 & \cdots & p_d & \cdots & p_{2d} & \cdots & \cdots & \cdots \\ & \ddots & & \ddots & & \ddots & & \\ & & p_0 & \cdots & p_d & \cdots & p_{2d} & \\ & & & \ddots & & \ddots & & \ddots \end{pmatrix} \end{array}$$

On obtient une nouvelle matrice de Toeplitz qui est la transposée de $M_p$.

#### Matrices de Hankel

Soit $h(\partial) = h_0 + h_1\partial + \cdots + h_{2d}\partial^{2d} + \cdots \in S$, on associe à $h$ l'opérateur qui à tout $p \in \mathbb{K}[x]$ associe $\pi_+(p(\partial^{-1})h(\partial))$. La matrice $M_h$ de cette application dans la base monomiale est :

$$M_h = \begin{array}{c} \\ 1 \\ \vdots \\ x^d \\ \vdots \\ x^{2d} \\ \vdots \end{array}
\begin{array}{c} \begin{array}{ccccccc} 1 & \cdots & x^d & \cdots & x^{2d} & \cdots & \end{array} \\
\begin{pmatrix} h_0 & \cdots & h_d & \cdots & h_{2d} & \cdots \\ \vdots & ⋰ & & ⋰ & & \\ h_d & \cdots & h_{2d} & \cdots & \cdots & \cdots \\ \vdots & ⋰ & & ⋰ & & \\ h_{2d} & \cdots & \cdots & \cdots & \cdots & \cdots \\ \vdots & & & \vdots & & \end{pmatrix} \end{array} \tag{5.2}$$

La matrice est infinie vers la droite et vers le bas. Le coefficient d'indices $(i,j)$ de $M_h$ est le coefficient de $\partial^i$ dans $\partial^{-j}h(\partial)$. Les indices commencent ici à zéro. Ainsi les coefficients de $M_h$ soient égaux le long des parallèles à la deuxième diagonale. C'est une caractérisation des matrices de Hankel dont nous donnons la définition ci-après :

**Définition 5.2.5** *Une matrice $H = (h_{i,j})_{i,j}$ est de Hankel si $h_{i+1,j-1} = h_{i,j}$, ou de façon équivalente si $h_{i,j}$ ne dépend que de $i+j$.*

Aux chapitres 2 et 4, on a vu qu'on peut identifier $\widehat{\mathcal{R}}$ avec $S$ et que par conséquent $S$ est naturellement muni d'une structure de $R$-module. L'action de $x$ sur $S$ est alors analogue à la multiplication par $\partial^{-1}$. On retrouve de nouveau le formalisme des systèmes inverses. Soit $h \in S$, alors $M_h$ est la matrice de l'application :

$$\mathcal{H}_h : \left\{ \begin{array}{ccc} R & \longrightarrow & S \\ p(x) & \longmapsto & p(x)h(\partial) = \pi_+(p(\partial^{-1})h(\partial)) \end{array} \right.$$

Il s'ensuit que toute matrice de Hankel $H$, de taille $h \times k$ avec $d = \max\{h, k\} \leq n+1$, est une sous-matrice $M_h$ de la forme 5.2 où $h$ est entièrement déterminé par la première ligne et la première colonne de $H$.

On considère $E = \langle 1, \cdots, x^{2d} \rangle$ et $F = \langle 1, \cdots, \partial^{2d} \rangle$ et on note $\Pi_E$ (resp. $\Pi_F$) la projection de $R$ sur $E$ (resp. de $S$ sur $F$), alors $H$ est la matrice de l'application linéaire :

$$\Pi_F \circ \mathcal{H}_h \circ \Pi_E$$

Ce nous permet facilement d'obtenir la proposition suivante :

**Proposition 5.2.6** *Toute matrice de Hankel est la matrice de la restriction (sur la source et sur le but) d'un opérateur de multiplication de la forme $\mathcal{H}_h$ où $h$ est entièrement déterminé par la première ligne et la première colonne de la matrice.*

De la même façon que pour les matrices de Toeplitz, ce point de vue permet d'obtenir un algorithme de produit rapide d'une matrice de Hankel par un vecteur en se ramenant à un produit de polynômes :

**Proposition 5.2.7** *Soit $H$ une matrice de Hankel $(d+1) \times (d+1)$ et $v \in \mathbb{K}^{d+1}$, alors le produit $Hv$ peut être calculé en $\mathcal{O}(d \log^*(d))$ opérations arithmétiques.*

### Bézoutiens

Nous rappelons dans un premier temps les définitions des polynômes bézoutiens et matrices bézoutiennes :

**Définition 5.2.8** *Soient $p$ et $q \in \mathbb{K}[x]$, le polynôme bézoutien de $p$ et $q$ est donné par :*

$$\Theta_{q,p}(x,y) = \frac{p(x)q(y) - p(y)q(x)}{x-y} = \sum_{i,j} \theta_{i,j}(q,p) x^i y^j$$

*et la matrice bézoutienne est alors donnée par :*

$$B(q,p) = (\theta_{i,j})_{i,j}\,.$$

L'identification de $S$ avec $\widehat{\mathcal{R}}$ permet d'associer à $\Theta_{q,p}$ une application linéaire de $S$ dans $R$ définie comme suit : $\forall \Lambda \in S$, on associe $\overline{\chi}(\Theta_{q,p})(\Lambda) = \sum_{i,j} \theta_{i,j} \Lambda(y^j) x^i = \sum_{i,j} \theta_{i,j} \langle x^j, \Lambda(\partial) \rangle_0 x^i$. Avec ces notations, $B_{q,p}$ est la matrice de $\overline{\chi}(\Theta_{q,p})$ exprimée de la base $(\partial^i)_{i \in \mathbb{N}}$ de $S$ dans la base $(x^i)_{i \in \mathbb{N}}$ de $R$.

Un cas particulièrement important est celui de la matrice bézoutienne $B_{1,p}$. Dans le chapitre 4, on a vu que si on note $p(x) = \sum_{i=0}^{d} p_i x^i$, alors :

$$B_{1,p} = \begin{pmatrix} p_1 & \cdots & p_d \\ \vdots & \cdot^{\cdot^{\cdot}} & \\ p_d & & 0 \end{pmatrix}$$

et les colonnes de cette matrice sont les coefficients des polynômes de Horner dans la base monomiale.

Il existe bien d'autres types de matrices structurées, comme les matrices de Vandermonde que nous avons déjà rencontrées, mais nous nous limiterons aux trois structures que nous venons de décrire ainsi qu'aux liens qui les relient et à des applications algorithmiques de l'exploitation de ces structures. Mais avant nous présentons un point de vue un peu plus courant sur ces matrices.

**Remarque 5.2.9** *Une notion très couramment utilisée est celle de rang de déplacement. Nous ne la traitons pas ici, mais elle occupe un rôle central dans beaucoup de méthodes sur les matrices structurées (voir [60]).*

### 5.2.3 Liens entre les structures Hankel et bézoutienne

Les opérateurs de Hankel sont associés à des applications de $\mathbb{K}[x]$ dans $\mathbb{K}[[\partial]]$ et les bézoutiens sont associés eux à des applications de $\mathbb{K}[[\partial]]$ dans $\mathbb{K}[x]$.

Soit $p(x) = \sum_{i=0}^{d} p_i x^i$ un polynôme de degré $d$ (i.e. $p_d \neq 0$). On note $\mathcal{I} = (p)$ l'idéal engendré par ce polynôme et $\mathcal{I}^\perp$ l'orthogonal de cet idéal qu'on identifie au sous-espace vectoriel de $\mathbb{K}[[\partial]]$ des séries $h(\partial)$ telles que $\langle h(\partial), q(x) \rangle_0 = 0$ pour tout $q \in \mathcal{I}$.

**Proposition 5.2.10** *La classe d'une série $h \in \mathcal{I}^\perp$ coïncide avec la classe des fractions rationnelles vérifiant :*

$$h(\partial) = \frac{\partial^{-1} r(\partial^{-1})}{p(\partial^{-1})} = h_0 + h_1 \partial + \cdots$$

*où* $r(x) = \sum_{i=0}^{d-1} a_i x^i$ *est un polynôme de* $\mathbb{K}[x]_{d-1}$.

*Preuve* : Voir [78]. ♣

Cette proposition signifie que les séries associées aux formes linéaires de $\mathcal{I}^\perp$ sont des séries rationnelles admettant toutes $p$ comme dénominateur commun. Cela n'a rien d'étonant sachant que $\mathcal{I}^\perp$ est un $\mathbb{K}[x]/\mathcal{I}$-module libre de rang 1. En effet, la série associée au résidu $\tau_p$ est la série $\tau_p(\partial) = \frac{\partial^{-1}}{p(\partial^{-1})}$. On a déjà vu au chapitre 4 que le résidu algébrique associé à $p$ est une forme linéaire de $\mathcal{I}^\perp$ vérifiant $B_{1,p}(\tau_p) = 1$. Or la matrice associée à $\tau_p$ est une matrice de Hankel. Cela nous conduit naturellement à approfondir la recherche de liens entre les structures de Bézout et de Hankel.

On note $H_{\tau_p}$ la matrice associée à la série représentant le résidu algébrique, on a alors la proposition suivante :

**Proposition 5.2.11** *Soit* $p \in \mathbb{K}[x]$, *on a :*

$$B_{1,p} H_{\tau_p} = \mathbb{I}_d \tag{5.3}$$

## 5.3 Matrices structurées associées à des polynômes multivariés

Dans cette section, nous reprenons brièvement les généralisations des structures Toeplitz, Hankel et bézoutienne telles qu'elles ont été exposées dans [78]. Notre objectif est d'exposer l'application de ces structures à la résolution de systèmes algébriques. Nous gardons les mêmes notations que dans les chapitres précédents.

On fixe maintenant quelques notations. On note $R = \mathbb{K}[x_1, \ldots, x_n]$ et $\widehat{\mathcal{R}} = \mathbb{K}[[\partial_1, \ldots, \partial_n]]$. On note $L = \mathbb{K}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ l'ensemble des polynômes de Laurent des variables $x_1, \ldots, x_n$. Au chapitre 2 on a vu une façon d'exprimer le fait que $\widehat{\mathcal{R}}$ soit un $R$-module. La proposition suivante nous donne une nouvelle façon de l'exprimer qui nous sera utile par la suite :

**Proposition 5.3.1** *Soient* $p$ *et* $q \in R$ *et* $\Lambda(\partial) \in \widehat{\mathcal{R}}$, *on a :*

$$p\Lambda(q) = \Lambda(pq) = \Pi_+(p(\partial^{-1})\Lambda(\partial))(q) = \langle \Pi_+(p(\partial^{-1})\Lambda(\partial)), q\rangle_0,$$

*où* $\Pi_+$ *est la projection sur l'espace vectoriel engendré par les monômes de la forme* $\partial^\alpha$, *où* $\alpha \in \mathbb{N}^n$.

### 5.3.1 Matrices quasi-Toeplitz et quasi-Hankel

#### Définitions

On donne maintenant les définitions des structures quasi-Toeplitz et quasi-Hankel :

**Définition 5.3.2** *Soient $E$ et $F$ deux sous-ensembles finis de $\mathbb{N}^n$ et soit $(m_{\alpha,\beta})_{\alpha\in E,\beta\in F}$ une matrice dont les lignes sont indicées par les monômes $\mathbf{x}^\alpha$ tels que $\alpha \in E$ et les colonnes sont indicées par les monômes de la forme $\mathbf{x}^\beta$ avec $\beta \in F$. Soit $\delta_i = (\delta_{i,j})_{j\in\{1,\ldots,n\}} \in \mathbb{N}^n$ :*

- *$M$ est une matrice quasi-Toeplitz si pour tout $\alpha \in E$ et $\beta \in F$ le coefficient $m_{\alpha,\beta} = t_{\alpha-\beta}$ ne dépend que de $\alpha - \beta$. Cela revient à dire que si $\alpha+\delta_i \in E$ et $\beta+\delta_i \in F$ alors $m_{\alpha+\delta_i,\beta+\delta_i} = m_{\alpha,\beta}$. Si $M$ est une matrice quasi-Toeplitz, on lui associe un polynôme $T_M(\mathbf{x}) = \sum_{\mathbf{u}\in E+F} t_{\mathbf{u}}\mathbf{x}^{\mathbf{u}}$ et un opérateur $\mathcal{M}_{T_M} : R \to R$ défini par $p \to T_M(\mathbf{x})p(\mathbf{x})$.*
- *$M$ est une matrice quasi-Toeplitz si $m_{\alpha,\beta} = h_{\alpha-\beta}$ ne dépend que de $\alpha-\beta$. Cela revient à dire si $\alpha+\delta_i \in E$ et $\beta-\delta_i \in F$ alors $m_{\alpha+\delta_i,\beta-\delta_i} = m_{\alpha,\beta}$. Si $M$ est une matrice quasi-Hankel on lui associe un polynôme de Laurent $H_M(\partial) = \sum_{\mathbf{u}\in E-F} t_{\mathbf{u}}\partial^{\mathbf{u}}$ et un opérateur $\mathcal{H}_{H_M}$.*

**Définition 5.3.3** *Soit $E \in \mathbb{N}^n$, on note $\Pi_E$ la projection définie par $\Pi_E(\mathbf{x}^\alpha) = \mathbf{x}^\alpha$ si $\alpha \in E$ et $0$ sinon. De la même façon, $\Pi_E$ représente la projection $\Pi_E : \widehat{\mathcal{R}} \to \widehat{\mathcal{R}}$ définie par $\Pi(\partial^\alpha) = \partial^\alpha$ si $\alpha \in E$ et $0$ sinon.*

Cette définition permet de définir les opérateurs quasi-Toeplitz et quasi-Hankel en termes de multiplication par des polynômes :

**Proposition 5.3.4** *Une matrice $M$ est $(E,F)$ quasi-Toeplitz (resp. $(E,F)$ quasi-Hankel) si et seulement si c'est la matrice de l'opérateur $\Pi_E\circ\mathcal{M}_{T_M}\circ\Pi_F$ (resp. $\Pi_E \circ \mathcal{H}_{H_M} \circ \Pi_F$).*

*Preuve* : Voir [78]. ♣

Grâce à cette proposition, la multiplication d'une matrice $(E,F)$ quasi-Toeplitz (resp. $(E,F)$ quasi-Hankel) par un vecteur $\mathbf{v} = (v_\beta)_{\beta\in F}$ est réduite à la multiplication de polynômes de Laurent. C'est l'objet de l'algorithme suivant :

**Algorithme 5.3.5**

<u>Entrée</u> : *Une matrice* $M = (m_{\alpha,\beta})_{\alpha\in E,\beta\in F}$ $(E,F)$ *quasi-Toeplitz (resp.* $(E,F)$ *quasi-Hankel) et un vecteur* $\mathbf{v} = (v_\beta)_{\beta\in F}$

- *Multiplier le polynôme* $T_M(\mathbf{x}) = \sum_{\mathbf{u}\in E+F} t_\mathbf{u}\mathbf{x}^\mathbf{u}$ *(resp.* $H_M(\partial) = \sum_{\mathbf{u}\in E-F} h_\mathbf{u}\partial^\mathbf{u}$*)* *par* $\mathbf{v}(\mathbf{x}) = \sum_{\beta\in F} v_\beta\mathbf{x}^\beta$ *(resp.* $\mathbf{v}(\partial^{-1}) = \sum_{\beta\in F} v_\beta\partial^{-\beta}$*).*

<u>Sortie</u> : *Retourner la projection du polynôme produit sur* $\mathbf{x}^E$ *(resp.* $\partial^E$*).*

### Complexité arithmétique

On décrit maintenant la complexité arithmétique du calcul avec des polynômes, ce qui permet de donner des bornes sur la manipulation de matrices de type quasi-Hankel et quasi-Toeplitz.

Soient $G \subset \mathbb{N}^n$ et $K \in \mathbb{N}$, on note $C_{K,Eval}(G)$ le nombre d'opérations arithmétiques nécessaire à l'évaluation d'un polynôme dont le support est $G$ sur un ensemble de $K$ points. Soient $E$ et $F$ deux sous-ensembles de $\mathbb{N}^n$, on note $C_{PolMult}(E,F)$ la complexité arithmétique de la multiplication d'un polynôme à support dans $E$ par un polynôme à support dans $F$. Le théorème suivant, prouvé dans [83] à partir de l'algorithme d'interpolation creuse de [16], exprime la complexité de la multiplication de polynômes à supports fixés.

**Théorème 5.3.6** *Soit* $E+F = \{\alpha_1,\ldots,\alpha_N\}$ *avec* $|\alpha_i| = d_i$, $\forall i \in \{1,\ldots,N\}$ *et* $d = max\{d_1,\ldots,d_n\}$. *On a alors :*

$$C_{PolMult}(E,F) = \mathcal{O}\left(C_{N,Eval}(E) + C_{N,Eval}(F) + N(\log^2(N) + \log(d))\right) \tag{5.4}$$

Avec ce résultat, on peut donner la complexité de la multiplication d'une matrice quasi-Toeplitz ou quasi-Hankel par un vecteur :

**Proposition 5.3.7** *Une matrice* $(E,F)$ *quasi-Hankel (resp.* $(E,F)$ *quasi-Toeplitz)* $M$ *peut être multipliée par un vecteur en* $\mathcal{O}\left(N\log^2(N) + N\log(d) + C_{M,N}\right)$ *opérations arithmétiques, où* $d = deg(H_M)$ *(resp.* $d = deg(T_M)$*),* $N = \#(E - 2*F)$ *(resp.* $N = \#(E+2F)$*) et* $C_{N,M}$ *est le coût de l'évaluation de tous les monômes de* $H_M$ *(resp.*$T_M$*) en* $N$ *points.*

L'intérêt de savoir multiplier rapidement une matrice par un vecteur a une application importante pour la résolution de systèmes linéaires (voir [53]) :

**Proposition 5.3.8** *Soit* $W\mathbf{v} = \mathbf{w}$ *un système linéaire non-singulier de* $N$ *équations. Alors avec* $N$ *multiplications de* $W$ *et* $W^t$ *par des vecteurs et avec* $\mathcal{O}(N^2)$ *opérations arithmétiques supplémentaires, on obtient la solution* $\mathbf{v}$ *du système linéaire considéré.*

On remarque que par définition si $W$ est quasi-Toeplitz ou quasi-Hankel alors $W^t$ est également quasi-Toeplitz ou quasi-Hankel. Ainsi la proposition précédente et le théorème 5.3.6 conduisent à un algorithme de résolution rapide de systèmes linéaires associés à des matrices quasi-Toeplitz et quasi-Hankel.

La proposition suivante, tirée de [78], nous sera également utile :

**Proposition 5.3.9**
*Soit* $W$ *une matrice carrée de taille* $N$ *réelle et symétrique. Soit* $S$ *un ensemble de nombres complexes (on suppose* $\#(S) > N$*). Alors il existe un algorithme probabiliste qui, à partir de* $N$ *valeurs tirées aléatoirement dans* $S$ *, indépendamment les unes des autres (avec une distribution uniforme sur* $S$*), soit échoue avec une probabilité d'au plus* $\frac{(N+1)N}{2\#(S)}$*, soit calcule* $\mathcal{O}(N)$ *multiplications de* $W$ *avec des vecteurs et donne le rang et la signature de* $W$ *avec* $\mathcal{O}(N^2\log(N))$ *opérations arithmétiques supplémentaires.*

### 5.3.2 Arithmétique dans une algèbre quotient

#### Contexte

On considère $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ définissant une application polynomiale $\mathbf{f} = (f_1, \ldots, f_n)$ et un idéal $\mathcal{I} = (f_1, \ldots, f_n) \subset \mathbb{K}[x_1, \ldots, x_n]$. On suppose que cet idéal définit un ensemble algébrique $Z(\mathcal{I}) = \{\zeta_1, \ldots, \zeta_d\}$ de dimension zéro. Cela implique que $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}$ est un $\mathbb{K}$-espace vectoriel de dimension finie $D \geq d$. On suppose connue $E = \{\alpha_1, \ldots, \alpha_D\} \subset \mathbb{N}^n$ tel que $\mathbf{x}^E$ soit une base de $\mathcal{A}$. Soit $F \subset \mathbb{N}^n$, on associe à $F$ l'ensemble $\Omega(F) = \left\{\mathbf{x}^\beta \,|\, \exists \alpha \in F \text{ et } k \in \{1, \ldots, n\} \text{ tels que } x_k\mathbf{x}^\alpha = \mathbf{x}^\beta \text{ et } \alpha \notin F\right\}$ que nous appelons, conformément à la terminologie du chapitre 2, la frontière de $F$. Soit $\Lambda \in \mathcal{I}^\perp$, on associe à $\Lambda$ la forme bilinéaire $(a, b) \to \Lambda(ab)$. Par abus de langage, on dira que $\Lambda$ est une forme linéaire non-dégénérée si la forme bilinéaire associée est non-dégénérée.

#### Construction d'une forme linéaire non-dégénérée

Dans cette partie, on construit une forme linéaire non-dégénérée sur $\mathcal{A}$. Notre objectif est de calculer les coefficients $\tau(\mathbf{x}^\alpha)$ pour $\alpha \in E + E + E$

d'une forme linéaire générique $\tau \in \widehat{\mathcal{A}} = \mathcal{I}^{\perp}$. Ceci se fera par induction sous les hypothèses suivantes :

**Hypothèses 1**

- $\mathbf{x}^E$ *est stable par dérivation, i.e. si* $\mathbf{x}^\alpha = x_i \mathbf{x}^\beta$, *pour* $i \in \{1, \ldots, n\}$, *alors* $\beta \in E$.
- *On connaît la forme normale de* $N_\beta = \sum_{\alpha \in E} n_{\beta,\alpha} \mathbf{x}^\alpha$ *de* $\mathbf{x}^\beta$ *pour tout* $\beta \in \Omega(E)$.
- *On connait les coefficients* $\tau_\alpha = \tau(\mathbf{x}^\alpha)$, $\forall \alpha \in E$, *où* $\tau$ *est une forme linéaire non-dégénérée sur* $\mathcal{A}$.

**Remarque 5.3.10** *La troisième hypothèse n'est pas très restrictive puisqu'un choix aléatoire pour les coefficients* $\tau_\alpha$ *conduit à une forme linéaire non-dégénérée avec une très forte probabilité de succès.*

Notre approche repose sur la propriété suivante :

**Proposition 5.3.11** *Pour tout* $\beta \in \Omega(E)$, *on a* $\tau_\beta = \tau(N_\beta) = \sum_{\alpha \in E} n_{\alpha,\beta} \tau_\alpha$. *Cette valeur peut être calculée en* $\mathcal{O}(D)$ *opérations arithmétiques, où* $D = \#(E)$. *Plus généralement, pour tout* $\alpha$ *et* $\gamma \in E$, *on a la relation de récurrence suivante :*

$$\tau_{\alpha+\gamma} = \sum_{\beta \in E} n_{\alpha,\beta} \tau_{\beta+\gamma}.$$

Si on suppose maintenant qu'on a calculé toutes les valeurs $\tau_\beta$ pour $\beta \in \Omega(E)$. Soit $\alpha = \alpha_0 + (\delta_{i,j})_{j \in \{1,\ldots,n\}} \in \Omega(\Omega(E))$ avec $\alpha_0 \in \Omega(E)$. Alors :

$$\tau(\mathbf{x}^\alpha) = \tau(x_i N_{\alpha_0}) = \sum_{\beta \in E} n_{\alpha_0,\beta} \tau(x_i \mathbf{x}^\beta).$$

On connaît alors tous les coefficients $n_{\alpha_0,\beta}$ et tous les $\tau(x_i \mathbf{x}^\beta)$. Ainsi, on obtient $teu_\alpha = \sum_{\beta \in E} n_{\alpha_0,\beta} \tau(x_i \mathbf{x}^\beta)$ en calculant un produit scalaire.

**Définition 5.3.12** *On note* $h = max\{|\alpha| \mid \alpha \in E\}$. *Soient* $\Omega_0 = E$, $\Omega_i = (\Omega_{i-1} \cap \Omega(\Omega_{i-1})) \cap E + E + E$, $i \in \{1, \ldots, 2 * h\}$. *Ainsi* $\Omega_{2h} = E + E + E$.

La proposition suivante permet de calculer tous les coefficients voulus de la forme linéaire $\tau$ :

**Proposition 5.3.13** *Pour tout $\alpha \in \Omega_i$, il existe $\alpha' \in \mathbb{N}^n$ et $\alpha_1 \in \Omega_1 \setminus \Omega_0$ tel que $\alpha = \alpha_0 + \alpha'$ avec $|\alpha'| \leq i-1$ et pour tout $\beta \in E$, on a $\beta + \alpha' \in \Omega_{i-1}$.*

*Preuve* : Supposons $i > 0$. Soit $\alpha \in \Omega_i \subset E+E+E$. Alors $\alpha$ peut être décomposé sous la forme $\alpha = \gamma_0 + \gamma_1 + \gamma_2$ où $\gamma_0, \gamma_1$ et $\gamma_2 \in E$ et par exemple $|\gamma_1 + \gamma_2| = i$. Comme $i \geq 1$, il existe $\alpha' = \gamma_1 + \gamma_2 - (\delta_{j,i})_{i\in\{1,\ldots,n\}} \in \mathbb{N}^n$, puisque $E$ est stable par dérivation. Ainsi $\alpha' \in E+E$. Il s'ensuit que $\alpha = \alpha_1 + \alpha'$ où $\alpha_1 = \gamma_0 + (\delta_{j,i})_{i\in\{1,\ldots,n\}} \in \Omega_1$ et $|\alpha'| \leq i-1$. Puisque $\forall \beta \in E$, $\beta + \alpha' \in \Omega_{i-1}$ et la proposition est prouvée. ♣

Ainsi si on a calculé tous les $\tau_\alpha$ pour $\alpha \in \Omega_{i-1}$, alors par la proposition 5.3.13, pour tout $\alpha \in \Omega_i$, on a $\alpha = \alpha' + \alpha_1$ avec $\alpha_1 \in \Omega_1$ et $|\alpha'| \leq i-1$. Ainsi, si $\alpha_1 \in \Omega_1 \setminus \Omega_0$, on a $\tau(\mathbf{x}^\alpha) = \tau(\mathbf{x}^{\alpha_1}\mathbf{x}^{\alpha'}) = \sum_{\beta\in E} n_{\alpha_1,\beta}\tau(\mathbf{x}^\beta\mathbf{x}^{\alpha'})$ avec $\beta + \alpha' \in \Omega_{i-1}$. Autrement dit, on peut calculer tous les coefficients de $\tau$ sur $\Omega_i$ à partir de ses valeurs sur $\Omega_{i-1}$. Cela conduit à l'algorithme suivant :

**Algorithme 5.3.14 (Calcul des coefficients de $\tau$ sur $E+E+E$)**

<u>*Entrée*</u> : *Les coefficients $\tau_\alpha$, $\alpha \in E$ et les formes normales $N_\alpha$, $\alpha \in \Omega(E)$.*

- *Pour $i$ allant de 1 à $2h$ faire*
  *pour tout $\alpha = \alpha_0 + \alpha_1$ comme dans la proposition 5.3.13, calculer $\tau_\alpha = \sum_{\beta\in E} n_{\alpha_1,\beta}\tau_{\beta+\alpha_0}$.*

<u>*Sortie*</u> : *Retourner $S = \sum_{\alpha\in E+E+E} \tau_\alpha \partial^\alpha$.*

La proposition suivante décrit la complexité de cet algorithme :

**Proposition 5.3.15** *La complexité arithmétique de l'algorithme 5.3.14 est $\mathcal{O}(3^n D^2)$.*

*Preuve* : Pour tout $\alpha \in E+E+E$, on calcule $\tau_\alpha$ en $\mathcal{O}(D)$ opérations arithmétiques. Comme il y a au maximum $\mathcal{O}(3^n D)$ éléments dans $E+E+E$, on obtient l'estimation de la proposition. ♣

### Matrice quasi-Hankel associée à $\tau$

On suppose connue une forme linéaire $\tau \in \widehat{\mathcal{A}}$ telle que la forme bilinéaire associée est non-dégénérée sur $\mathcal{A} \times \mathcal{A}$. On admet que cette forme linéaire est donnée sous la forme de ses coefficients $(\tau(\mathbf{x}^\alpha))_{\alpha\in F}$ où $F = E+E+E$.

**Définition 5.3.16** *Pour tout* $\Lambda \in \widehat{\mathcal{A}}$ *et pour tout* $F \subset \mathbb{N}^n$, *soit* $H_\Lambda^F$ *la matrice quasi-Hankel* $(\tau(\mathbf{x}^{\alpha+\beta}))_{\alpha,\beta\in F}$.

**Proposition 5.3.17** *La matrice* $H_\Lambda^F$ *peut être multipliée par un vecteur en* $\mathcal{O}(3^n\#(F)\log(3^n\#(F)))$ *opérations arithmétiques.*

*Preuve* : C'est une application de la proposition 5.3.7 à la multiplication de la matrice $(F, F)$ quasi-Toeplitz $H_\Lambda^F$ en remarquant que $\#(F+F+F) = 3^n\#(F)$. ♣

**Proposition 5.3.18**
*Vérifier que le système* $H_\Lambda^F\mathbf{u} = \mathbf{v}$ *a une solution unique et, si c'est le cas, la calculer nécessite* $\mathcal{O}(3^n\#(F)^2\log(3^n\#(F)))$ *opérations arithmétiques. La même estimation de complexité peut être appliquée au calcul du rang de* $H_\Lambda^F$, *mais avec un algorithme probabiliste (voir la proposition 5.3.9) impliquant le choix de* $\#(F)$ *paramétres aléatoires avec une probalité d'échec d'au plus* $\frac{(\#(F)+1)\#(F)}{2\#(S)}$ *en supposant que les paramètres proviennent d'un ensemble fini* $S$.

### 5.3.3 Bases duales pour $\tau$

Comme $\tau$ définit une forme bilinéaire non-dégénérée, il existe une famille de polynômes $(\mathbf{w}_\alpha)_{\alpha\in E}$ telle que $\tau(\mathbf{x}^\alpha\mathbf{w}_\beta) = \delta_{\alpha,\beta}$, i.e. $(\mathbf{w}_\alpha)_{\alpha\in E}$ est une base duale de la base $\mathbf{x}^E$ pour $\tau$. D'après le chapitre 4, on dispose alors de la formule de Cauchy :

$$p \equiv \sum_{\alpha\in E}\tau(p\mathbf{w}^\alpha)\mathbf{x}^\alpha \equiv \sum_{\alpha\in E}\tau(p\mathbf{x}^\alpha)\mathbf{w}_\alpha$$

**Définition 5.3.19** *Pour tout* $p \in \mathcal{A}$, *on note* $[p]_\mathbf{x}$ *et* $[p]_\mathbf{w}$ *les vecteurs associés à* $p$ *dans la base* $\mathbf{x}^E$ *et* $(\mathbf{w}_\alpha)_{\alpha\in E}$ *respectivement.*

Soit $\mathbf{w}_\alpha = \sum_{\beta\in E} w_{\alpha,\beta}\mathbf{x}^\beta$, on note alors $W_\tau = (w_{\alpha,\beta})_{\alpha,\beta\in E}$. Par définition des bases, on a :

$$\tau(\mathbf{w}_\alpha\mathbf{x}^\gamma) = w_{\alpha,\beta}\tau(\mathbf{x}^{\beta+\gamma}) = \delta_{\alpha,\gamma}. \tag{5.5}$$

En termes de matrices, l'équation 5.5 implique que :

$$H_\tau W_\tau = Id \tag{5.6}$$

où $H_\tau = H_\tau^E = (\tau(\mathbf{x}^{\beta+\gamma}))_{\beta,\gamma\in E}$. Par définition de $W_\tau$ et par l'équation 5.6, on obtient :

$$[p]_\mathbf{x} = W_\tau[p]_\mathbf{w} \text{ et } [p]_\mathbf{w} = H_\tau[p]_\mathbf{x}. \tag{5.7}$$

Le résultat suivant découle alors de la proposition 5.3.18 :

**Proposition 5.3.20**
*Pour tout $p \in \mathcal{A}$, les coordonnées de $p$ dans la base $\mathbf{x}^E$ peuvent être calculées de ses coordonnées dans la base $(\mathbf{w}_\alpha)_{\alpha\in E}$ en $\mathcal{O}(3^n D^2 \log(3^n D))$ opérations arithmétiques.*

### 5.3.4 Produit dans $\mathcal{A}$

En appliquant la formule de Cauchy à $f \in R$, on a $f \equiv \sum_{\alpha\in E} \tau(f\mathbf{x}^\alpha)\mathbf{w}_\alpha = \sum_{\alpha\in E} f * \tau(\mathbf{x}^\alpha)\mathbf{w}_\alpha$ dans $\mathcal{A}$. De plus, en exprimant la forme linéaire $f * \tau$ en termes de série différentielle , on obtient $f * \tau = \sum_{\alpha\in\mathbb{N}^n} f * \tau(\mathbf{x}^\alpha)\partial^\alpha$, si bien que les coefficients des $(\partial^\alpha)_{\alpha\in E}$ dans $f * \tau$ sont les coordonnées du vecteur $[f]_\mathbf{w}$.

De la même façon, pour tous $f$ et $g \in \mathcal{A}$, les coefficients de $(\partial^\alpha)_{\alpha\in E}$ dans l'expression de $fg * \tau$ sont les coefficients du vecteur $[fg]_\mathbf{w}$. Cela conduit à l'algorithme suivant :

**Algorithme 5.3.21 (Produit dans $\mathcal{A}$)**

- *Calculer $[fg]_\mathbf{w}$ en calculant les coefficients de $(\partial^\alpha)_{\alpha\in E}$ dans l'expression de $fg * \tau$.*
- *Résoudre en $\mathbf{u}$ le système $[fg]_\mathbf{w} = H_\tau \mathbf{u}$.*
- <u>*Sortie*</u> *: Retourner le vecteur $\mathbf{u}$ qui est le vecteur des coordonnées de $fg$ dans la base $\mathbf{x}^E$, i.e. $\mathbf{u} = [fg]_\mathbf{x}$.*

**Proposition 5.3.22** *Le produit $fg$ dans $\mathcal{A}$ peut être calculé en $\mathcal{O}(3^n D^2 \log(3^n D))$ opérations arithmétiques.*

*Preuve* : $fg*\tau$ est le produit de polynômes à support dans $E$ et $E+E+E$. Ce produit peut être calculé en $\mathcal{O}(3^n D^2 \log(3^n D))$ opérations arithmétiques. La complexité de la résolution du système linéaire est du même ordre par la proposition 5.3.20. ♣

### 5.3.5 Inversion dans $\mathcal{A}$

La formule de Cauchy implique que $f\mathbf{x}^\alpha = \sum_{\alpha\in E} f * \tau(\mathbf{x}^{\alpha+\beta})\mathbf{w}_\beta$, ce qui signifie que $[f\mathbf{x}^\alpha]_\mathbf{w}$ est le vecteur des coordonnées de $[f*\tau(\mathbf{x}^{\alpha+\beta})]_{\beta\in E}$, i.e. c'est la colonne de $H_{f*\tau}$ indicée par $\alpha$. En d'autres termes, $[f\mathbf{x}^{\alpha}]_{\mathbf{w}} = H_{f*\tau}[x^{\alpha}]_{\mathbf{x}}$. Par linéarité, pour tout $g \in \mathcal{A}$, on a :

$$[fg]_{\mathbf{w}} = H_{f*\tau}[g]_{\mathbf{x}} = H_{\tau}[fg]_{\mathbf{x}}.$$

Ainsi si $fg = 1$ dans $\mathcal{A}$, i.e. $g = f^{-1}$, on a $H_{f*\tau}[g]_{\mathbf{x}} = H_{\tau}[1]_{\mathbf{x}}$. Cela conduit à l'algorithme suivant pour le calcul de l'inverse d'un polynôme dans $\mathcal{A}$ :

**Algorithme 5.3.23 (Inversion dans $\mathcal{A}$)**

*Entrée :* $f \in \mathcal{A}$.
- *Calculer* $\mathbf{v} = H_{\tau}[1]_{\mathbf{x}}$.
- *Résoudre en* $\mathbf{u}$ *le système linéaire* $H_{f*\tau}\mathbf{u} = \mathbf{v}$ *ou retourner une erreur si* $H_{f*\tau}$ *n'est pas inversible.*

*Sortie :* *Retourner le vecteur* $\mathbf{u}$ *qui est le vecteur* $[f^{-1}]_{\mathbf{x}}$.

**Proposition 5.3.24** *L'inverse de* $f$ *d'un élément inversible* $f \in \mathcal{A}$ *peut être calculé en* $\mathcal{O}(3^n D^2 \log(3^n D))$ *opérations arithmétiques.*

### 5.3.6 Méthodes itératives

Les algorithmes que nous proposerons pour l'approximation des racines consistent à calculer des idempotents de $\mathcal{A}$ en utilisant des méthodes itératives et en utilisant le fait que les racines du système à résoudre se déduisent facilement à partir de ces idempotents. Nos algorithmes ont pour cadre $\mathbb{C}^n$. Les deux méthodes étudiées ici sont exposées dans le cadre univarié par J.P. Cardinal dans [26]. Ces algorithmes itératifs reposent sur les opérations arithmétiques dans $\mathcal{A}$.

#### Méthodes de Joukovski

Dans le cas univarié ces méthodes consistent à itérer des fractions rationnelles. La première application est une modification de l'application de Joukovski, définie par $z \rightarrow \frac{1}{2}(z + \frac{1}{z})$ ou une variante $z \rightarrow \frac{1}{2}(z - \frac{1}{z})$. Les points fixes (qui sont attractifs) de l'application de Joukovski sont 1 et $-1$ et ceux de l'application de Joukovski modifiée sont $\mathbf{i}$ et $-\mathbf{i}$.

On utilise ces mêmes applications dans le cas multivarié. On donne maintenant un premier algorithme :

**Algorithme 5.3.25 (Méthode du signe)**

*Entrée :* *Un polynôme* $u_0 = h \in \mathcal{A}$.

- $u_1 = \frac{1}{2}(u_0 - \frac{1}{u_0}$.
- *Tant que* $\|u_k - u_{k-1}\| > 2^{-b}$ *faire*

$$u_{k+1} = \frac{1}{2}(u_k - \frac{1}{u_k}); \; k = k+1.$$

<u>Sortie</u> : *Retourner la dernière valeur* $u_k$ *calculée.*

En corollaire de la proposition 5.3.24, on obtient la proposition suivante :

**Proposition 5.3.26** *Chaque itération de l'algorithme 5.3.25 nécessite* $\mathcal{O}(3^n D^2 \log(3^n D))$ *opérations arithmétiques.*

On note $\mathrm{re}(\zeta)$ et $\mathrm{im}(\zeta)$ les parties réelles et imaginaires d'un nombre complexe $\zeta$ respectivement. On note par $\zeta$ un point de $Z(\mathcal{I})$.

**Proposition 5.3.27** *Le suite* $(u_i)_{i\in\mathbb{N}}$ *de la proposition 5.3.25 converge quadratiquement vers* $\sigma = \sum_{|im(()\zeta)|>0} \mathbf{e}_\zeta - \sum_{|im(()\zeta)|<0} \mathbf{e}_\zeta$ *et on a :*

$$\|u_i - \sigma\| \leq K\rho^{2i}$$

*pour une valeur réelle* $\mathbb{K}$ *, où :*

$$\rho^+ = max\left\{\frac{h(\zeta)-\mathbf{i}}{h(\zeta)+\mathbf{i}} | \zeta \in Z(\mathcal{I}) \text{ tel que } im(\zeta) > 0\right\}$$

$$\rho^- = max\left\{\frac{h(\zeta)+\mathbf{i}}{h(\zeta)-\mathbf{i}} | \zeta \in Z(\mathcal{I}) \text{ tel que } im(\zeta) < 0\right\}$$

*et* $\rho = max\{\rho^+, \rho^-\}$.

*Preuve* : Il s'agit d'appliquer l'analyse de convergence de la méthode de Joukovski (voir [58]) à la matrice de multiplication par $u_i$ dans $\mathcal{A}$ dont l'ensemble des valeurs propres est $\{u_i(\zeta) | \zeta \in Z(\mathcal{I})\}$. ♣

Soient :

$$\mathbf{e}^+ = \sum_{\mathrm{im}(\zeta)>0} \mathbf{e}_\zeta = \frac{1}{2}(1+\sigma)$$

et

$$\mathbf{e}^- = \sum_{\mathrm{im}(\zeta)<0} \mathbf{e}_\zeta = \frac{1}{2}(1-\sigma)$$

Les polynômes $\mathbf{e}^+$ et $\mathbf{e}^-$ sont des idempotents de $\mathcal{A}$. Si $h \in \mathcal{A}$ est une équation linéaire en $\mathbf{x}$, alors chacun des $\mathbf{e}^+$ et $\mathbf{e}^-$ est associé aux racines dans un demi-espace de $\mathbb{C}^n$ défini par $\mathrm{im}(\zeta) > 0$ et $\mathrm{im}(\zeta) < 0$ respectivement. Réciproquement, une forme linéaire appropriée définit des idempotents $\mathbf{e}^+$ et $\mathbf{e}^-$ associés à deux demi-espaces de $\mathbb{C}^n$. De plus, pour tout polytope de $\mathbb{C}^n$ défini par des intersections de demi-espaces, on peut calculer une famille de polynômes dont le produit est associé au polytope. En particulier, toute boîte est déterminée par $4^n$ équations linéaires et les idempotents associés à la boîte par $4^n$ applications de l'algorithme 5.3.25. Focalisons-nous maintenant sur le cas de boîtes presque plates contenant l'ensemble des réels $\mathbb{R}^n = \{\mathbf{x} \in \mathbb{C}^n \mid \mathrm{im}(x_i) = 0, \forall i \in \{1, \ldots, n\}\}$. Dans ce cas, le choix de $h = x_i - \epsilon$ et $h = x_i + \epsilon$ conduit à l'approximation des idempotents suivants :

$$\mathbf{e}^-_{i,\epsilon} = \sum_{\mathrm{im}(\zeta) > -\epsilon} \mathbf{e}_\zeta \text{ et } \mathbf{e}^+_{i,\epsilon} = \sum_{\mathrm{im}(\zeta) < \epsilon} \mathbf{e}_\zeta.$$

Leurs produits peut être calculé en $\mathcal{O}(3^n D^2 \log(3^n D))$ opérations arithmétiques et conduit aux polynômes $\mathbf{r}_{i,\epsilon} = \sum_{|\mathrm{im}(\zeta)| < 0} \mathbf{e}_\zeta$, $\forall i \in \{1, \ldots, n\}$. Le produit $\mathbf{r}_\epsilon = \mathbf{r}_{1,\epsilon} \cdots \mathbf{r}_{n,\epsilon}$ peut être calculer en $\mathcal{O}(3^n D^2 \log(3^n D))$ opérations arithmétiques. Cela conduit à la somme des idempotents du système fondamental d'idempotents associé aux racines proches d'une valeur purement réelle. On considère alors l'algorithme suivant, qui permet de calculer cette somme :

**Algorithme 5.3.28 (Somme d'idempotents)**

*Entrée :* *Une valeur* $\epsilon > 0$.

- *Pour $i$ allant de 1 à $n$ faire*
  - $u_0 = x_i \pm \epsilon$.
  - $u_1 = \frac{1}{2}(u_0 - \frac{1}{u_0}$, $k = 1$.
  - *Tant que* $\|u_k - u_{k-1}\| > 2^{-b}$ *faire*

$$\left\{ u_{k+1} = \frac{1}{2}(u_k + \frac{1}{u_k}) \text{ et } k = k + 1. \right\}$$

  - *Calculer* $\mathbf{e}_{i,\epsilon}$ *et* $\mathbf{r}_{iu,\epsilon}$.
- *Sortie :* *Retourner la valeur* $\mathbf{r}_\epsilon = \mathbf{r}_{1,\epsilon} \cdots \mathbf{r}_{n,\epsilon}$.

Avec les résultats de la sous-section précédente on obtient facilement la proposition suivante :

**Proposition 5.3.29**
*Une approximation $\mathbf{r}_\epsilon$ de $\mathbf{r}$ avec une erreur de l'ordre de $\epsilon = 2^{-b}$ peut être calculée en $\mathcal{O}(\mu 3^n D^2 \log(3^n D))$ opérations arithmétiques, où :*

$$\mu = \mu(b, \rho) = \log |b / \log(\rho)|,$$

*et :*

$$\rho = max \left\{ \begin{array}{c} max\left\{|\frac{\zeta_i+\mathbf{i}}{\zeta_i-\mathbf{i}}| \mid \zeta \in Z(\mathcal{I}), im(\zeta_i) > 0\right\}, \\ max\left\{|\frac{\zeta_i-\mathbf{i}}{\zeta_i+\mathbf{i}}| \mid \zeta \in Z(\mathcal{I}), im(\zeta_i) < 0\right\} \end{array} \right\}$$

.

### Méthode de Sebastio e Silva

On propose maintenant une extension au cas multivarié d'une méthode itérative déjà connue dans le cas univarié, proposée par J. Sebastio e Silva dans [88], reprise par J. P. Cardinal dans [26] et connue en analyse matricielle sous le mon de méthode des carrés itérés [53]. L'algorithme est le suivant :

**Algorithme 5.3.30 (Carrés itérés)**

*Entrée :* $u_0 = h \in \mathcal{A}$.

- $u_1 = \frac{u_0^2}{\|u_0^2\|}$, $k = 1$.
- *Tant que* $\|u_k - u_{k-1}\| > 2^{-b}$ *faire*

$$u_{k+1} = \frac{u_k^2}{\|u_k^2\|} \textit{ et } k = k + 1.$$

*Sortie :* *Retourner* $u_k$.

Chaque itération de l'algorithme nécessite $\mathcal{O}(3^n D^2 \log(3^n D))$ opérations arithmétiques et on a la propriété suivante :

**Proposition 5.3.31**
*Soit $h \in \mathcal{A}$, on suppose qu'il existe une unique racine $\zeta$ maximisant $|h|$. On peut approximer l'idempotent $\mathbf{e}_\zeta$, avec une précision en $2^{-b}$, en $\mathcal{O}(\nu 3^n D^2 \log(3^n D))$ opérations arithmétiques, où :*

$$\nu = \nu(b, \gamma) = \frac{b}{|\log(\gamma)|}$$
$$\gamma = \frac{|h(\zeta|}{|\zeta'|}$$

*$\zeta'$ étant une racine minimisant $|h|$ sur $Z(\mathcal{I})$.*

*Preuve :* Il s'agit de l'analyse de la convergence pour la méthode des carrés itérés appliquée à la matrice de multiplication par $u_i$ dans $\mathcal{A}$ dont les valeurs propres sont $\{u_i(\zeta) = h(\zeta)^i | \zeta \in Z(\mathcal{I})\}$. ♣

### 5.3.7 Compter et approximer les racines réelles et complexes

On s'intéresse maintenant à l'application des méthodes que nous venons d'exposer pour compter et approximer les racines complexes et réelles d'un système algébrique.

L'algorithme pour compter les racines est un algorithme probabiliste basé sur la proposition 5.3.18. Cet algorithme est utilisé pour compter le nombre de racines d'un système algébrique de dimension zéro.

L'algorithme pour l'approximation des solutions n'est pas probabiliste (si le jacobien du polynôme $h$ choisi ne s'annule pas aux solutions), mais la complexité dépend des $\rho$ et $\gamma$ (précédemment définis), ce qui demeure un facteur gênant lorsque ces valeurs sont proches de 1.

#### Compter les racines complexes et réelles

Le théorème suivant est extrait de [78] :

**Théorème 5.3.32**
*Le nombre de racines (resp. de racines réelles) d'un système algébrique est donné par le rang (resp. par la signature) de la matrice quasi-Hankel* $H_\tau^E$ .

En corollaire de ce théorème et des résultats de complexités précédents, on obtient :

**Corollaire 5.3.33**
*Le nombre de racines et de racines réelles d'un système algébrique peut être calculé par un algorithme probabiliste générant $D$ paramètres aléatoires et réalisant $\mathcal{O}(3^n D^2 \log(3^n D))$ opérations arithmétiques. Si les paramètres proviennent d'un ensemble fini $S$, alors la probabilité d'échec est d'au plus* $\frac{(3^n D+1)3^n D}{2\#(S)}$.

#### Approximation d'une racine

**Théorème 5.3.34**
*L'idempotent associé à la racine $\zeta$ maximisant $|h|$, où $h \in \mathcal{A}$, peut être calculé, avec une précision en $2^{-b}$, avec $\mathcal{O}(\nu 3^n D^2 \log(3^n D))$ opérations arithmétiques, où $\nu$ est définie dans la proposition 5.3.31.*

La complexité de la reconstruction des coordonnées de $\zeta$ à partir de l'idempotent $\mathbf{e}_\zeta$ est donnée par le théorème suivant :

**Théorème 5.3.35**
*Les $n$ coordonnées d'une racine $\zeta$ simple peuvent être déterminées de la*

*connaissance de $\mathbf{e}_\zeta$ en $\mathcal{O}(3^n D^2 \log(3^n D))$ opérations arithmétiques. Ce coût est multiplié par $n$ si la racine est multiple.*

*Preuve :* On note $\mathbf{f}$ le système algébrique à résoudre. On calcule $Jac_{\mathbf{f}}\mathbf{e}_\zeta \in \mathcal{A}$. D'après [78] dans le cas d'une racine simple, on a :

$$H_\tau^E[Jac_{\mathbf{f}}\mathbf{e}_\zeta]_x = \lambda[\zeta^\alpha]_{\alpha\in E}$$

ce qui peut être calculé avec la complexité annoncée. Cela donne immédiatement les coordonnées de $\zeta$ si $\mathbf{x}^E$ contient $1, x_1, \ldots, x_n$, ce qui est généralement le cas. Si la racine est multiple on utilise la relation :

$$x_i Jac_{\mathbf{f}}\mathbf{e}_\zeta = \zeta_i Jac_{\mathbf{f}}\mathbf{e}_\zeta$$

et on obtient les coordonnées de $\zeta$ par $n+1$ multiplications dans $\mathcal{A}$. ♣

### Approximation d'une racine sélectionnée

D'après le théorème 5.3.35, il suffit d'approximer l'idempotent associé à la racine voulue.

Supposons qu'on souhaite calculer la valeur d'une racine de $\mathbf{f} = 0$ dont la coordonnée $x_i$ est la plus proche d'une valeur $u$ donnée. Supposons que $u$ n'est pas la coordonnée d'une racine, si bien que $x_i - u$ est inversible dans $\mathcal{A}$. Notons $h(\mathbf{x})$ cet inverse. On a $h(\mathbf{x})(x_i - u) \equiv 1$ et $h(\zeta) = \frac{1}{\zeta_1 - u}$. La racine $\zeta$ maximise donc $|h|$. On applique alors la méthode de Sebastio e Silva.

Le polynôme $h$ peut être calculé en $\mathcal{O}(3^n D^2 \log(3^n D))$ opérations arithmétiques et $\mathbf{e}_\zeta$ en $\mathcal{O}(\nu 3^n D^2 \log(3^n D))$ opérations arithmétiques, où $\nu$ est définie dans la proposition 5.3.31. On peut également calculer plusieurs racines à partir de plusieurs valeurs de $u$ distinctes.

### Compter les racines réelles et celles contenues dans un polytope

Si on connaît une approximation de l'idempotent $\mathbf{r}$ associé à un polytope, on peut connaître le nombre de racines contenues dans ce polytope en remplaçant, dans le calcul du nombre de racines, la forme linéaire $\tau$ par $\mathbf{r}\tau$ (ce qui implique $\mathcal{O}(3^n D^2 \log(3^n D))$ opérations arithmétiques). Considérons maintenant le cas où le polytope est une petite boîte plate approximant $R^n$.

Soit $\mathcal{A}_\epsilon^{\mathbb{R}} = \mathbf{r}_\epsilon \mathcal{A}$ la sous-algèbre de $\mathcal{A}$ correspondant aux idempotents associés aux racines dont la partie imaginaire est inférieure ou égale à $\epsilon = 2^{-b}$.

On note $\tau' = \mathbf{r}_\epsilon \tau$, on a la proposition suivante :

**Proposition 5.3.36** • *la forme linéaire $\tau'$ définit une forme bilinéaire non-dégénérée sur $\mathcal{A}_\epsilon^{\mathbb{R}}$,*

- *le nombre de racines dont la partie imaginaire est inférieure à* $\epsilon = 2^{-b}$ *est le rang de la matrice* $H^E_{\mathbf{r}_\epsilon * \tau} = (\tau(\mathbf{r}_\epsilon x^{\alpha+\beta}))_{\alpha,\beta \in E}$,
- *Soit* $E'$ *un sous-ensemble de* $E$ *tel que la sous-matrice* $H^{E'}_{\tau'}$ *soit de rang plein, alors* $\mathbf{x}^{E'}$ *est une famille libre de* $\mathcal{A}_\epsilon$*, de plus si* $\#(E')$ *est égale au rang de la matrice* $H^E_{\mathbf{r}_\epsilon * \tau}$ *et si le système n'a que des racines simples alors* $\mathbf{x}^{E'}$ *est une base de* $\mathcal{A}_\epsilon$.

*Preuve* : Voir [78]. ♣

**Proposition 5.3.37** *Le calcul du nombre de racines dont la partie imaginaire est inférieure à* $2^{-b}$ *peut se faire en* $\mathcal{O}(\mu 3^n D^2 \log(3^n D))$ *opérations arithmétiques, où* $\mu$ *est défini dans la proposition 5.3.29.*

### Approximation d'une racine presque réelle ou d'une racine contenue dans une boîte

Pour approximer une racine réelle ou une racine contenue dans une boîte de $\mathbb{C}^n$ maximisant $|h|$, où $h \in \mathcal{A}$, on applique l'algorithme 5.3.30 dans $\mathcal{A}$ (ou $\mathcal{A}^{\mathbb{R}}_\epsilon$) et par la proposition 5.3.31 on obtient :

**Théorème 5.3.38**
*Une approximation d'une racine presque réelle ou contenue dans une boîte, maximisant* $|h|$ *peut être obtenue en* $\mathcal{O}((\mu + \nu) 3^n D^2 \log(3^n D))$ *opérations arithmétiques, où* $\mu$ *et* $\nu$ *sont définis dans la proposition 5.3.31.*

On peut utiliser ce processus pour calculer les autres racines par déflation : on remplace $\mathbf{r}_\epsilon$ par $\mathbf{r}'_\epsilon = \mathbf{r}_\epsilon + \mathbf{e}_\zeta$ et on calcule $\tau'' = \mathbf{r}'_\epsilon * \tau$, puis on applique la même itération pour calculer la racine maximisant $|h|$ en dehors de $\zeta$. On peut également se restreindre aux racines contenues dans une boîte. La complexité de chaque pas est donnée par le théorème 5.3.38, ce qui donne le résultat suivant pour le calcul des $\delta$ racines (réelles) contenues dans une boîte :

**Théorème 5.3.39** *Les* $\delta$ *racines (réelles) contenues dans une boîte donnée (avec une précision en* $2^{-b}$*) peut être approximées en* $\mathcal{O}(\delta(\mu+\nu) n 3^n D^2 \log(D) \log(b))$ *opérations arithmétiques.*

# Chapitre 6

# Conclusion

Dans cette thèse nous avons montré que la dualité est un outil puissant qui nous a permis de traiter de façon effective les problèmes suivants :

- Au chapitre 2, nous avons traité la représentation des algèbres de dimension zéro et donné des formules d'interpolation explicites.
- Au chapitre 3, nous avons utilisé notre travail sur la représentation des algèbres de dimension zéro pour construire des fonctions d'itération pour le calcul simultané de toutes les racines d'un système algébrique. Nous avons dérivé de ces fonctions d'itération des méthodes dont nous avons montré qu'elles sont efficaces expérimentalement.
- Au chapitre 4, nous nous sommes intéressés aux algèbres de Gorenstein et plus particulièrement aux intersections complètes où nous avons vu que les bézoutiens et les résidus algébriques permettent d'obtenir des algorithmes pour la géométrie algébrique effective.
- Enfin, au chapitre 5, nous avons montré comment l'utilisation du résidu et des matrices structurées permet de développer des algorithmes itératifs avec de bonnes complexités asymptotiques.

Un aspect important, à nos yeux, est que la dualité éclaircit la structure des algèbres quotients. Une bonne compréhension de cette structure permet l'interpolation et l'approximation. Un des problèmes de notre approche est l'utilisation de matrices de type Vandermonde. On peut penser à d'autres bases d'interpolation que la base des idempotents pour éviter cet inconvénient. Cela permettrait sans doute de stabiliser le comportement numérique des algorithmes d'approximation que nous avons proposés. L'étude théorique des méthodes de calcul simultané des racines d'une équation ou d'un système algébrique n'est pas encore complètement comprise. Nous espérons que l'interprétation géométrique de ces méthodes, que nous proposons au chapitre 3, conduira à une meilleure compréhension de leurs comportements globaux. Des généralisations d'autres méthodes itératives sont envisageables. De plus, l'interpolation algébrique intervient dans d'autres cadres que l'approximation de racines. Cela ouvre beaucoup de perspectives aux méthodes que nous avons étudiées.

# Bibliographie


[1] L.A. Aizenberg and A. M. Kytmanov. Multdimensional analogues of newtons formulas for systems of nonlinear algebraic equations and some of their applications. *Trans. from Sib. Mat. Zhurnal*, 22(2) :19–39, 1981.

[2] Eugene L. Allgower and Kurt Georg. *Numerical Path Following*. Springer, 1990.

[3] Franck Aries and Rachid Senoussi. An implicitization algorithm for rational surfaces with no base points. *Journal of Symbolic Computation*, pages 357–365, 2001.

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

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

[6] W. Auzinger and H. J. Stetter. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. In *Proc. Intern. Conf. on Numerical Math.*, volume 86 of *Int. Series of Numerical Math*, pages 12–30. Birkhäuser Verlag, 1988.

[7] E. Becker, J.P. Cardinal, M.F. Roy, and Z. Szafraniec. Multivariate Bezoutians, Kronecker symbol and Eisenbud-Levin formula. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications*, volume 143 of *Prog. in Math.*, pages 79–104. Birkhäuser, Basel, 1996.

[8] Anne-Mercedes Bellido. Construction de fonction d'itération pour le calcul simultan é des racines d'une équation $f(s)$. *C.R. Acad. Sci. Paris*, 1992.

[9] Anne-Mercedes Bellido. *Construction de fonctions d'itération pour le calcul simulta né des solutions d'équations et de systèmes d'équations algébriques.* PhD thesis, Université Paul Sabatier de Toulouse, 1992.

[10] Anne-Mercedes Bellido. Construction of iteration functions for the simultaneous computation of the solutions of equations and algebraic systems. *Numerical Algorithms*, 6 :313–351, 1994.

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

[12] C.A. Berenstein and A. Yger. Residue calculus and Effective Nullstellensatz. *Amer. J. Math.*, 121, 1999.

[13] D. Bini. Numerical computation of polynomial zeros by means of aberth's method. *Numerical Algorithms*, 13, 1996.

[14] D. Bini and G Fiorentino. Adaptative multiprecision algorithm for univariate polynomial zeros. In Computational Mechanics Publication, editor, *Proc. of the First International MATHEMATICA Symposium*, pages 53–60, Southampton, 1995.

[15] D. Bini and V. Pan. *Polynomial and matrix computations.* Progress in Theoretical Computer Science. Birkhäuser Verlag, 1994.

[16] D. Bini and V. Y. Pan. *Polynomial and matrix computations, Vol 1 : Fundamental Algorithms.* Birkhäuser, Boston, 1994.

[17] L. Blum, F. Crucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer, 1998.

[18] D. Bondyfalat, B. Mourrain, and V. Y. Pan. Controlled iterative methods for solving polynomial systems. In O. Gloor, editor, *Proc. Intern. Symp. on Symbolic and Algebraic Computation*, pages 252–259. NewYork, ACM Press., 1998.

[19] D. Bondyfalat, B. Mourrain, and V. Y. Pan. Computation of a specified root of a polynomials system of equations using eigenvector. *Lin. Alg. and its Appl.*, 319 :193–209, 2000.

[20] B. Buchberger. *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (German).* PhD thesis, Math. Inst, Univ. of Innsbruck, Austria, 1965. (also in Aequationes Math. 4/3, 1970).

[21] L. Busé. Residual resultant over the projective plane and the implicitization problem. *proceedings ISSAC2001*, pages 48–55, 2001.

[22] L. Busé, M. Elkadi, and B. Mourrain. Generalized resultant over unirational algebraic varieties. *J. of Symbolic Computation*, 29 :515–526, 2000.

[23] J. Canny. *The Complexity of Robot Motion Planning.* M.I.T. Press, Cambridge, Mass., 1988.

[24] J. Canny and J.M. Rojas. An optimal condition for determining the exact number of roots of a polynomial system. In *Proc. ISSAC*, pages 96–102, Bonn, July 1991.

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

[26] J. P. Cardinal. On two iterative methods for approximating the roots of a polynomial. In J. Renegar, M. Shub, and S. Smale, editors, *Proc. AMS-SIAM Summer Seminar on Math. of Numerical Analysis, (Park City, Utah, 1995)*, volume 32 of *Lectures in Applied Math.*, pages 165–188. American Mathematical Society Press, Providence, 1996.

[27] J.P. Cardinal and B. Mourrain. Algebraic approach of residues and applications. In J. Renegar, M. Shub, and S. Smale, editors, *Proc. AMS-SIAM Summer Seminar on Math. of Numerical Analysis, (Park City, Utah, 1995)*, volume 32 of *Lectures in Applied Math.*, pages 189–210. American Mathematical Society Press, Providence, 1996.

[28] D. Castro, K. Hägele, J.E. Morais, and L.M. Pardo. Kronecker and newton approaches to solving : A first comparaison. *Journal of Complexity*, 16(1), 2000.

[29] R.M. Corless, P.M. Gianni, B.M. Trager, and S.M. Watt. The singular value decomposition for polynomial systems. In A.H.M Levelt, editor, *Proc. ISSAC*, pages 195–207, 1995.

[30] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer Verlag, New York, 1992.

[31] David A. Cox, Ronald Goldman, and Zhang Ming. On the validity of implicitization by moving quadrics for rationnal surfaces with no base points. *J. Symbolic Computation*, 29, 2000.

[32] Carlos D'Andrea. Resultants and moving surfaces. *Journal of Symbolic Computation*, 31 :585–602, 2001.

[33] C. de Boor and A. Ron. On multivariate polynomial interpolation. *Constructive Approximation*, 6 :287–302, 1990.

[34] T. Dokken. Approximate implicitization. *Math. Methods in CAGD ; Oslo*, 2001.

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

[36] M. Elkadi and B. Mourrain. Some applications of bezoutians in effective algebraic geometry. Rapport de Recherche 3572, INRIA, Sophia Antipolis, 1998.

[37] M. Elkadi and B. Mourrain. A new algorithm for the geometric decomposition of a variety. In S. Dooley, editor, *Proc. Intern. Symp. on Symbolic and Algebraic Computation*, pages 9–16. ACM Press, New-York, 1999.

[38] M. Elkadi and B. Mourrain. Algorithms for residues and Lojasiewicz exponents. *J. of Pure and Applied Algebra*, 153 :27–44, 2000.

[39] M. Elkadi and B. Mourrain. Introduction à la résolution des systèmes d'équations algébriques, 2002. Notes de cours, DEA de Mathématiques, Univ. de Nice.

[40] I.Z. Emiris and B. Mourrain. Matrices in Elimination Theory. *J. of Symbolic Computation*, 28(1&2) :3–44, 1999.

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

[42] J.-C. Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero ($f_5$). In Teo Mora, editor, *International Symposium on Symbolic and Algebraic Computation 2002*, pages 75–83, 2002.

[43] J.C. Faugère. A new efficient algorithm for computing Gröbner Basis (F4). *J. of Pure and Applied Algebra*, 139 :61–88, 1999.

[44] S. Fortune. Polynomial root finding using iterated eigenvalue computation. In B. Mourrain, editor, *Proc. ISSAC*, pages 121–128. New-York, ACM Press., 2001.

[45] FRISCO (Framework for the Integration of Symbolic-Numeric Computing). ESPRIT Long Term Research Project 21.024. `http ://extweb.nag.co.uk/projects/FRISCO.html`.

[46] A. Frommer. A unified approach to methods for the simultaneous computation of all zeros of generalized polynomials. *Numer. Math.*, 54 :105–116, 1988.

[47] P.A. Fuhrmann. *A polynomial approach to linear algebra.* Springer-Verlag, 1996.

[48] A. Galligo and S.M. Watt. A numerical absolute primality test for bivariate polynomials. In *Proc. ISSAC*, pages 217–224, 1997.

[49] N Gasca and T. Sauer. On the history of multivariate polynomial interpolation. *Advances in Computational and Applied Mathematics*, 122 :23–35, 2000.

[50] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In *Proc Int. Meeting on Commutative Algebra*, volume XXXIV of *Symp. Mathematica*, pages 216–255, Cortona,1991.

[51] M. Giusti, Heintz. J, Morais. J.E, J. Morgenstern, and Pardo L.M. Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124(1-3) :101–146, 1998.

[52] Marc Giusti, Grégoire Lecerf, and Bruno Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1) :154–211, 2001.

[53] G.H. Golub and C.F. Van Loan. *Matrix computations.*, volume XVI. Oxford : North Oxford Academic, 1983.

[54] L. Gonzalez-Vega. Implicitization of parametric curves and surfaces by using multidimensional newton formulae. *J. Symbolic Comput.*, 23, 1997.

[55] L. Gonzalez-Vega and Trujillo G. Implicitization of parametric curves and surfaces by using symetric functions. *ISSAC'95, ACM Press*, pages 180–186, 1995.

[56] L. González-Vega and G. Trujillo. Using symmetric functions to describe the solution of a zero dimensional ideal. In G. Cohen, M. Giusti, and T. Mora, editors, *AAECC'95*, volume 948 of *LNCS*, pages 232–247. Springer-Verlag, 1995.

[57] Ph. Griffiths and J. Harris. *Principles of Algebraic Geometry.* Wiley Interscience, New York, 1978.

[58] P. Henrici. *Applied and Computational Complex Analysis*, volume I. Wiley, 1988.

[59] C.M. Hoffmann. *Geometric and Solid Modeling.* Morgan Kaufmann, 1989.

[60] T. Kailath and A. H. Sayed, editors. *Fast Reliable Algorithms for Matrices with Structure.* Society for Industrial and Applied Mathematics (SIAM), Philadelphia, 1999.

[61] L. Kronecker. Über einige inetrpolationsformeln für ganze funktionen mehrerer variabeln. In *Kronecker Werke*, volume I, pages 133–141. H. Hensel. Lecture at the Academy of sciences, December 21, 1865.

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

[63] A. Lascoux. Inversion des matrices de Hankel. *Linear Algebra and Its Applications*, 129 :77–102, 1990.

[64] Alain Lascoux. The newton interpolation formula, with more variables. http ://phalanstere.univ-mlv.fr/ al/, 2001.

[65] Alain Lascoux. Note on interpolation in one and several variables. http ://schubert.univ-mlv.fr/ al/, 2001.

[66] D. Lazard. Résolution des systèmes d'équations algébriques. *Theo. Comp. Science*, 15 :77–110, 1981.

[67] T.Y. Li. Numerical solution of multivariate polynomial systems by homotopy continuation methods. *Acta Numerica*, 6 :399–436, 1997.

[68] Sandra Liccardi and Teo Mora. Implicitization of hypersurfaces and curves by the primbasissatz and basis conversion. *proceding ISSAC 94*, pages 191–196, 1994.

[69] G.G. Lorentz and R.A. Lorentz. Bivariate hermite interpolation and application to algebraic geometry. *Numerish Mathematik*, 1990.

[70] D. Manocha. *Algebraic and Numeric Techniques for Modeling and Robotics*. PhD thesis, Comp. Science Div., Dept. of Electrical Engineering and Computer Science, Univ. of California, Berkeley, May 1992.

[71] D. Manocha and J. Canny. The impicit representation of rational parametric surfaces. *J. Symbolic Computation*, 13 :485–510, 1992.

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

[73] B. Mourrain. Isolated points, duality and residues. *J. of Pure and Applied Algebra*, 117 & 118 :469–493, 1996. Special issue for the Proc. of the 4th Int. Symp. on Effective Methods in Algebraic Geometry (MEGA).

[74] B. Mourrain. A new criterion for normal form algorithms. In M. Fossorier, H. Imai, Shu Lin, and A. Poli, editors, *Proc. AAECC*, volume 1719 of *LNCS*, pages 430–443. Springer, Berlin, 1999.

[75] B. Mourrain and V. Y. Pan. Multidimensional structured matrices and polynomial systems. *Calcolo, Special Issue for the workshop : Structure, Algorithms and Applications*, 33 :389–401, 1997.

[76] B. Mourrain and V. Y. Pan. Solving special polynomial systems by using structured matrices and algebraic residues. In F. Cucker and M. Shub, editors, *Foundations of Computational Mathematics (Rio de Janeiro)*, pages 287–304. Springer-Verlag, 1997.

[77] B. Mourrain and V. Y. Pan. Asymptotic acceleration of solving multivariate polynomial systems of equations. In *Proc. STOC*, pages 488–496. ACM Press., 1998.

[78] B. Mourrain and V. Y. Pan. Multivariate polynomials, duality and structured matrices. *J. of Complexity*, 16(1) :110–180, 2000.

[79] B. Mourrain, Y. V. Pan, and O. Ruatta. Asymptotic acceleration of solving multivariate polynomial systems of equations. Fondation of Computational Mathematics, pages 267–294. World Scientific, NewJersey, London, Singapore, Hong Kong, 2002.

[80] B. Mourrain and O. Ruatta. Relation between roots and coefficients, interpolation and application to system solving. *JSC*, 2002.

[81] B. Mourrain and Ph. Trébuchet. Solving projective complete intersection faster. In C. Traverso, editor, *Proc. Intern. Symp. on Symbolic and Algebraic Computation*, pages 231–238. New-York, ACM Press., 2000.

[82] B. Mourrain and Ph. Trébuchet. Algebraic methods for numerical solving. In *Proc. of the 3rd International Workshop on Symbolic and Numeric Algorithms for Scientific Computing'01 (Timisoara, Romania)*, 2002.

[83] Bernard Mourrain, Victor Y. Pan, and Olivier Ruatta. Assymptotic acceleration of solving multivariate polynomial systems of equations. In *Fondation of Computational Mathematics*, pages 267–294. World Scientific, NewJersey, London, Singapore, Hong Kong, 2002.

[84] F. Rouillier. Solving zero-dimensional polynomial systems throuhg Rational Univariate Representation. Technical Report 3426, INRIA, Lorraine, France, May 1998.

[85] O. Ruatta. A multivariate weierstrass iterative rootfinder. In B. Mourrain, editor, *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 276–283, London, Ontario, 2001. New-York, ACM Press.

[86] T. Sauer. Algebraic aspects of polynomial interpolation in several variables. *Journal of Approximation Theory*, IX, 2002. K. Chui and L. Schumaker (Ed .).

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

[88] J Sebastiao e Silva. Sur une méthode d'approximation semblable à celle de Graeffe. *Portugal Math. J.*, 2 :271–279, 1941.

[89] S. Smale. The fundamental theorem of algebra and complexity theory. *Bull. Amer. Math. Soc.*, 4(1) :1–36, 1981.

[90] H.J. Stetter. Principles of numerical polynomial algebra. In *Proc. Workshop Symbolic on Symbolic-Numeric Algebra for Polynomials (SNAP-96)*, Sophia-Antipolis, France, July 1996.

[91] A. K. Tsikh. *Multidimensional residues and their applications.* Number 103 in Translations of Mathematical Monographs. American Mathematical Society, 1992. Translated from the 1988 Russian original by E. J. F. Primrose.

[92] M. Van Barel and A. Bultheel. A lookahead algorithm for the solution of block toeplitz systems. *@LAA*, 266 :291–335, 1997.

[93] B.L. van der Waerden. *Modern Algebra.* F. Ungar Publishing Co., New York, 3rd edition, 1950.

[94] J. Verschelde. Toric newton method for polynomial homotopies. *J. Symb. Comput.*, 29(4 and 5) :777–793, 2000.

[95] J. Verschelde and R. Cools. Symbolic homotopy construction. *J. Applied Algebra to Engineering and Code-Correcting*, 4(3) :169–183, 1993.

[96] J. Verschelde, P. Verlinden, and R. Cools. Homotopies exploiting Newton polytopes for solving sparse polynomial systems. *SIAM J. Numerical Analysis*, 31(3) :915–930, 1994.

[97] J. von zur Gathen. Algebraic complexity theory. In J. Traub, editor, *Annual Review of Computer Science*, pages 317–347. Annual Reviews, Palo Alto, Cal., 1988.

## Dualité algébrique, structures et applications

Dans cette thèse nous nous intéressons aux structures des algèbres quotients et plus particulièrement à l'apport de la dualité pour la représentation des algèbres de coordonnées.

Une première partie de cette thèse est consacrée à la représentation des algèbres de dimension zéro et à des applications de la dualité à des problèmes d'interpolation. Nous généralisons les bases d'interpolation de Lagrange et d'Hermite pour lesquelles nous donnons des formules explicites. Cela nous permet de donner les relations entre les racines d'un système algébrique et ses coefficients avec des formules généralisant celles du cas univarié.

Dans une deuxième partie, nous appliquons les résultats développés dans la première partie à la conception de méthodes itératives pour l'approximation simultanée de l'ensemble des solutions d'un système algébrique.

La troisième partie est consacrée aux résidus algébriques. Nous rappelons les notions relatives aux algèbres de Gorenstein et à leurs représentations. Nous introduisons les bézoutiens et les résidus algébriques dont nous donnons des applications en géométrie.

Dans la quatrième partie, nous nous intéressons à l'algorithmique associé aux matrices quasi-Toeplitz, quasi-Hankel, ..., telles que définies par B. Mourrain et V.Y. Pan. Nous en montrons des applications dans le cadre de l'algorithmique permettant des accélérations asymptotiques de méthodes de résolution de systèmes algébriques.

**Mots Clés :** Algèbre et géométrie effectives, algorithmique, dualité, représentations, interpolation polynomiale multivariée, résidus, bézoutiens, méthodes symboliques-numériques, méthodes itératives.

## Algebraic duality, structures and applications

In this thesis we are interested in quotient algebra structures and more specifically in contributions of duality theory to representation theory of coordinate algebras of zero-dimensional algebraic sets.

The first part of the text is dedicated to representation theory of zero dimensional algebras and to interpolation problems. We generalize Lagrange and Hermite interpolation bases and give explicit formulae for them. In this framework we give closed formulae linking the roots of an algebraic system and its coefficients.

In a second part, we apply those results to the design of iterative methods for simultaneous approximation of all roots of algebraic systems.

The third part is dedicated to algebraic residues, their computational aspects and applications.

In the last part, we are interested in algorithms linked to quasi-Toeplitz, quasi-Hankel, . . . matrices as defined by B. Mourrain and V.Y. Pan. We show applications of such algorithms to asymptotic accelerations of iterative methods to solve algebraic systems.

**Key words :** Effective algebra and geometry, algorithms, duality, representation theory, multivariate interpolation, residues, bézoutians, symbolic-numeric methods, itérative methods.