UNIVERSITÉ DE LIMOGES
ÉCOLE DOCTORALE Science - Technologie - Santé
FACULTÉ des Sciences et Techniques

XLIM - **D**épartement de **M**athématiques et **I**nformétique

Thèse

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Discipline : Mathématiques et Applications Spécialité : Calcul formel

Présentée et soutenue
par

Hassan El Houari

Le 17 Octobre 2007

Algorithms for locally nilpotent derivations in dimension two and three

Thèse dirigée par Moulay A. Barkatou et M'hammed El Kahoui

Jury

Président :			
Abdelilah Kandri-Rody	Professeur	Université Cadi Ayyad	Marrakech
Rapporteurs :			
Abdeslam Mimouni	Professeur	Université du Roi Fahd	Arabie Saoudite
Vladimir Shpilrain	Professeur	City College	New York
Examinateurs :			
Moulay A. Barkatou	Professeur	Université de Limoges	Limoges
M'hammed El Kahoui	Professeur	Université Cadi Ayyad	Marrakech
André Galligo	Professeur	Université de Nice	Nice
Lahoucine Izelgue	Professeur	Université Cadi Ayyad	Marrakech
Henri Lombardi	Professeur	Université de Franche-Comté	Besançon

This work is a joint supervision thesis between
Limoges University and Cadi Ayyad University in Moroccco,
It has been performed in four years from September 2003 to October 2007
under the joint direction of Professor Moulay A. Barkatou (Limoges University) and
Professor M'hammed El Kahoui (Cadi Ayyad University).

Acknowledgements

First of all, I would like to express my respectful gratitude and appreciation to my advisor Professor M'hammed El Kahoui, whose efforts and support made this dissertation possible. I am indebted for his constant assistance, encouragement, supervision and the tremendous support during the period of this work. He has been to me the best advisor I could imagine.

A special word of thanks goes to Professor Moulay A. Barkatou for providing insight, guidance, and friendship, as well as from many discussions throughout my stay at Limoges. Thank you Moulay.

I wish to express my gratitude to professors Lahoucine Izelgue, Abdeslam Mimouni and Vladimir Shpilrain for agreeing to be referees of this work. Their remarks and painstaking efforts to improve the quality of this work are greatly appreciated.

It is a great honor for me to see among the jury members Professors Abdelelah Kandri-Rody, André Galligo and Henri Lombardi. I am profoundly indebted to them for the time and energy which they have spent on my PhD defense.

I would like to thank all professors, who have taught me mathematics, especially, Professors Salah Eddine Labhalla, Driss Bouziane and Brahim Sadik for their courses during DESA.

I also would like to thank all the staff of departments of mathematics in Cadi Ayyad University as well as in Limoges University for their sympathy and the way they have contributed to facilitate administrative tasks for me.

Recognition must be given to my colleagues for their generous support and special working atmosphere while doing my thesis. Many thank also to my friends for their good will and warm encouragements. I wish them both the best of luck.

Finally, and most importantly, my deep gratitude goes to my family, particulary my Mother, Without their continuous encouragement, support and understanding, it would have been impossible for me to accomplish all of my study.

I am dedicating this work to the loving memory of my father,
Mohammed El Houari, who died on
3 October 1991.

Contents

Introduction

Let $\mathcal{A}$ be a commutative ring with unity and $\mathcal{X}$ be a derivation of $\mathcal{A}$. Such derivation is called locally nilpotent if for any element $a \in \mathcal{A}$, there exits an integer n such that $\mathcal{X}^n(a) = 0$. The study of this kind of derivations goes back at least in the middle of the twentieth century. To our knowledge, this came into existence from the areas of Lie theory, invariant theory and differential equations, where the connection between derivations, group actions and vector fields is established.

Nowadays, locally nilpotent derivations have made remarkable progress and became an important topic in understanding affine algebraic geometry and commutative algebra. This is due to its close relation to many classical problems in these areas. For example, the Jacobian Conjecture, which was first formulated by Keller in 1939 [63], asserts that a polynomial map $f = (f_1, \ldots, f_n)$, of the polynomial algebra $\mathbb{C}[x_1, \ldots, x_x]$, is an automorphism if its jacobian $\mathrm{Jac}(f)$ is a nonzero constant. This problem is of great importance in many disciplines, especially algebra, analysis and complex geometry. It is among the eighteen challenging problems for the twenty-first century proposed by Steven Smale [97]. Using the language of locally nilpotent derivations, this problem can easily be formulated as follows:

Let $f_1, \ldots, f_{n-1}$ be polynomials in $\mathbb{C}[x_1, \ldots, x_n]$. If the Jacobian derivation $\mathcal{X}_{f_1,\ldots,f_{n-1}}$ has a slice, i.e., an element s such that $\mathcal{X}_{f_1,\ldots,f_{n-1}}(s) = 1$, then $\mathcal{X}_{f_1,\ldots,f_{n-1}}$ is locally nilpotent and its ring of constants is $\mathbb{C}[f_1, \ldots, f_{n-1}]$.

In spite of many advances in attempt to solve this problem, it is still a big mystery, even for the two dimensional case. Over the last years, many incorrect proofs have been given to this problem, the last one was given by Carolyn Dean in 2004. One of the encouraging results in order to simplify this problem is the reduction given in [101, 8]. It was proved that it suffices to investigate the Jacobian Conjecture for polynomial mappings of the form $f = x + h$ with $\mathrm{Jac}(h)$ nilpotent and h homogeneous of degree three. In this perspective, the three-dimensional Jacobian Conjecture has been solved for all homogeneous polynomial maps of the form $x + h$, where h is homogeneous of degree greater or equal to two, for more details see [79].

Another example, in which locally nilpotent derivations can be used, is the Cancellation Problem. This problem asks whether every complex algebraic variety $\mathcal{V}$ satisfying $\mathcal{V} \times \mathbb{C} \cong_{\mathbb{C}} \mathbb{C}^n$ is isomorphic to $\mathbb{C}^{n-1}$. In terms of locally nilpotent derivations, this problem can also be interpreted as follows:

Given a locally nilpotent derivation $\mathcal{X}$ of $\mathbb{C}[x_1, \ldots, x_n]$ having a slice, does it follow that s is a coordinate ? i.e., s is the image of x_1 under an automorphism of $\mathbb{C}[x_1, \ldots, x_n]$.

The cancellation problem has been first posed by Zariski in 1942, and since then it has been proven for the case two variables by Rentschler [87] and for the case three variables by Fujita [55] and Miyanishi-Sugie [80] in the characteristic zero case and by Russell in the case of positive characteristic [89]. However, for $n \geq 4$ it is still unsolved. Recently, Musuda proved that every triangular derivation having a slice, respectively, every locally nilpotent derivation of rank a most 3 having a slice, on the polynomial ring, is a partial derivative, which in particular, gives two new cases in which the Cancellation problem has a positive solution, see [74].

From the above formulation of the cancellation problem, we observe that it is directly related to the recognizing coordinate problem. i.e., recognize polynomials which may be the image of x_1 under an automorphism of $\mathbb{C}[x_1, \ldots, x_n]$. Recognizing and characterizing coordinates one way or another is of crucial importance for various questions in algebraic geometry, especially, in the study of polynomial automorphisms of the affine space. Many researchers, including Drensky, van den Essen, Makar-Limanov, Shpilrain, Yu and other, were working on different aspects of this problem, see for instance [65, 71, 41, 100, 32, 95, 17, 12, 14]. In [77], Maubach proposed a new conjecture concerning coordinates and locally nilpotent derivations called the Commuting Derivations Conjecture. This conjecture asks whether, for $n-1$ commuting linearly independent locally nilpotent derivations $\mathcal{X}_1, \ldots, \mathcal{X}_{n-1}$ over $\mathcal{K}[\underline{x}] := \mathcal{K}[x_1, \ldots, x_n]$, the polynomial f satisfying $\cap \mathcal{K}[\underline{x}]^{\mathcal{X}_i} = \mathcal{K}[f]$ is a coordinate, where $\mathcal{K}$ is a commutative field of characteristic zero. The answer of this question is unknown except for the three dimensional case, which was proved by the same author. As a consequence, and taking into account that the cancellation problem holds for two dimensional case, all coordinates of the form $p(x)y + q(x, z, t)$ in the polynomial ring $\mathcal{K}[x, y, z, t]$ have been described. Later on, El Kahoui in his paper [33], studied the structure of affine unique factorization $\mathcal{K}$-algebras of transcendence degree n without nonconstant units, equipped with $n-1$ commuting linearly independent locally nilpotent derivations, and as a by-product, he showed that the commuting derivations conjecture is equivalent to the weak version of the Abhyankar-Sathaye Conjecture, which asks if a polynomial $f \in \mathcal{K}[\underline{x}]$ satisfying $\mathcal{K}(f)[\underline{x}] \simeq_{\mathcal{K}(f)} \mathcal{K}(f)^{[n-1]}$ is a coordinate in $\mathcal{K}[\underline{x}]$. Shortly after, this relationship allowed van den Essen to announce that any polynomial f in $\mathcal{K}^{[3]}$, which is a coordinate in $\mathcal{K}^{[3+m]}$ for some $m \geq 1$, is a coordinate in $\mathcal{K}^{[3]}$, see [45].

From the algorithmic point of view, the question of deciding whether a given polynomial f is a coordinate, is still completely open for $n \geq 3$. J. Berson, in his thesis [14], constructed a new class of coordinates over a Dedekind domain, and in four variables case, he proposed an algorithm to recognize such coordinates. In case $n = 2$, various algorithms have been given to this problem [38, 18, 19, 95, 17, 13]. For example, in [38], van den Essen used locally nilpotent derivations to give an algorithmic characterization of coordinates in two variables over a field of characteristic zero. A few years after, the same author with Berson treated the same problem replacing the ground field $\mathcal{K}$ by a finitely generated algebra containing the rational numbers [13].

Locally nilpotent derivations can also be used to attack other problems in algebraic geometry and commutative algebra, such as the Embedding Problem, the Linearization Problem, the Fourteenth Problem of Hilbert and the Automorphism Problem. In [42], the cancellation problem, the embedding problem and the linearization problem were discussed and it has been shown how these problems can be related to a special class of locally nilpotent derivations. In fact, for each regular map from $\mathcal{K}^r$ onto $\mathcal{K}^n$, a special triangular derivation has been defined. Then, using these derivations, a characterization of all embeddings of $\mathcal{K}^r$ in $\mathcal{K}^n$ has been given. This characterization asserts that a regular map from $\mathcal{K}^r$ onto $\mathcal{K}^n$ is an embedding if and only if its associated derivation, which is locally nilpotent, has a slice system. This made possible to launch a relation between the cancellation problem and the embedding problem and led to candidate counterexamples for both the cancellation problem and the linearization problem in dimension five, see also [54].

From the geometric point of view, locally nilpotent derivations of a polynomial ring, over an algebraically closed field $\mathcal{K}$ of characteristic zero, correspond bijectively to algebraic group actions of $(\mathcal{K}, +)$ over the affine space $\mathcal{K}^n$. Such algebraic group actions are called algebraic G_a-actions and are all of the form $\exp(t\mathcal{X})$, where $\mathcal{X}$ is a locally nilpotent derivation of $\mathcal{K}[\underline{x}]$. So, the study of locally nilpotent derivations can be reduced to the study of algebraic group actions of $(\mathcal{K}, +)$. Locally nilpotent derivations in one variable are all of the form $a\partial_{x_1}$, where a is an element of $\mathcal{K}$. For the higher dimensional case, many contributions have been done in order to understand this kind of derivations from the geometric and algebraic point of view. Nevertheless, the current understanding of this topic is still limited. The only completely understood case is the polynomial ring in two variables over a field $\mathcal{K}$. This is due to a result of Rentschler in [87], which states that all algebraic G_a-actions on the plane $\mathcal{K}^2$ are triangular in a suitable coordinate system. This gives a complete classification of all planar algebraic G_a-actions, and likewise, all locally nilpotent derivations of $\mathcal{K}[x, y]$. This result does not hold for $n \geq 3$ as shown by Bass in [7]. In fact, Bass settled the existence of an algebraic G_a-action on $\mathcal{K}^3$ which can not be conjugated to a triangular G_a-action. Since then, various works has been done in this direction and among the obtained results is the well-known one of Kaliman in three dimensional case [61], which states that every free G_a-action is a translation. In terms of locally nilpotent derivations, this is equivalent to say that every fixed point free locally nilpotent derivation of polynomial ring, in three dimensional case, is a partial derivative.

As an approach to understand locally nilpotent derivations in three dimensional case, an interesting and motivating idea has been given by Freudenburg in [52]. It is called local slice construction and basically consists in describing a new way to modify a given locally nilpotent derivation in order to construct another new one. The question, which was posed after illustrating this idea, is whether every locally nilpotent derivation can be constructed from a partial derivation via a finite sequence of local slice constructions. This question has been solved affirmatively by the same author for the case of irreducible locally nilpotent derivations of rank at most two in $\mathcal{K}[x, y, z]$ [52, 54], and by Daigle for the case of homogeneous locally nilpotent derivations in three dimensional case [27]. Local slice construction was first given in order to understand and generalize the example of locally nilpotent derivation of rank 3, which was given in [51]. In this sense, by using Fibonacci sequence, a class of three-rank homogeneous locally nilpotent derivations has been constructed, which plays a crucial role in the classification of the standard homogeneous locally nilpotent derivations in three dimensional case.

In the end of the last century, Makar-Limanov has made a significant contribution to understand algebraic geometry, which is considered among the important tools coming out from the study of locally nilpotent derivations. More precisely, to an integral domain $\mathcal{A}$, he associated a new ring called the ML-invariant, which is the intersection of the kernels of all locally nilpotent derivations of $\mathcal{A}$, see [70]. This invariant has been used to prove that the hypersurface $x + x^2y + z^2 + t^3 = 0$ in $\mathbb{C}^4$ is not isomorphic to $\mathbb{C}^3$ [71], and is presently one of the powerful tools in the classification of algebraic surfaces, see [31, 6, 25, 26]. For instance, in [25] Daigle studied locally nilpotent derivations of the coordinate ring of algebraic surfaces defined by polynomials $\phi(z) - xy = 0$ in $\mathcal{K}[x, y, z]$, such surfaces are called Danielewski surfaces, and as consequence, he gave a full description of all locally nilpotent derivations of a special Danielewski surface, i.e., a Danielewski surface which its ML-invariant equal $\mathcal{K}$. Afterward, he gave an important results which characterize all the special Danielewski surfaces in terms of locally nilpotent derivations see, [26].

Outline of the Thesis

The aim of this thesis is to present, on one hand, some problems in which locally nilpotent derivations play a crucial role, namely, the coordinate problem and the parametrization problem. On the other hand, give some algorithms concerning locally nilpotent derivations, which may contribute in understanding locally nilpotent derivations in three dimensional case. It is organized as follows.

In chapter 1 we present a brief introduction of the concept of a locally nilpotent derivation over rings and give some basic facts to be used in this thesis.

In chapter 2 we deal with the coordinates problem in the polynomial ring $\mathcal{A}[x, y]$, where $\mathcal{A}$ is a unique factorization domain. First we treat the problem in the case where $\mathcal{A} = \mathcal{K}$ is a field. We give an algorithm to check whether a given polynomial f in $\mathcal{K}[x, y]$ is a coordinate, and if so, to compute a coordinate's mate of f. Then we extend the obtained result over fields to unique factorization domains of characteristic zero. A notable feature of the given algorithm is that it always produces a coordinate mate of minimum possible degree.

In chapter 3 we address the problem of computing some invariants, namely the plinth ideal and the rank, of locally nilpotent derivations in dimension three. We give an algorithm which computes a generator of the plinth ideal for a given locally nilpotent derivation. As a by-product, we give an algorithmic classification of locally nilpotent derivations according to their rank.

Chapter 4 concerns triangulable locally nilpotent derivations in dimension three. We use the results obtained in chapter 3 to provide a method for recognizing triangulable locally nilpotent derivation of the polynomial ring $\mathcal{K}[x, y, z]$, and in case the given derivation is triangulable, the algorithm produces a coordinate system in which the derivation takes a triangular form.

Finally, chapter 5 deals with the polynomial parametrization of an affine space nonsingular curve. We give a new approach for parameterizing an algebraic curve by using the language of locally nilpotent derivations. We show that any polynomial parametrization of the given curve is a solution of an ordinary differential system whose underlying derivation is locally nilpotent. We also show that we may always choose the derivation in such a way that the resulting parametrization has its coefficients in the ground field. In the case where the curve is a complete intersection, we give an easy and explicit way to find such a derivation.

Résumé en français

Cette thèse porte sur l'étude algorithmique des problèmes liés aux dérivations localement nilpotentes et leurs applications aux automorphismes polynomiaux de l'espace affine.

Une dérivation $\mathcal{X}$ sur $\mathcal{A}$ est dite localement nilpotente si pour tout élément a de $\mathcal{A}$ il existe un entier positif n tel que $\mathcal{X}^n(a) = 0$, tout en tenant compte que $\mathcal{A}$ est un anneau commutatif unitaire. Les dérivations localement nilpotentes sur les anneaux sont des objets de grande importance dans beaucoup de domaines de mathématiques. Ses propriétés ont été étudiées par beaucoup de chercheurs, en utilisant des techniques des groupes algébriques, la géométrie algébrique, la théorie des représentations et l'algèbre commutative, à notre connaissance, l'étude des dérivations localement nilpotentes remonte au milieu du XX^{eme} siècle, et elle est issue de la théorie de groupe de Lie, la théorie des invariantes et des équations différentielles. Cet amalgame a permis d'établir la connexion entre les dérivations, les actions de groupe et les champs de vecteurs.

Durant la dernière décennie, les dérivations localement nilpotentes ont connu un véritable progrès. Elles sont devenues un élément essentiel pour la compréhension de la géométrie algébrique affine et d'algèbre commutative. Cette importance est due au fait que certains problèmes classiques dans ces domaines, telles que la conjecture jacobienne, le problème d'élimination, le problème de plongement, le problème de linéarisation et le 14^{eme} problème de Hilbert, ont été reformulés dans la théorie des dérivations localement nilpotentes. Par exemple, la conjecture jacobienne, qui affirme qu'une application polynomiale $f = (f_1, \dots, f_n)$ de $\mathbb{C}[x_1, \dots, x_x]$ est un automorphisme si son Jacobian $\mathrm{Jac}(f)$ est une constante non nulle, a été formulée de la manière suivante : Soient $f_1, \dots, f_n$ des polynômes de $\mathbb{C}[x_1, \dots, x_n]$. Si la dérivation jacobienne $\mathcal{X}_{f_1,\dots,f_{n-1}}$ a un élément principal, alors la dérivation $\mathcal{X}_{f_1,\dots,f_{n-1}}$ est localement nilpotente et son anneau de constantes est $\mathbb{C}[f_1, \dots, f_{n-1}]$. Ce problème est d'une grande importance dans de nombreuses disciplines tel que l'algèbre, l'analyse et la géométrie complexe [41]. Malgré de nombreux progrès réalisés pour la résolution de ce problème et même dans le cas de deux variables, il reste sans solution notable depuis sa première apparition en 1939. Ce champ scientifique est toujours considéré comme un des grands axes de recherche qui reste à explorer. Dans ce contexte, un des résultats encourageants dans les essais de simplifier ce problème est la condition suffisante proposée dans [101, 8]. Il a été montré que la conjecture jacobienne peut se réduire a l'étude des polynômes de la forme $f_i = x_i + h_i$, où $\mathrm{Jac}(h)$ est nilpotent et h homogène du degré trois. Dans cette perspective, le case de dimension trois a été complètement résolue pour toutes les polynômes homogènes de la forme $x + h$, où h est homogène du degré plus grand ou égal à deux [79].

Un autre exemple est celui du problème d'élimination dans lequel on demande si une variété algébrique complexe $\mathcal{V}$ telle que $\mathcal{V} \times \mathbb{C} \cong_{\mathbb{C}} \mathbb{C}^n$ est isomorphe à $\mathbb{C}^{n-1}$. En faisant appel aux dérivations localement nilpotentes $\mathcal{X}$ de $\mathbb{C}[x_1, \ldots, x_n]$, ce problème est équivalent au fait que tout élément principal s d'une dérivation localement nilpotente est une coordonnée, c.à.d, s est l'image de x_1 par un automorphisme de $\mathbb{C}[x_1, \ldots, x_n]$. Le problème d'élimination a été évoqué pour la première fois par Zariski en 1942 et il a trouvé solution consécutivement, dans le cas de deux et trois variables par Rentschler [87], Fujita [55] et Miyanishi-sugie [80]. Cependant, Pour le cas ou $n \geq 4$ il reste encore ouvert. Par ailleurs, le problème d'élimination est également lié au problème de la reconnaissance des coordonnées, qui est un objet primordial lorsqu'on étudie les automorphismes polynomiaux de l'algèbre de polynômes. La reconnaissance des coordonnées d'une manière ou d'une autre est de grand impact en géométrie algébrique affine, spécialement, dans l'étude des automorphismes polynômes de l'espace affine. Beaucoup de mathématiciens, y compris Drensky, van den Essen, Makar-Limanov, Shpilrain, Yu et autres, travaillaient sur différents aspects de ce problème, voir par exemple [65, 71, 41, 100, 32, 95, 17, 12, 13, 14]. Grâce au théorème d'Abhyanka et Moh [1] ce problème a été résolu pour le cas de deux variables. Cependant, il demeure complètement ouvert pour n supérieur a 3. En utilisant des dérivations localement nilpotentes, van den Essen a proposé une caractérisation algorithmique des coordonnées à deux variables sur un corps de caractéristique nulle [38], et dans [13], le même auteur avec J. Berson ont présenté un autre algorithme qui identifie les coordonnées à deux variables a coefficient dans une algèbre de type finie contenant les nombres rationnels.

D'un point de vue géométrique, les dérivations localement nilpotentes sur un anneau de polynômes, à coefficient dans un corps algébriquement clos $\mathcal{K}$ de caractéristique zéro, correspondent aux actions algébriques de $(\mathcal{K}, +)$ sur l'espace affine $\mathcal{K}^n$. Beaucoup de contributions ont été faites dans le but de comprendre ce genre de dérivations de point de vue algébrique et géométrique [6, 31, 25, 27, 33, 54, 61, 70, 72, 83, 87]. Malgré cela, la compréhension actuelle de ce sujet est encore limitée. Le seul cas qui, bien compris complètement, est le cas d'un anneau de polynômes à deux variables a coefficients dans un corps $\mathcal{K}$. Cela est dû à un résultat de Rentschler [87], qui dit que toutes les actions algébriques sur le plan $\mathcal{K}^2$ sont triangulaires dans un système de coordonnées. Ce résultat n'est pas valable pour $n \geq 3$. En effet, un contre-exemple a été donné par Bass [7] pour le cas $n = 3$ où il a montré l'existence d'une action algébrique sur $\mathcal{K}^3$ qui ne peut être conjuguée à une action algébrique triangulaire. Depuis, de nombreux travaux ont été faites dans cette direction. Parmi les résultats obtenus, est celle donnée par Kaliman en dimensions trois [61]. Il a démontré que chaque action algébrique n'ayant pas un point fixe est une translation. En termes de dérivations localement nilpotentes, cela équivaut que chaque dérivation localement nilpotente sans point fixe, sur l'anneau de polynômes à trois variables, est un dérivé partiel.

D'autre part, une idée intéressante pour étudier les dérivations localement nilpotentes en trois dimensions a été mentionnée par Freudenburg [52] et elle est connue depuis sous le nom de la construction des éléments principaux locaux. Cette idée est basée principalement sur la modification d'une dérivation localement nilpotente donnée pour construire une autre, et elle a été postulée pour la première fois dans le but de comprendre et de généraliser l'exemple donné pour la dérivation localement nilpotente de rang 3 [51]. Dans ce contexte, la question qui a été posée par Freudenburg dans le but de comprendre les dérivations en dimension trois et de savoir si toute dérivation localement nilpotente peut être construite à partir d'une dérivé partielle via une séquence de la construction des éléments principaux locaux. Effectivement, cette question a trouvé une réponse significative par le même auteur dans le cas des dérivations localement nilpotentes irréductibles de rang ≤ 2 dans l'anneau $\mathcal{K}[x, y, z]$ et par Daigle pour le cas de dérivations localement nilpotentes homogènes en trois dimension [27, 52, 54].

Cette thèse a pour objectif de présenter, d'une part, quelques problèmes dans lesquels les dérivations localement nilpotentes jouent un rôle crucial, à savoir le problème des coordonnées et le problème de paramétrisation polynomial des courbes algébriques dans l'espace affine. Et d'autre part, de donner quelques algorithmes qui peuvent contribuer à la compréhension des dérivations localement nilpotente en dimension trois. Dans ce sens, cette thèse sera organisée comme suit:

Au chapitre 1, nous introduisons quelques notations et définitions de base concernant les dérivations localement nilpotentes qui vont être utilisées durant tous le manuscrit.

Chapitre 2:
Les coordonnées en dimension deux sur un anneau factoriel

Soient $\mathcal{A}[\underline{x}] := \mathcal{A}[x_1, \ldots, x_n]$ et $f \in \mathcal{A}[\underline{x}]$. On dit que f est une coordonnée s'il existe des polynômes $f_1, \ldots, f_{n-1}$ tels que $\mathcal{A}[\underline{x}] = \mathcal{A}[f, f_1, \ldots, f_{n-1}]$. Reconnaissance les polynômes susceptibles d'être des coordonnées dans $\mathcal{A}[\underline{x}]$ est l'un des principaux points qui feront l'objet d'étude de groupe d'automorphismes de l'algèbre de polynômes $\mathcal{A}[\underline{x}]$. Malgré les nombreux travaux qui ont été réalisés dans ce contexte, ce problème est complètement ouvert lorsque n est supérieur a 3. Récemment, une nouvelle méthode a été développée par J. Berson pour objectif de construire une classe de coordonnées en se basant sur les plongements dans l'espace affine [13, chapitre 6]. Dans le cas de deux variables, différents algorithmes ont été proposés pour ce problème, voir [38, 18, 19, 95, 17, 13]. Néanmoins, lorsqu'on s'intéresse à trouver un compagnon, c.a.d, un polynôme g qui vérifie $\mathcal{K}[f, g] = \mathcal{K}[x, y]$, les méthodes existantes sont plus ou moins compliquées au niveau du calcul. Par exemple, dans l'article [19], une formule intégrale a été développée pour calculer un polynôme g vérifiant $\mathrm{Jac}(f, g) = 1$, et par conséquent, elle résout le problème de compagnon. La même question a été résolue en gardant la trace des réductions de Gröbner effectuées pour vérifier si f est une coordonnée [95]. En utilisant la théorie des dérivations localement nilpotentes, une autre solution à ce problème a été proposée par Va den Essen dans [38]. Son résultat affirme qu'un polynôme f est une coordonnée si et seulement si la dérivation jacobienne $\mathcal{X}_f = \partial_y f \partial_x - \partial_x f \partial_y$ est localement nilpotente et $\mathcal{I}(\partial_x f, \partial_y f) = 1$, et donc la question de calculer un compagnon pour f se réduit à calculer un élément principal de $\mathcal{X}_f$, i.e., un élément s tel que $\mathcal{X}_f(s) = 1$.

En s'appuyant sur le résultat de van den Essen, nous présentons, dans ce chapitre, un autre critère de reconnaissance de coordonnées en dimension deux qui est une simplification de celui de van den Essen. En effet, nous montrons qu'un polynôme f est une coordonnée si seulement la dérivation $\mathcal{X}_f$ est localement nilpotente et que l'élément qui se trouve juste avant le commencement des zéros $\mathcal{X}_f^{r_1}(x)$ est un élément de $\mathcal{K}^*$. Dans ce cas, un compagnon de f est donné par $g := (\mathcal{X}_f^{r_1}(x))^{-1}\mathcal{X}_f^{r_1-1}(x)$. L'avantage de ce résultat, c'est qu'il réduit le calcul à vérifier uniquement la nilpotente locale de la dérivation $\mathcal{X}_f$. Autrement dit, le calcul effectué nécessaire pour vérifier la nilpotence locale de $\mathcal{X}_f$ est suffisant pour vérifier si f est une coordonnée et à calculer un compagnon dans le cas où il existe. Une caractéristique remarquable de ce critère, c'est qu'il fournit une solution simple du problème du compagnon. En plus, le compagnon produit par cette méthode est toujours plus petit par rapport au degré, ce que nous montrerons dans le théorème 2.2.6.

La reconnaissance des coordonnées en dimension supérieure est beaucoup plus compliquée. Une approche pour l'envisager c'est de voir les coordonnées dans un anneau de polynômes à deux variables à coefficients dans un anneau qui n'est pas un corps. Dans ce sens, nous étendrons le résultat obtenu au cas d'un corps à un anneau factoriel de caractéristique nulle. Nous donnons le théorème 2.3.3 qui caractérise les coordonnées en deux variables à coefficient dans un anneau factoriel. La réalisation de ce résultat en algorithme nécessite d'avoir d'abord une solution algorithmique du problème de la décomposition suivante: Étant donné $f, g \in \mathcal{A}[x, y]$ et $a \in \mathcal{A}$, où $\mathcal{A}$ est un anneau factoriel. Comment décider si $g = h(f) \mod(a)$, où h est un polynôme dans $\mathcal{A}[t]$? Pour cela, nous construisons une suite $h_{i,j}$ de polynômes, en utilisant la division Euclidien, qui nous aide à avoir une solution de notre problème de décomposition. Puis, nous terminons ce chapitre par donner une description détaillée de l'algorithme qui permet de reconnaître les coordonnées en deux variables sur un anneau factoriel de caractéristique nulle, puis, nous présentons quelques exemples des coordonnées en dimension deux.

Chapitre 3
Caractérisation du rang des dérivations localement nilpotentes

Avoir une bonne description du groupe de $\mathcal{K}$-automorphismes $Aut_{\mathcal{K}}(\mathcal{K}[\underline{x}])$, de l'algèbre de polynômes $\mathcal{K}[\underline{x}]$, est l'un des problèmes majeurs en algèbre commutative. Grâce au résultats de Van der Kulk et Jung [66, 59], on sait que tout élément de $Aut_{\mathcal{K}}(\mathcal{K}[x_1, x_2])$ se décompose en produit d'automorphismes affines et triangulaires, Cependant, $Aut_{\mathcal{K}}(\mathcal{K}[\underline{x}])$ reste complètement difficile à appréhender lorsque $n \geq 3$. On sait depuis peu que dans le cas $n = 3$, ce groupe n'est pas seulement engendré par des automorphismes affines et triangulaires. Shestakov et Umirbaev [94] ont en particulier démontré récemment que le célèbre automorphisme de Nagata n'admet pas de décomposition en automorphisme de ce type. Or il se trouve que cet automorphisme s'obtient en termes d'automorphisme exponentielle, c.a.d, de la forme $\exp(\mathcal{X})$, où $\mathcal{X}$ est une dérivation localement nilpotente de l'anneau de polynômes $\mathcal{K}[x, y, z]$. Dans cette optique, une approche à suivre pour étudier le groupe $Aut_{\mathcal{K}}(\mathcal{K}[\underline{x}])$ est celle qui vise à avoir une bonne description du sous groupe d'automorphismes exponentielles. D'autre part, puisque il y a une correspondance bijective entre les automorphismes exponentielles et les dérivations localement nilpotentes, donc on peut se réduire à trouver une bonne description des dérivations localement nilpotentes de $\mathcal{K}[\underline{x}]$. Les dérivations localement nilpotentes sur $\mathcal{K}[x_1]$ sont toutes de la forme $a\partial_{x_1}$, où a est un élément de $\mathcal{K}$. On connaît aussi que les dérivations localement nilpotentes de $\mathcal{K}[x, y]$ sont complètement classées, cela dû à un résultat de Rentchler (voir théorème 1.2.1). Concernant le cas de trois variables, de nombreux mathématiciens y compris Daigle, Freudenburg et Kaliman ont contribué à une meilleure connaissance du sujet en développant des méthodes bien différentes qui constituent un grand pas vers une classification des dérivations localement nilpotentes en dimension trois, voir [21, 22, 27, 23, 28, 50, 52, 61, 54]. Toutefois, certains des résultats obtenus, utilisant les méthodes topologiques, ne sont pas de nature algorithmique. Il serait donc agréable d'obtenir une classification algorithmique des dérivations localement nilpotentes en dimension trois, mais cela semble être un problème fastidieux.

Dans ce chapitre, nous abordons certains invariants des dérivations localement nilpotentes à savoir l'idéal socle $\mathcal{S}^{\mathcal{X}} = \mathcal{X}(\mathcal{K}[\underline{x}]) \cap \mathcal{K}[\underline{x}]^{\mathcal{X}}$ et le rang, qui est le nombre minimal des dérivés partielles nécessaire pour exprimer la dérivation $\mathcal{X}$, on le note par $rank(\mathcal{X})$. Nous définissons d'abord la notion d'élément principal local minimal d'une dérivation localement nilpotente, sur un anneau commutative unitaire, qui est l'indispensable clef de tout ce qui suit. Puis, nous mentionnons une caractérisation de tous les éléments principaux locaux minimaux; nous montrons que dans le cas où l'anneau $\mathcal{A}$ est factoriel, les éléments principaux locaux minimaux existent toujours. En plus, cette existence est d'une nature algorithmique, nous donnons un processus pour calculer un élément principal local minimal à partir d'un élément principal local donné, ce que nous expliquons dans la sous-section 3.1.2. Dans le cas d'un anneau de polynômes à trois variables, cela nous aide de déduire un résultat important concernant les générateurs de l'idéal socle. En fait, en se basant sur la platitude de l'anneau $\mathcal{K}[x, y, z]$ sur $\mathcal{K}[x, y, z]^{\mathcal{X}}$, Daigle et Kaliman ont constaté que l'idéal socle est toujours principal [28]. Ce résultat, nous permet de trouver les générateurs de cet idéal: nous démontrons que l'idéal socle d'une dérivation localement nilpotente $\mathcal{X}$ est engendré par l'image d'un élément principal local minimal de la dérivation $\mathcal{X}$, i.e., $\mathcal{S}^{\mathcal{X}} = (\mathcal{X}(s))$ pour un élément principal local minimal s de $\mathcal{X}$. Notre résultat est basé aussi sur celui de Miyanishi [81], qui affirme que l'anneau des constants d'une dérivation localement nilpotente sur l'algèbre $\mathcal{K}[x, y, z]$ est toujours un anneau de polynômes à deux variables. Notons que la preuve donnée par Miyanishi est de nature topologique et jusqu'à maintenant il n'y en a pas une autre preuve algorithmique. Pour cela nous supposons, durant tout la suite de ce chapitre, qu'un système de coordonnées de l'anneau des constantes $\mathcal{K}[x, y, z]^{\mathcal{X}}$ est disponible.

Le dernier paragraphe de ce chapitre a pour but de donner une classification des dérivations localement nilpotentes selon leur rang. Pour ce faire, rappelons que la seule dérivation sur $\mathcal{K}[\underline{x}]$ de rang zéro c'est la dérivation nulle et chaque dérivation de rang 1 est toujours de la forme $p(y_1, \ldots, y_{n-1}).y_n$, dans un système des coordonnées $y_1, \ldots, y_n$. Une telle dérivation est localement nilpotente si et seulement si p ne dépend pas de y_n. Notons aussi que si $\mathcal{X}$ est une dérivation localement nilpotente irréductible alors pour tout élément c tel que $\mathcal{X}(c) \neq 0$, les dérivations $c\mathcal{X}$ et $\mathcal{X}$ ont le même rang. Cela signifie que, pour le calcul de rang, nous pouvons se restreindre, sans perte de généralité, à des dérivations irréductibles. Dans [50], il a été montré qu'une dérivation localement nilpotente de $\mathcal{K}[\underline{x}]$ est de rang 1 si et seulement si son anneau des constants est un anneau des polynômes à $n-1$ variables et qu'elle a un élément principal. En dimension 3, et en tenant compte le théorème de Miyanishi, une dérivation localement nilpotente irréductible est de rang 1 si et seulement si l'algorithme 4, qui calcule l'élément principal local minimal, produit un élément principal. Cela veut dire que le cas des dérivations de rang 1 est bien classé. Pour les dérivations localement nilpotentes de rang 2, nous montrons que le rang d'une dérivation localement nilpotente vaut 2 si seulement si le générateur de l'idéal socle est un polynôme en un seul variable u et que u est une coordonnée dans l'anneau des constantes de $\mathcal{X}$. Ce qui est en fait algorithmiquement testable. En effet, il est algorithmiquement possible de vérifier si un polynôme en deux variables est une coordonnée. Nous utilisons pour cela l'algorithme donné dans le chapitre 2. D'autre part, le fait que le générateur de l'idéal socle est un polynôme en un seul variable peut être vérifié à l'aide de la décomposition fonctionnelle des polynômes, voir [56].

À la fin de ce chapitre, nous faisons une implémentation du programme qui calcule le rang. Comme nous n'avons pas une version algorithmique de la théorème de Miyahishi, nous nous limitons au cas des dérivations de $\mathcal{K}[x, y, z]$ représentés dans une forme Jacobienne, disons $\mathrm{Jac}(f, g, .)$, et dont l'anneau de constantes est généré par f, g.

Chapitre 4
Dérivations localement nilpotentes triangulable en trois dimensions

Une dérivation localement nilpotente $\mathcal{X}$ de $\mathcal{K}[\underline{x}]$ est dite triangulaire dans le système de coordonnées $(x_1, \ldots, x_n)$ si pour tout $i = 1, \ldots, n$, nous avons $\mathcal{X}(x_i) \in \mathcal{K}[x_1, \ldots, x_{i-1}]$. On dit que $\mathcal{X}$ est triangulable s'il existe un $\mathcal{K}$-automorphisme $\sigma \in \mathcal{K}[\underline{x}]$ tels que $\sigma\mathcal{X}\sigma^{-1}$ est triangulaire dans le système de coordonnées $(x_1, \ldots, x_n)$, i.e., il existe un système de coordonnées $(y_1, \ldots, y_n)$ dans lequel $\mathcal{X}$ a une forme triangulaire. Donner un critére de triangulabilité des dérivations est l'un des problèmes majeurs en ce qui concerne l'étude des dérivations localement nilpotentes. Il est pertinent aux autres différents problèmes fondamentaux en géométrie algébrique, comme le problème d'automorphismes modérées(Tameness problem) [41, 54]. Grâce au résultat de Rentchler [87], on sait que les dérivations localement nilpotentes en dimension deux sont toutes triangulables, ce résultat a été utilisè après pour donner une autre preuve du théorème de Jung [59] concernant les automorphismes modérées en dimension deux. Pour le cas de plusieurs variables, le premier exemple d'une dérivation localement nilpotente non-triangulable en dimension 3 a été donné par Bass [7]. Ensuite, la construction de Bass a été généralisée par Popov [85] pour obtenir des dérivations localement nilpotentes non-triangulables en toutes dimensions supérieures à 3. Depuis, de nombreuses tentatives ont été faites pour trouver un critère de triangulabilité. Dans [85], Popov a proposé une condition nécessaire de triangulabilité, basée sur la structure des points fixes de la variété. Cependant, cette condition n'est pas suffisante comme a été constaté dans [21]. Autres critères de triangulabilité en dimension 3 ont été développés par plusieurs mathématiciens dans ce domaine (voir [50, 21, 49, 23]). Pourtant, il est loin de les rendre algorithmique.

L'objectif de ce chapitre est de mettre au point un algorithme pour vérifier si une dérivation localement nilpotente $\mathcal{X}$ donnée, de $\mathcal{K}[x, y, z]$, est triangulable, et dans le cas échéant de trouver un système de coordonnées dans lequel $\mathcal{X}$ a une forme triangulaire. Pour ce faire, rappelons que les dérivations triangulables en dimension n sont de rang au plus $n - 1$. D'autre part, les dérivations localement nilpotentes de rang 1 sont évidemment triangulables. Ce qui indique qu'en dimension 3, le seul cas que nous avons besoin de traiter est celui des dérivations de rang 2. Dans ce sens, nous simplifions d'abord la forme du problème de triangulabilité en fonction de la notion d'élément principal local minimal; nous montrons que pour chaque dérivation triangulaire $\mathcal{X}$ sur $\mathcal{K}[x, y, z]$, il existe toujours un système de coordonnées (u, v, w) dans lequel la dérivation $\mathcal{X}$ peut s'écrire de la forme suivant $\mathcal{X}(u) = 0$, $\mathcal{X}(v) = c(u)$ et $\mathcal{X}(w) = q(u, v)$, où $c(u)$ est un générateur de l'idéal socle de la dérivation $\mathcal{X}$. D'autre part, le fait que la dérivation considérée est de rang 2, implique que, dans le cas ou la dérivation est triangulable, tous les systèmes de coordonnées dans lesquels la dérivation est triangulaire partagent la même coordonnée u. Donc, puisque nous avons déjà u, trouver l'un de ces systèmes de coordonnées se réduit à trouver seulement deux compagnons v, w de u, de tel sorte que v soit un élément principal local minimal de la dérivation et $\mathcal{X}(w)$ soit un polynôme en u et v. Dans ce but, nous notons l'idéal $\mathcal{I}_c^{\mathcal{X}} := c\mathcal{K}[x, y, z] \cap \mathcal{K}[x, y, z]^{\mathcal{X}}[s]$, où $c = \mathcal{X}(s)$ est un générateur de l'idéal socle. Cet idéal contient des informations essentielles concernant la triangulabilité de la dérivation $\mathcal{X}$, en fait, par le théorème 4.3.1 nous montrons qu'une condition nécessaire et suffisante pour la triangulabilité de $\mathcal{X}$ est que l'idéal $\mathcal{I}_c^{\mathcal{X}}$ contient un polynôme de la forme $H = p + Q(u, s + \ell(u, p))$, où p c'est un compagnon de u dans l'anneau des constants de $\mathcal{X}$. En utilisant le théorème de reste Chinois, nous démontrons que cet critère peut se réduire à trouver un polynôme de la forme $p + Q_i(u, s + \ell_i(u, p))$ dans chaque idéal $\mathcal{I}_{c_i^{n_i}}^{\mathcal{X}}$, où $c = c^{n_1} \dots c^{n_r}$, avec les c_i sont premiers deux à deux.

La section 4.4 s'intéresse à donner une autre caractérisation algorithmique de la triangulabilité qui nous permet de calculer un système de coordonnées de $\mathcal{K}[x, y, z]$ dans lequel la dérivation $\mathcal{X}$ possède la forme triangulaire qu'on cherche. Puis, nous terminons ce chapitre par donner une implémentation de l'algorithme de triangulabilité.

Chapitre 5
Paramétrisation polynomiale des courbes intersections complète non singulieres

La paramétrisation des courbes algébriques est un outil fondamental pour de nombreuses applications, parmi lesquelles on peut citer la modélisation géométrique, l' informatique graphique et CAGD (Computer Aided Geometric Design). Donner une paramétrisation d'une courbe algébrique revient à exprimer une correspondance bijective entre le corps des fonctions de la courbe et le corps des fonctions du plan projectif. Le calcul d'une paramétrisation rationnelle consiste essentiellement en deux étapes consécutives, la première étape portant sur l'analyse des singularités de la courbe dans le plan projectif, qui peut être réalisé soit par la technique d'explosion ou par les séries de

Puiseaux. La deuxième étape consiste à trouver un point non singulier de la courbe dont les coordonnées génèrent un corps d'extension, du corps de base, de degré aussi petite que possible. Pour plus de détail, nous vous renvoyons à [3, 10, 58, 86, 90, 92, 93, 91].

Les courbes rationnelles qui peuvent être décrites par une paramétrisation polynomiale forment une classe intéressante, dans le sens où il existe des méthodes qui leurs sont applicables et non pas aux courbes rationnelles en général, voir [4, 34, 40, 48, 47, 46, 73]. Donc, il sera utile d'avoir un critère de paramétrisation polynomiale des courbes algébriques. La condition sur laquelle une courbe algébrique peut être paramétrée rationnellement est que son genre doit être égal à zéro, c.a.d, le nombre de ses points singuliers, comptés avec leur multiplicité, est maximum [98]. En utilisant ce résultat, Abhyankar, dans [2], a démontré qu'une courbe algébrique rationnelle plane est paramétrable polynomialement si et seulement si elle a une place à l'infini. Une caractérisation de ces courbes avec un algorithme pour calculer une paramétrisation dans le cas où elle existe a été proposée par Manocha dans [73]. Cependant, cette méthode exige qu'une paramétrisation rationnelle de la courbe algébrique soit disponible. Récemment, deux nouveaux algorithmes ont été développés pour calculer une paramétrisation polynomiale d'une courbe plane sans point singulière. Le premier algorithme fondé sur le théorème de Abhyankar-Moh [1] a été donné dans [57], et le deuxième algorithme fondé sur des réductions de Gröbner [95] a été donné dans [96].

Dans ce chapitre, nous allons proposer une nouvelle méthode de paramétrisation en se basant sur la théorie des dérivations localement nilpotentes. Nous donnons un critère qui est nécessaire et suffisant pour la paramétrisation polynomiale des courbes algébriques non singulières dans l'espace affine. Dans le cas des courbes algébriques qui sont intersection complète, nous présentons un algorithme simple qui produit une telle paramétrisation. L'idée principale derrière notre méthode, c'est que si une courbe irréductible non singulier $\mathcal{C}$ a une paramétrisation polynomiale $x(t)$, alors cette paramétrisation est en fait une solution d'une équation différentielle $\dot{x} = p(x)$, où les composantes de p sont des polynômes. En plus, cette équation différentielle n'a pas de point fixe sur la courbe $\mathcal{C}$. En termes algébrique, cela signifie que la dérivation correspondant à cette équation différentielle est localement nilpotente et engendre le module de dérivations $\mathcal{D}_{\overline{\mathcal{K}}}(\overline{\mathcal{K}}[\mathcal{C}])$ de l'anneau des coordonnées $\overline{\mathcal{K}}[\mathcal{C}]$ de la courbe $\mathcal{C}$, où $\overline{\mathcal{K}}$ est la clôture algébrique de $\mathcal{K}$. Nous verrons aussi qu'on a toujours la possibilité de choisir une dérivation dont les coefficients sont dans le corps de base $\mathcal{K}$, qui est la raison principale derrière le fait que nous pouvons toujours trouver une paramétrisation à coefficients dans $\mathcal{K}$. En plus, la dérivation qui génère le module $\mathcal{D}_{\overline{\mathcal{K}}}(\overline{\mathcal{K}}[\mathcal{C}])$ a un élément principal s et poursuit une paramétrisation de la courbe $\mathcal{C}$, dans ce cas, est donné par

$$x_i(t) = \sum_j \frac{1}{j!} \exp(-s\mathcal{X})(\mathcal{X}^j(x_i))t^j, \qquad i = 1, \ldots, n.$$

Rendre ce résultat algorithmique demande du travail, spécialement la vérification des deux premières conditions, à savoir la décision que $\mathcal{D}_{\overline{\mathcal{K}}}(\overline{\mathcal{K}}[\mathcal{C}])$ est de rang 1 et de trouver un de ses générateurs. Donc cette optique, nous nous restreignons à un cas particulier des courbes algébriques sur lequel nous donnons un algorithme qui donne une paramétrisation. C'est le cas des courbes qui sont intersection complète. Rappelons qu'une courbe algébrique $\mathcal{C}$ est dite intersection complète si son idéal associe $\mathcal{I}_{\mathcal{K}}(\mathcal{C})$ est engendré exactement par $n-1$ polynômes $f_1, \ldots, f_{n-1}$. Dans ce cas, nous montrons que le module des dérivations $\mathcal{D}_{\overline{\mathcal{K}}}(\overline{\mathcal{K}}[\mathcal{C}])$ est toujours de rang 1 engendré par la dérivation jacobienne $\mathcal{X}_{f_1,\ldots,f_{n-1}}$. Ce résultat nous aide à présenter le théorème 5.4.2 dans lequel nous donnons une simple caractérisation des ensembles algébriques définies par $n-1$ polynômes qui sont susceptibles d'être des courbes algébriques, non singulières, irréductibles et qui sont polynomialement paramétrisables.

Le reste de ce chapitre est consacré à donner une vue détaillée sur les étapes de la méthode de projection en comparaissant avec la notre. Puis, nous terminons ce chapitre par donner quelques exemples, et comparer les performances de notre méthode avec celle de la projection.

Chapter 1

Preliminaries

In this introductory chapter we recall definitions and some basic properties concerning locally nilpotent derivations over rings, especially over polynomial rings, which will often be useful for us throughout this thesis. For more background on locally nilpotent derivations, we refer to [41, 83, 54].

In all the sequel, $\mathcal{K}$ denotes a commutative field of characteristic zero and all considered rings are commutative of characteristic zero with unit. We devote our attention to a special type of commutative rings, namely the polynomial rings. Often we will use the abbreviation $\mathcal{K}[\underline{x}]$ to mean the polynomial ring in terms of the variables $x_1, \ldots, x_n$ with coefficients in $\mathcal{K}$, and by $\mathcal{K}^{[n]}$ we mean the $\mathcal{K}$-algebra of polynomials in n unspecified variables.

1.1 Over-view on derivations

Definition 1.1.1 *Let $\mathcal{A}$ be a ring. A derivation of $\mathcal{A}$ is a map $\mathcal{X} : \mathcal{A} \longrightarrow \mathcal{A}$ such that for any $a, b \in \mathcal{A}$, the following properties holds:*

$$\begin{aligned} \mathcal{X}(a+b) &= \mathcal{X}(a) + \mathcal{X}(b), \\ \mathcal{X}(ab) &= a\mathcal{X}(b) + b\mathcal{X}(a). \end{aligned}$$

For example, in the polynomial ring $\mathcal{K}[\underline{x}]$, the usual partial derivatives ∂_{x_i} with respect to x_i are derivations of $\mathcal{K}[\underline{x}]$. Another well-known example is the so-called triangular derivations of $\mathcal{K}[\underline{x}]$, i.e., derivations of the polynomial ring $\mathcal{K}[\underline{x}]$ which satisfy $\mathcal{X}(x_i) \in \mathcal{K}[x_1, \ldots, x_{i-1}]$ for any $i = 1, \ldots, n$.

In the case of when $\mathcal{A}$ is an $\mathcal{R}$-algebra, $\mathcal{R}$ is a ring, we say that a derivation of $\mathcal{A}$ is an $\mathcal{R}$-derivation if it annihilates all elements of $\mathcal{R}$. The collection of all derivations (resp. $\mathcal{R}$-derivations) of $\mathcal{A}$ will be denoted by $\mathcal{D}(\mathcal{A})$ (resp. $\mathcal{D}_{\mathcal{R}}(\mathcal{A})$) and it is an $\mathcal{A}$-module. Moreover, if $[.,.]$ is the Lie bracket, then $(\mathcal{D}(\mathcal{A}), +, ., [,])$ is a Lie algebra.

In the case of an $\mathcal{R}$-algebra $\mathcal{A}$ and under the assumption that $\mathcal{A}$ is finitely generated by a set $\mathcal{G}$, any derivation $\mathcal{X}$ of $\mathcal{A}$ is completely determined by the images $\mathcal{X}(a)$, $a \in \mathcal{G}$. In particular if $\mathcal{A}$ is a polynomial ring we have the following well-known result, see [41, Proposition 1.2.5].

Proposition 1.1.2 *Let $\mathcal{A} := \mathcal{R}[\underline{x}]$. Then $\mathcal{D}_{\mathcal{R}}(\mathcal{A})$ is a free $\mathcal{A}$-module with basis $\partial_{x_1}, \dots, \partial_{x_n}$ and $[\partial_{x_i}, \partial_{x_j}] = 0$ for all i, j. In other words, for any $\mathcal{X} \in \mathcal{D}_{\mathcal{R}}(\mathcal{A})$:*

$$\mathcal{X} = \sum_{i=1}^{n} f_i \partial_{x_i}$$

where the f_i's are elements of $\mathcal{A}$.

1.1.1 Locally nilpotent derivations

A nonzero derivation of a ring $\mathcal{A}$ is said to be locally nilpotent if for any element a of $\mathcal{A}$, there exists a positive integer $n > 1$ such that $\mathcal{X}^n(a) = 0$, where $\mathcal{X}^n$ stands for the n-fold composition $\mathcal{X} \circ \dots \circ \mathcal{X}$. In this case, we define the degree of a with respect to $\mathcal{X}$ as $\deg_{\mathcal{X}} a = n - 1$, where n is the smallest integer such that $\mathcal{X}^n(a) = 0$. An element $s \in \mathcal{A}$ is called a local slice of $\mathcal{X}$ if $\mathcal{X}(s) \neq 0$ and $\mathcal{X}^2(s) = 0$. Moreover, if $\mathcal{X}(s) = 1$, then s is called a slice of $\mathcal{X}$. Notice that a nonzero locally nilpotent derivation needs not have a slice, for example the derivation $x\partial_y$ of $\mathcal{K}[x, y]$ has no slice. However it always has a local slice.

A trivial example of locally nilpotent derivations is the partial derivatives ∂_{x_i} on the polynomial ring $\mathcal{K}[\underline{x}]$ since $\partial_{x_i}(x_j) = \delta_{i,j}$. Another class of locally nilpotent derivations is given by the following proposition.

Proposition 1.1.3 *Every triangular derivation of the ring $\mathcal{K}[\underline{x}]$ is locally nilpotent.*

Proof. We will prove this by induction on n. For $n = 1$ the claimed result is clear. Now assume that the result holds for $n-1$. Clearly, $\mathcal{X}$ maps $\mathcal{K}[x_1, \dots, x_{n-1}]$ into itself and so restricts to a triangular derivation, say $\mathcal{Y}$, of $\mathcal{K}[x_1, \dots, x_{n-1}]$. By induction hypothesis $\mathcal{Y}$ is locally nilpotent. From the fact that $\mathcal{X}(x_n) \in \mathcal{K}[x_1, \dots, x_{n-1}]$ we deduce that $\mathcal{X}^n(x_n) = 0$ for n large enough. ∎

For $n \geq 3$, locally nilpotent derivations are not triangular in general, for instance see [85, 7, 21] for counterexamples. In chapter 4 we will treat this problem in dimension three and give conditions under which a given derivation has a triangular form in a suitable coordinate system.

Let $\mathcal{A}$ be a commutative ring and $\mathcal{X}$ a derivation of $\mathcal{A}$. By $\mathcal{A}^{\mathcal{X}}$, we mean the set of elements $a \in \mathcal{A}$ which satisfy $\mathcal{X}(a) = 0$. This set is an integrally closed subring of $\mathcal{A}$, called the ring of constants of $\mathcal{X}$ or the kernel of $\mathcal{X}$. The following useful result concerns the ring of constants of a locally nilpotent derivation and can be found in [41, Proposition 1.3.32]

Proposition 1.1.4 *Let $\mathcal{A}$ be a $\mathcal{K}$-domain and $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{A}$. Then the ring of constants $\mathcal{A}^{\mathcal{X}}$ is factorially closed, i.e., if $a \in \mathcal{A}^{\mathcal{X}}$ and $a = bc$ for some $b, c \in \mathcal{A}$, then $b, c \in \mathcal{A}^{\mathcal{X}}$.*

As a consequence of this proposition, $\mathcal{A}$ and $\mathcal{A}^{\mathcal{X}}$ have the same unit elements, i.e., $(\mathcal{A}^{\mathcal{X}})^* = \mathcal{A}^*$. Furthermore, every irreducible element of $\mathcal{A}^{\mathcal{X}}$ is irreducible in $\mathcal{A}$, in particular, if $\mathcal{A}$ is a unique factorization domain, then so is $\mathcal{A}^{\mathcal{X}}$.

1.1.2 Local nilpotency criterion

Let $\mathcal{A}$ be a commutative $\mathcal{K}$-algebra, $\mathcal{X}$ be a locally nilpotent derivation on $\mathcal{A}$ and t be an indeterminate over $\mathcal{A}$. We extend $\mathcal{X}$ to a derivation of $\mathcal{A}[t]$ by setting $\mathcal{X}(t) = 0$, and for any $a \in \mathcal{A}[t]$, we define the exponential map $\exp(t\mathcal{X})$ as follows:

$$\exp(t\mathcal{X}).a = \sum_{i \geq 0} \frac{\mathcal{X}^i(a)}{i!} t^i.$$

Since the derivation is locally nilpotent the above sum is always a finite sum. Furthermore, the map $\exp(t\mathcal{X})$ is an $\mathcal{K}[t]$-automorphism of $\mathcal{A}[t]$ with the inverse given by $\exp(-t\mathcal{X})$.

To check whether a given derivation is locally nilpotent is still an open problem in the general case. However, in the case of a finitely generated $\mathcal{R}$-algebra, we have the following useful result from [41, Proposition 1.3.16]

Proposition 1.1.5 *Let $\mathcal{A}$ be an $\mathcal{R}$-algebra with a generating set $\mathcal{G}$, and $\mathcal{X}$ be a derivation on $\mathcal{A}$. Then $\mathcal{X}$ is locally nilpotent if and only if for every $a \in \mathcal{G}$, there exists an integer n such that $\mathcal{X}^n(a) = 0$.*

In [38, 1.4.17], van den Essen gave a partial solution to the problem of recognizing locally nilpotent derivations on polynomial rings over fields of characteristic zero. His method was built of the disposal of sufficiently many algebraically independent elements in the ring of constants. Indeed, he proved that for any nonzero derivation $\mathcal{X}$ of $\mathcal{K}[\underline{x}]$, if $n-1$ algebraically independent elements $f_1, \ldots, f_{n-1}$ over $\mathcal{K}$, which are in $\mathcal{K}[\underline{x}]^{\mathcal{X}}$, are known and if we let η be the maximum of degrees of the algebraic extensions among the field extensions $\mathcal{K}(f_1, \ldots, f_{n-1})(x_i) \subset \mathcal{K}(\underline{x})$, then η is finite and $\mathcal{X}$ is locally nilpotent if and only if $\mathcal{X}^{\eta+1}(x_i) = 0$ for all x_i.

In the case of Jacobian derivations this yields the following useful criterion. First, let us fix some notations. Let $f_1, \ldots, f_{n-1}$ be elements of the polynomial ring $\mathcal{K}[\underline{x}]$. The Jacobian derivation of $\mathcal{K}[\underline{x}]$ determined by $f_1, \ldots, f_{n-1}$ is the derivation defined by

$$\mathcal{X}_{f_1,\ldots,f_{n-1}}(h), = \det\mathrm{Jac}(f_1, \ldots, f_{n-1}, h) \qquad \forall h \in \mathcal{K}[\underline{x}]$$

where $\mathrm{Jac}(f_1, \ldots, f_{n-1}, h)$ is the Jacobian matrix of $(f_1, \ldots, f_{n-1}, h)$.

Theorem 1.1.6 *Let $\mathcal{X} := \mathcal{X}_{f_1,\ldots,f_{n-1}}$ be a Jacobian derivation of the polynomial ring $\mathcal{K}[\underline{x}]$. If $\mathcal{X}$ is locally nilpotent, then $\mathcal{X}^{d+1}(x_i) = 0$ for any i, where $d = \prod_{i=1}^{n-1} \deg f_i$.*

Proof. Let $\mathcal{V}_f$ be the affine algebraic set defined by the ideal $f_1 = \ldots = f_{n-1} = 0$ and $\mathcal{K}[\mathcal{V}_f]$ its coordinate ring. Let us write $\gamma(\underline{x}, t) = (\gamma_1(\underline{x}, t), \ldots, \gamma_n(\underline{x}, t))$ with $\gamma_i(\underline{x}, t) = \exp(t\mathcal{X}).x_i$. Since $exp(t\mathcal{X})$ is a $\mathcal{K}[t]$-automorphism of $\mathcal{K}[\mathcal{V}_f][t]$, we have

$$f_i(\gamma(\underline{x}, t)) = \exp(t\mathcal{X}).f_i(\underline{x})$$

for any $i = 1, \ldots, n-1$. According to the fact that $\mathcal{X}(f_i) = 0$, this gives

$$f_i(\gamma(\underline{x}, t)) = f_i(\underline{x}) \tag{1.1}$$

Let $d_i = \deg_t(\gamma_i(\underline{x}, t))$ and $\alpha \in \mathcal{V}_f$ be such that $\deg(\gamma_i(\alpha, t)) = \deg_t(\gamma_i(\underline{x}, t))$ for any $i = 1, \ldots, n$. This means that $d_i = \deg_{\mathcal{X}}(x_i)$.

On the other hand, the fact that $f_i(\alpha) = 0$ implies that $f_i(\gamma(\alpha, t)) = 0$ for any $i = 1, \ldots, n-1$, and therefore the algebraic curve $\mathcal{C}_f$ parametrized by $\gamma(\alpha, t)$ belongs to $\mathcal{V}_f$.

Let c be an indeterminate. Clearly, the polynomial $\gamma_i(\underline{\alpha, t}) - c$ is irreducible in $\mathcal{K}(c)[\underline{t}]$, and so it has d_i distinct roots in an algebraic closure $\overline{\mathcal{K}(c)}$ of $\mathcal{K}(c)$. If we denote by $\overline{\mathcal{C}_f}$ the extension of $\mathcal{C}_f$ to $\overline{\mathcal{K}(c)}$, then any root τ of $\gamma_i(\alpha, t) - c$ gives a point β of $\overline{\mathcal{C}_f}$ which satisfies $\beta_i = c$. Conversely, any point β of $\overline{\mathcal{C}_f}$ with $\beta_i = c$ satisfies $\beta = \gamma(\alpha, \tau)$, where $\gamma_i(\alpha, \tau) = c$ for some $\tau \in \overline{\mathcal{K}(c)}$. Thus, d_i is the number of points β of $\overline{\mathcal{C}_f}$ such that $\beta_i = c$. On the other hand, the set of such points includes to the solution set of the system

$$f_1(x) = 0, \ldots, f_{n-1}(x) = 0, \quad x_i = c.$$

By Bézout theorem, this system has at most $\prod_{i=1}^{n-1} \deg(f_i)$ solutions, which implies that $d_i \leq \prod_{i=1}^{n-1} \deg(f_i)$. ■

In the case of two variables, this result is the same as the one given in [41, Theorem 1.3.52]. This is due to the fact that every locally nilpotent derivation in two variables is of the jacobian form $\partial_{x_2} f \partial_{x_1} - \partial_{x_1} f \partial_{x_2}$ for some $f \in \mathcal{K}[x_1, x_2]$. In hope to give a local nilpotency criterion for any derivation of $\mathcal{K}[\underline{x}]$, we state the following conjecture which has been proved for the triangular derivations case.

LNC Conjecture : Let $\mathcal{X} \in \mathcal{D}_{\mathcal{K}}(\mathcal{K}[\underline{x}])$ be a locally nilpotent derivation. Then $\mathcal{X}^{m+1}(x_i) = 0$ for all i, where $m = \sum_{j=0}^{n-1} d^j$ where $d = max_i(\deg_{\mathcal{X}}(x_i))$.

1.1.3 Finite generation of the ring of constants

Let $r \in \mathcal{A}$ and $\xi_r = \pi_r \circ \exp(t\mathcal{X})$, where $\pi_r : \mathcal{A}[t] \longrightarrow \mathcal{A}$ is the substitution homomorphism defined by $\pi_r(g(t)) = g(r)$. For each element a of $\mathcal{A}$ and by a simple computation we have the following algebraic identity, see [41, Lemma 1.3.20]

$$a = \sum \frac{1}{i!} \xi_{-r}(\mathcal{X}^i(a)) r^i \tag{1.2}$$

In case s is a slice of $\mathcal{X}$, for any $a \in \mathcal{A}$, the coefficients $\xi_{-s}(\mathcal{X}^i(a))$ belong to $\mathcal{A}^{\mathcal{X}}$ for any i. This yields the following fundamental result, which dates back a least to [99].

Proposition 1.1.7 *Let $\mathcal{A}$ be a $\mathcal{K}$-algebra and $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{A}$ with a slice s. Then $\mathcal{A}$ is a polynomial ring in s over $\mathcal{A}^{\mathcal{X}}$, i.e., $\mathcal{A} = \mathcal{A}^{\mathcal{X}}[s]$. Moreover, $\mathcal{X} = \partial_s$.*

An interesting question, when studying derivations, is to describe their rings of constants. This question has a special interest since it can be related to some other problems as, for instance, the cancellation problem. In the case of polynomial rings over a field, it is given as:

Finite generators Problem : Let $\mathcal{A} := \mathcal{K}^{[n]}$ and $\mathcal{X}$ be a derivation on $\mathcal{A}$. Is it true that $\mathcal{A}^{\mathcal{X}}$ is a finitely generated $\mathcal{K}$-algebra?

As a consequence of (1.2), we have the following important result, which completely solves this problem in case of locally nilpotent derivations having slices, see [41, Corollary 1.3.23].

Lemma 1.1.8 *Let $\mathcal{A}$ be a $\mathcal{K}$-algebra. Let $\mathcal{X}$ be a locally nilpotent derivation on $\mathcal{A}$ having a slice s. Then $\mathcal{A}^{\mathcal{X}} = \xi_{-s}(A)$. In particular, if $\mathcal{G}$ is a generating set for $\mathcal{A}$, then $\xi_{-s}(\mathcal{G})$ is a generating set for $\mathcal{A}^{\mathcal{X}}$.*

In case of locally nilpotent derivations without slices, an algorithm of computing all generators of the ring of constants has been given by van den Essen. This algorithm provided that the ring of constants to be finitely generated, see [37] or [41, p. 37, 1.4]. For derivations, which are not necessarily locally nilpotent, the algorithm given by S. Maubach [75] can be used to compute generators of the ring of constants up to a certain predetermined degree bound. The same author proved that this problem has an affirmative answer for a special class of derivations, namely the triangular monomial derivations, see [76]. In [67] S. Kuroda gave a sufficient condition for finite generation of the ring of constants, but this holds just for homogeneous derivations on a finitely generated graded normal domain over a field.

As proven in [30], this problem is closely related to the famous 14-th problem of Hilbert which asks if, for any subfield $\mathcal{L}$ of the rational function field $\mathcal{K}(\underline{x})$ containing $\mathcal{K}$, the ring $\mathcal{L} \cap \mathcal{K}[\underline{x}]$ is finitely generated $\mathcal{K}$-algebra. In [102] G. Zariski proved that the Hilbert's 14-th Problem has an affirmative answer in case the transcendence degree of $\mathcal{L}$ over $\mathcal{K}$ is at most 2. As a consequence of this we have the following result due to M. Nagata and A. Nowicki [82].

Corollary 1.1.9 *Let $\mathcal{X}$ be a derivation of $\mathcal{K}[\underline{x}]$. If $n \leq 3$ then the ring $\mathcal{K}[\underline{x}]^{\mathcal{X}}$ is finitely generated over $\mathcal{K}$.*

For the case $n \geq 4$, some counterexamples have been given to this problem. For instance, the well-known counterexample of P. Roberts in [88] was generated in [39, 64] to prove the existence of locally nilpotent derivations with non-finitely generated ring of constants in all dimension higher than 7. In [24] D. Daigle and G. Freudenburg adapted the counterexample constructed by G. Freudenburg [53] in 6 variables, to give another one, in the case $n = 5$, which realized as the kernel of the following triangular derivations

$$\mathcal{X} = x_1^2 \partial_{x_3} + (x_1 x_3 + x_2)\partial_{x_4} + x_4 \partial_{x_5}$$

in the polynomial ring $\mathcal{K}[x_1, x_2, x_3, x_4, x_5]$. The four dimensional case, still remains unknown. However, recently S. Kuroda in [69] realized that the counterexample he gave in [68] for the 14-th problem of Hilbert can be achieved as a ring of constants of a derivation. Thereby, the Finite generators Problem is completely treated for the case of polynomial ring over a field.

If we restrict to the case of polynomial rings in two variables, we have the following stronger theorem due to Nagata and Nowicki [82].

Theorem 1.1.10 *Let $\mathcal{X}$ be a nonzero derivation of $\mathcal{K}[x,y]$. Then there exists a polynomial f such that $\mathcal{K}[x,y]^{\mathcal{X}} = \mathcal{K}[f]$.*

This result may be extended by replacing the ground field $\mathcal{K}$ by any unique factorization domain of characteristic zero, see [33, 14].

Remark 1.1.11 *It is possible to have a trivial ring of constants, i.e., $\mathcal{K}[x,y]^{\mathcal{X}} = \mathcal{K}$. An example of such case is given in [83, 7.3.1].*

The following result is proved by Miyanishi [81] for the case $\mathcal{K} = \mathbb{C}$ and can be extended to the general case in a straightforward way by using Kambayashi's transfer principle [62], see also [15] for an algebraic proof.

Theorem 1.1.12 *Let $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{K}[x,y,z]$. Then there exist $f, g \in \mathcal{K}[x,y,z]$ such that $\mathcal{K}[x,y,z]^{\mathcal{X}} = \mathcal{K}[f,g]$.*

Contrary to Theorem 1.1.10 which is of algorithmic nature, it is not clear from the existing proofs of Theorem 1.1.12 how to compute, for a given locally nilpotent derivation $\mathcal{X}$ of $\mathcal{K}[x,y,z]$, two polynomials f, g such that $\mathcal{K}[x,y,z]^{\mathcal{X}} = \mathcal{K}[f,g]$.

1.2 Characterization of locally nilpotent derivations

Understanding locally nilpotent derivations on polynomial rings over a field is one of the basic problems in the study of derivations. The case of one variable is clear, namely all locally nilpotent derivations in $\mathcal{K}[x]$ are of the form $\alpha\partial_x$ for some $\alpha \in \mathcal{K}$.

In two variables case, the following result due to R. Rentschler, gives a complete description of locally nilpotent derivations [87].

Theorem 1.2.1 *Let $\mathcal{X}$ be a nonzero locally nilpotent derivation on $\mathcal{K}[x,y]$. Then there exists two polynomials $f, g \in \mathcal{K}[x,y]$ and a univariate polynomial h such that $\mathcal{K}[x,y] = \mathcal{K}[f,g]$, $\mathcal{K}[x,y]^{\mathcal{X}} = \mathcal{K}[f]$ and $\mathcal{X} = h(f)\partial_g$.*

As a consequence of this theorem, if $\mathcal{A}$ is a unique factorization domain containing $\mathbb{Q}$ and $\mathcal{X}$ is a locally nilpotent derivation of $\mathcal{A}[x,y]$, then there exists $f \in \mathcal{A}[x,y]$ and a univariate polynomial h such that $\mathcal{A}[x,y]^{\mathcal{X}} = \mathcal{A}[f]$ and $\mathcal{X} = h(f)(\partial_y f \partial_x - \partial_x f \partial_y)$, see [23]. In case $\mathcal{A}$ is an arbitrary ring, the situation is much more involved, see e.g., [**?**]. However, we have the following result from [11, Theorem 3.3].

Theorem 1.2.2 *Let $\mathcal{A}$ be a Noetherian domain containing $\mathbb{Q}$ and $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{A}[x,y]$ such that $1 \in \mathcal{I}(\mathcal{X}(x), \mathcal{X}(y))$. Then there exists a polynomial f such that $\mathcal{A}[x,y]^{\mathcal{X}} = \mathcal{A}[f]$ and $\mathcal{X}$ has a slice s. In particular, $\mathcal{A}[x,y] = \mathcal{A}[f,s]$ and $\mathcal{X} = \partial_s$.*

By using Theorem 1.1.12, D. Daigle gave the following useful result, which describes all locally nilpotent derivations in three variables case [22].

Proposition 1.2.3 *Any nonzero locally nilpotent derivation $\mathcal{X}$ of $\mathcal{K}[x,y,z]$ is a multiple of the Jacobian derivation, i.e, $\mathcal{X} = a\mathcal{X}_{f,g}$, where $a \in \mathcal{K}[x,y,z]^{\mathcal{X}}$.*

It is well known that for $n \geq 4$ the ring of constants of a locally nilpotent derivation is not necessary generated by $n-1$ elements, see for example [84]. However, in case the transcendence degree of $\mathcal{Q}t(\mathcal{A})$ is finite, where $\mathcal{A}$ is a $\mathcal{K}$-domain, we have the following algebraic identity

$$\mathrm{trdeg}_{\mathcal{K}}\mathcal{Q}t(\mathcal{A}^{\mathcal{X}}) = \mathrm{trdeg}_{\mathcal{K}}(\mathcal{Q}t(\mathcal{A}))^{\mathcal{X}} - 1 \tag{1.3}$$

This means that the ring of constants always contains $n-1$ algebraically independent elements. Using this result, we get the following theorem due to Makar-Limanov in the case of polynomial rings over a field, see [70, Lemma 8].

Theorem 1.2.4 *Let $\mathcal{X}$ be an irreducible locally nilpotent derivation of $\mathcal{A} = \mathcal{K}^{[n]}$ and $f_1, \ldots, f_{n-1}$ be $n-1$ algebraically independent elements of $\mathcal{A}^{\mathcal{X}}$. Then there exists a nonzero element $a \in \mathcal{Q}t(\mathcal{A}^{\mathcal{X}})$ such that $\mathcal{X} = a\mathcal{X}_{f_1,\ldots,f_{n-1}}$. In particular, $\mathcal{X}_{f_1,\ldots,f_{n-1}}$ is locally nilpotent.*

A generalization of this result is also given by the same author. He gave a description of all locally nilpotent derivations of any affine $\mathcal{K}$-domain, where $\mathcal{K}$ is algebraically closed. For more detail we refer to [72].

1.3 One-parameter subgroups of the polynomial automorphism group

Let $\mathcal{K}$ be a field and $\mathcal{K}[\underline{x}]$ be the ring of polynomials in n variables with coefficients in $\mathcal{K}$. Let $\sigma = (f_1, \ldots, f_n)$ be an n-uple in $\mathcal{K}[x]^n$. Consider the endomorphism of $\mathcal{K}[\underline{x}]$ which send each x_i to f_i, this endomorphism can be seen as a polynomial map of the space $\mathcal{K}^n$ given by the substitution

$$a = (a_1, \ldots, a_n) \longmapsto \sigma(a) = (f_1(a), \ldots, f_n(a))$$

for all elements $a \in \mathcal{K}^n$. We say that σ is a polynomial automorphism of $\mathcal{K}[\underline{x}]$, if $\mathcal{K}[\underline{x}] = \mathcal{K}[f_1, \ldots, f_n]$. The collection of all automorphisms of $\mathcal{K}[\underline{x}]$ will be denoted by $Aut_{\mathcal{K}}(\mathcal{K}[\underline{x}])$ and called the group of $\mathcal{K}$-automorphisms of $\mathcal{K}[\underline{x}]$. One of the known automorphisms is the so-called the affine automorphism, i.e., the automorphism $\sigma \in Aut_{\mathcal{K}}(\mathcal{K}[\underline{x}])$ such that $\deg(\sigma(x_i)) = 1, i = 1, \ldots, n$. Another one is the so-called triangular automorphism, i.e., the automorphism defined as

$$\sigma(x_i) = a_i x_i + f(x_1, \ldots, x_{i-1}), a_i \in \mathcal{K}^*, i = 1, \ldots, n$$

The tame subgroup of $Aut_{\mathcal{K}}(\mathcal{K}[\underline{x}])$ is the subgroup generated by the affine and triangular automorphisms, and is denoted by $TA_{\mathcal{K}}(\mathcal{K}[\underline{x}])$. Automorphisms which belong to $TA_{\mathcal{K}}(\mathcal{K}[\underline{x}])$ are called tame, and those which are not tame are called wild.

Automorphisms of $\mathcal{K}^{[2]}$ are well understood. They are all tame and $Aut_{\mathcal{K}}(\mathcal{K}^{[2]})$ is the free amalgamated product of affine and triangular automorphisms along their intersection, see [66, 59]. However, $Aut_{\mathcal{K}}(\mathcal{K}^{[n]})$ remains a big mystery for the case $n \geq 3$. Recently, an algorithm for recognizing tame automorphisms in three dimensional case is given in [94], as a consequence of that, the existence of wild automorphisms was established.

In spite of many advances in this direction, it still difficult to describe this group. Moreover, one still does not know what it is necessary to add with the tame automorphisms to obtain them all and this question appears well far from being solved. An attempt to start the study of $Aut_{\mathcal{K}}(\mathcal{K}[\underline{x}])$ is to investigate its one-parameter subgroups, namely algebraic actions of $(\mathcal{K}, +)$ on the affine n-space over $\mathcal{K}$. Such actions are commonly called algebraic G_a-actions, and are of the form $\exp(t\mathcal{X})_{t\in\mathcal{K}}$, where $\mathcal{X}$ is a locally nilpotent derivation of $\mathcal{K}[\underline{x}]$. So studying one-parameter subgroups of $Aut_{\mathcal{K}}(\mathcal{K}[\underline{x}])$ can be reduced to the study locally nilpotent derivations of $\mathcal{K}[\underline{x}]$. In regard to this, the classification problem of algebraic actions on $\mathcal{K}^n$ can be reduced to the classifications of locally nilpotent derivations of $\mathcal{K}[\underline{x}]$.

As shown in Theorem 1.2.1, all locally nilpotent derivations in two variables are clearly classified. Moreover, this classification is algorithmic. In three dimensional case, several deep results which constitute a big step towards a classification of locally nilpotent derivations are obtained, Proposition 1.2.3 is one of them, see also [54] and the references therein. However, some of these results, which are obtained by using topological methods, are not of algorithmic nature.

Recently in [29], D. Daigle studied the so-called basic elements in three variables over a field, i.e., irreducible polynomials which belong to, at least, two rings of constants, and in an attempt to approach the classification problem of locally nilpotent derivations in three variables, he asks if every ring of constants of a locally nilpotent derivation contains a basic element of $\mathcal{K}[x, y, z]$.

It would be very useful to obtain an algorithmic classification of locally nilpotent derivations in dimension three, but this seems to be a difficult problem. One way to approach this is to classify derivations according to their rank. In chapter 3, we address the less ambitious problem of computing some invariants, namely the plinth ideal and the rank, of locally nilpotent derivations in dimension three, and as a consequence, we will show that the rank of a locally nilpotent derivation in dimension three can be computed by using classical techniques of computational commutative algebra, namely Gröbner bases and functional decomposition of multivariate polynomials.

1.4 Coordinates in polynomial rings

A polynomial $f \in \mathcal{K}[\underline{x}]$ is called coordinate if there exists a list of polynomials $f_1, \ldots, f_{n-1}$ such that $\mathcal{K}[\underline{x}] = \mathcal{K}[f, f_1, \ldots, f_{n-1}]$. In the same way, a list $f_1, \ldots, f_r$ of polynomials, with $r \leq n$, is called a system of coordinates if there exists a list $f_{r+1}, \ldots, f_n$ of polynomials such that $\mathcal{K}[\underline{x}] = \mathcal{K}[f_1, ..., f_n]$. A system of coordinates of length n will be called a coordinate system. The study of coordinates in polynomial rings over fields naturally leads to do the same but over rings. Given a ring $\mathcal{A}$ and $f \in \mathcal{A}[\underline{x}]$, we say that f is a residual coordinate if f is a coordinate of $\mathcal{K}_{\mathcal{P}}[\underline{x}]$ for any prime ideal $\mathcal{P}$ of $\mathcal{A}$, where $\mathcal{K}_{\mathcal{P}}$ stands for the residual field of $\mathcal{A}$ in $\mathcal{P}$.

Studying coordinates in the polynomial ring $\mathcal{K}[\underline{x}]$, is one of the major topics in the study of its group of automorphisms $Aut_{\mathcal{K}}(\mathcal{K}[\underline{x}])$. Some work in this direction has been achieved, see for instance [43, 12, 32]. For example, in [43] several ways to characterize coordinates in two variables over $\mathbb{Q}$-algebras are given. Also, various results about coordinates in two variables, that were previously known only for fields, are extended to arbitrary $\mathbb{Q}$-algebras. The following theorem is one of them, it is proved in [15] for the Noetherian case and extended to the general case in [43].

Theorem 1.4.1 *Let $\mathcal{A}$ be a ring containing $\mathbb{Q}$. Then any residual coordinate of $\mathcal{A}[x, y]$ is a coordinate of $\mathcal{A}[x, y]$.*

A well-known conjecture of Abhyankar and Sathaye concerning coordinates states that:

Abhyankar-Sathaye Conjecture: Let $f \in \mathcal{K}[\underline{x}]$ such that $\mathcal{K}[\underline{x}]/f \simeq_{\mathcal{K}} \mathcal{K}^{[n-1]}$. Then f is a coordinate in $\mathcal{K}[\underline{x}]$.

This conjecture is proved by the famous Abhyankar-Moh's theorem [1] in the case of two variables. Whereas, for $n \geq 3$, it is still open in spite of much research in this direction. However, in the case of three variables, we have the following result proved by Kaliman in [60] for the case $\mathcal{K} = \mathbb{C}$ and extended to the general case in [28].

Theorem 1.4.2 *Let f be a polynomial in $\mathcal{K}[x, y, z]$ and assume that for all but finitely many $\alpha \in \mathcal{K}$ the $\mathcal{K}$-algebra $\mathcal{K}[x, y, z]/(f - \alpha)$ is $\mathcal{K}$-isomorphic to $\mathcal{K}^{[2]}$. Then f is a coordinate of $\mathcal{K}[x, y, z]$.*

A polynomial f of $\mathcal{K}[\underline{x}]$ is called a local coordinate if it satisfies

$$\mathcal{K}(f)[\underline{x}] \simeq_{\mathcal{K}(f)} \mathcal{K}(f)^{[n-1]}.$$

As a consequence of Theorem 1.4.2, any local coordinate of $\mathcal{K}[x, y, z]$ is in fact a coordinate, see [35]. The original proof of Theorem 1.4.2 is of topological nature, and it is not clear how to compute polynomials g, h such that $\mathcal{K}[f, g, h] = \mathcal{K}[x, y, z]$.

In algorithmic point of view, checking whether a given polynomial of $\mathcal{A}[\underline{x}]$ is a coordinate is still an open problem for $n \geq 3$. Coordinates of one variable are obviously clear, namely, every coordinate of $\mathcal{A}[x]$ is of the form $ax + b$, with a is a unit of $\mathcal{A}$ and $b \in \mathcal{A}$. In the case of two variables and $\mathcal{A}$ is a field, the first result of this direction was that of S. Abhyankar and T. Moh in [1]. They proved that a polynomial $f \in \mathcal{K}[x, y]$ is coordinate if and only if $(\partial_x f, \partial_y f) = 1$ and the curve $\mathcal{C}_f$ defined by $f = 0$ has one place at infinity. Then various and more or less explicit solutions have been given to this problem, see e.g., [38, 18, 19, 95, 17, 13].

However, the closely related question of computing a coordinate's mate, i.e., a polynomial g such that $\mathcal{K}[f, g] = \mathcal{K}[x, y]$, is either not treated or solved in a more or less involved way, see [13]. For instance, in [19] an integral formula is given for computing a Jacobian mate, i.e. a polynomial g such that $\mathrm{Jac}(f, g) = 1$, and as a by-product, it solves the question of coordinate's mate. In [95], the same question is solved by keeping track of the so-called nonsingular Gröbner reductions performed to check whether f is a coordinate.

In chapter 2 we will show another algorithmic criterion of coordinates in two variables over a unique factorization domain $\mathcal{A}$ of characteristic zero. A notable feature of this method is that it always produces a mate of minimum degree.

Chapter 2

Coordinates in two variables over UFD's

This chapter is devoted to the recognition problem of coordinates in a polynomial ring in two variables over a unique factorization domain. First, we are interested in algorithmically recognizing coordinates and computing mates over fields of characteristic zero. We show also that the method we describe always produces a younger mate. Then we study coordinates in two variables over UFD's of characteristic zero and give algorithmic solutions to both the recognition and the mate problems.

2.1 Basic facts

Let $\mathcal{A}$ be a ring with unit containing the rational numbers and $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{A}$. A triangular polynomial $f = ay + p(x)$ (resp., $bx + q(y)$) of $\mathcal{A}[x, y]$ is a coordinate if and only if a (resp., b) is a unit of $\mathcal{A}$, and if so $g = x$ (resp. $g = y$) is a coordinate's mate of f. The triangular case being trivial, so from now on we will assume that the considered polynomials are non-triangular.

The following lemma is a classical result concerning automorphisms of the affine plane, and can be found in [78].

Lemma 2.1.1 *Let $\mathcal{A}$ be a domain of characteristic zero and (f, g) be an automorphism of $\mathcal{A}[x, y]$, and let $\deg(f(0, y)) = d_1$ and $\deg(g(0, y)) = d_2$. Then $\deg_y(f) = d_1$ and $\deg_y(g) = d_2$. Moreover, if both d_1 and d_2 are positive, then f and g are monic with respect to y and $d_1|d_2$ or $d_2|d_1$.*

The following lemma is useful and its general case can be found in [41, Proposition 1.1.31, p. 11].

Lemma 2.1.2 *Let $\mathcal{K}$ be a field and let f and g be two polynomials in $\mathcal{K}[x, y]$ such that $\mathrm{Jac}(f, g) = 1$. Then f and g are algebraically independent over $\mathcal{K}$.*

Proof. Assume that there is a polynomial $h \in \mathcal{K}[x, y]$ of minimal degree such that $h(f, g) = 0$. Then we have

$$\partial_x h(f, g)\partial_x f + \partial_y h(f, g)\partial_x g = 0, \tag{2.1}$$

$$\partial_x h(f,g)\partial_y f + \partial_y h(f,g)\partial_y g = 0. \tag{2.2}$$

Multiplying the equation (2.1) by $\partial_y g$ and the equation (2.2) by $\partial_x g$ we obtain

$$\partial_x h(f,g)\mathrm{Jac}(f,g) = 0.$$

In the same way, by multiplying the equation (2.1) by $\partial_y f$ and the equation (2.2) by $\partial_x f$ we get

$$\partial_y h(f,g)\mathrm{Jac}(f,g) = 0.$$

Since h is assumed to be of minimal degree, then

$$\partial_x h(x,y) = \partial_y h(x,y) = 0. \tag{2.3}$$

Since $\mathcal{K}$ is of characteristic zero, then the identity (2.3) means that h is constant and so $h = 0$. ∎

A basic fact concerning slices of locally nilpotent derivations is given in the following theorem which is a consequence of Theorem 1.1.10 and Proposition 1.1.7. The proof we supply here is elementary and constructive.

Theorem 2.1.3 *Let $\mathcal{A}$ be a UFD of characteristic zero and $\mathcal{X} = \mathcal{X}_f$ be a locally nilpotent derivation of $\mathcal{A}[x,y]$. Assume that $\mathcal{X}$ has a slice g. Then $\mathcal{A}[x,y]^{\mathcal{X}} = \mathcal{A}[f]$ and $\mathcal{A}[x,y] = \mathcal{A}[f,g]$.*

Proof. The case where f is linear is trivial, so we will assume in the sequel that f is nonlinear. Let P be a polynomial in $\mathcal{A}[x,y]^{\mathcal{X}}$. By induction on the degree of P, we will prove that $P \in \mathcal{A}[f]$. The case when $\deg(P) = 0$ is clear. Assume now that the result remains true for every polynomial of degree at most m and let P be a polynomial of $\mathcal{A}[x,y]^{\mathcal{X}}$ of degree $m+1$. Then

$$\partial y f \partial x P - \partial x f \partial y P = 0.$$

On the other hand we have

$$\partial y f \partial x g - \partial x f \partial y g = 1.$$

From the two last equalities we obtain the relations

$$\begin{cases} \partial x P = F(x,y)\partial x f, \\ \partial y P = F(x,y)\partial y f, \end{cases}$$

where $F(x,y) = \partial x g \partial y P - \partial y g \partial x P$. Since f is nonlinear then $\deg(F) \leq m$. On the other hand, an easy computation shows that $\partial_x F \partial_y f - \partial_y F \partial_x f = 0$. By induction hypothesis, we may write $F(x,y) = h(f)$ with $h \in \mathcal{A}[T]$. This proves that $P = H(f) + \alpha$, where $H \in \mathcal{Q}t(\mathcal{A})[T]$ is such that $H' = h$.
Now, we turn to prove that H has its coefficients in $\mathcal{A}$. Since $\mathcal{A}$ is a UFD there is an element β of $\mathcal{A}$ such that $H_1 = \beta H \in \mathcal{A}[t]$ and $H_1(t)$ is primitive. Therefore $\beta P(x,y) = H_1(f)$, which gives

$$H_1(f) = 0 \mod \beta. \tag{2.4}$$

Assume that β is not a unit in $\mathcal{A}$ and let c be a prime factor of β. On the first hand, the fact that $\mathcal{X}_f(g) = 1$ implies that f is nonconstant in $(\mathcal{A}/c)[t]$. On the other hand, equation 2.4 gives

$$H_1(f) = 0 \mod c,$$

and hence $H_1(t) = 0 \mod c$ according to the fact that $\mathcal{A}/c$ is a domain and f is nonconstant in $(\mathcal{A}/c)[t]$. But this means that c divides the coefficients of H_1, and contradicts the fact that H_1 is primitive. Thus, β is a unit in $\mathcal{A}$ and so H has its coefficients in $\mathcal{A}$.

The fact that $\mathcal{X}$ remains locally nilpotent in $\mathcal{Q}t(\mathcal{A})[x, y]$ implies that (f, g) is an automorphism of $\mathcal{Q}t(\mathcal{A})[x, y]$. Let (f_1, g_1) be the inverse of (f, g), and let us prove that f_1 and g_1 are in fact polynomials in $\mathcal{A}[x, y]$. Since $\mathcal{A}$ is a UFD there is an element λ of $\mathcal{A}$ such that $f_2 = \lambda f_1$ is primitive in $\mathcal{A}[x, y]$.

Assume that λ is not a unit of $\mathcal{A}$ and let c be a prime divisor of λ. From the identity $f_2(f, g) = \lambda x$, we deduce that

$$f_2(f, g) = 0 \mod (c),$$

and by lemma 2.1.2 we get

$$f_2(x, y) = 0 \mod (c).$$

But this means that c divides all the coefficients of f_2, and this contradicts the assumption that f_2 is primitive. Thus, λ is a unit in $\mathcal{A}$ and so f_1 has its coefficients in $\mathcal{A}$. In the same way we prove that $g_1 \in \mathcal{A}[x, y]$. ▪

2.2 Coordinates over a field

In this section we present another criterion for the Recognizing Coordinate's Problem in the case of a field of characteristic zero. A notable feature of this criterion is that it gives a simple solution to the question of coordinate's mate. Moreover, the produced coordinate's mate is always of minimal degree.

The following theorem, which gives an algorithmic characterization of coordinates in two variables over a field, is the main result in this section.

Theorem 2.2.1 *Let $\mathcal{K}$ be a field and f be a non-triangular polynomial in $\mathcal{K}[x, y]$. Then f is a coordinate if and only if the two following conditions hold:*

i) the derivation $\mathcal{X}_f$ is locally nilpotent,

ii) $r_1 = \deg_{\mathcal{X}_f} x \geq 2$ and $\mathcal{X}_f^{r_1}(x)$ is constant.

In this case, also $r_2 = \deg_{\mathcal{X}_f} y \geq 2$ and $\mathcal{X}_f^{r_2}(y)$ is constant and $\mathcal{X}_f^{r_1-1}(x)$, as well as $\mathcal{X}_f^{r_2-1}(y)$, is a coordinate's mate of f.

Proof. $\Rightarrow$) Let g be a coordinate mate of f. Without loss of generality, we may assume that $\mathcal{X}_f(g) = 1$. This proves in particular that $\mathcal{X}_f^2(g) = 0$. Since on the other hand $\mathcal{X}_f(f) = 0$ and $\mathcal{K}[x, y] = \mathcal{K}[f, g]$, we deduce that $\mathcal{X}_f$ is locally nilpotent.
Let (f_1, g_1) be the inverse of (f, g). So $x = f_1(f, g)$. Since $\mathcal{X}_f = \partial_g$, it follows that

$$\mathcal{X}_f^i(x) = (\partial_{y^i}^i f_1)(f, g) \tag{2.5}$$

for all i. Write $f_1 = \sum a_i(x)y^i$, with $\deg_y f_1 = r$. Then by lemma 2.1.1 $a_r \in \mathcal{K}^*$ and hence $\mathcal{X}_f^r(x) = r!a_r \in \mathcal{K}^*$. This shows that $\deg_{X_f} x = r$. The fact that $r \geq 2$ follows from the assumption that f is non-triangular.

Finally, $\mathcal{X}_f^{r-1}(x) = r!a_r g + (r-1)!a_{r-1}(f)$, which is clearly a coordinate's mate of f.

$\Leftarrow$) By Theorem 2.1.3 $\mathcal{K}[x, y] = \mathcal{K}[f, g]$, where $g = (\mathcal{X}_f^{r_1}(x))^{-1}\mathcal{X}_f^{r_1-1}(x)$. ∎

The following algorithm gives the main steps to be performed in order to check that f is coordinate over $\mathcal{K}$ and if so to compute its mate.

Algorithm 1: Coordinate's algorithm over field

Input : A polynomial $f \in \mathcal{K}[x, y]$.
Output : Either a message that f is not coordinate or a mate $g \in \mathcal{K}[x, y]$ of f.

for i to $\deg f + 1$ **do**
  Compute $\mathcal{X}_f^i(x)$ and $\mathcal{X}_f^i(y)$
  if $\mathcal{X}_f^{r_1+1}(x) = 0$ and $\mathcal{X}_f^{r_2+1}(y) = 0$ for some $r_1, r_2 \leq \deg f$ **then**
    if $\mathcal{X}_f^{r_1}(x)$ and $\mathcal{X}_f^{r_2}(y)$ are nonzero constants **then**
      f is coordinate and $(\mathcal{X}_f^{r_1}(x))^{-1}\mathcal{X}_f^{r_1-1}(x)$, as well as, $(\mathcal{X}_f^{r_2}(y))^{-1}\mathcal{X}_f^{r_2-1}(y)$ is a coordinate's mate of f.
    else
      f is not coordinate
    end if
  else
    f is not coordinate
  end if
end for

Remark 2.2.2 *This result shows that the necessary computations performed to check whether $\mathcal{X}_f$ is locally nilpotent, namely the computation of the iterates $\mathcal{X}_f^i(x)$ and $\mathcal{X}_f^i(y)$ up to $\deg(f)+1$, are enough for checking whether f is a coordinate and for computing a coordinate's mate in case it exists. Moreover, the obtained coordinate's mate is younger as we will show in the next.*

2.2.1 The inverse formula of polynomial automorphisms

Let $\mathcal{A}$ be a commutative ring with unit containing the rational numbers and let $\mathcal{A}[\underline{x}]$ be a polynomial ring. Let $F = (f_1, \ldots, f_n)$ be an automorphism of $\mathcal{A}[\underline{x}]$. A well known method to compute the inverse of F is to compute the Gröbner basis of the ideal $\mathcal{I}(f_1 - u_1, \dots, f_n - u_n)$ in the polynomial ring $\mathcal{K}[\underline{x}, \underline{u}]$, with respect to the lexicographic order $x_1 \succ \dots \succ x_n \succ u_1 \succ \dots \succ u_n$, which is of the form $\{x_1 - g_1, \dots, x_n - g_n\}$, where g_i are polynomials in $\mathcal{K}[\underline{u}]$. In this case, if we let $G = (g_1, \dots, g_n)$, then G is the inverse of F, see [36] or [41, 3.2, p. 63]. Using the derivation theory, another formula of the inverse of polynomial automorphisms is given in [41, Proposition 3.1.4, p. 62] by computing, for each $d \geq 1$, the homogeneous component of degree d of F. M. El Kahoui, in unpublished work, gave a determinantal formula, similar to the McKay-Wong one [78], for computing the inverse of a polynomial automorphism of an affine plane by using the subresultant theory.

From the proof of Theorem 2.2.1, we deduce another formula which gives an expression of the inverse of an automorphism of $\mathcal{K}[x, y]$ (formula (2.5)). In fact, this can be established in the more general case of automorphisms of $\mathcal{A}[\underline{x}]$, where $\mathcal{A}$ is a commutative ring with unit containing the rational numbers.

Given $n-1$ polynomials $f_1, \dots, f_{n-1}$ in $\mathcal{A}[\underline{x}]$, let $\mathcal{X}_{f_1,\dots,f_{n-1}}$ be the Jacobian derivation of $\mathcal{A}[\underline{x}]$. When $F = (f_1, \dots, f_n)$ is an $\mathcal{A}$-automorphism of $\mathcal{A}[\underline{x}]$, the derivation $\mathcal{X}_{f_1,\dots,f_{n-1}}$ is locally nilpotent since

$$\mathcal{X}_{f_1,\dots,f_{n-1}}(f_i) = \delta_{i,n}.$$

Proposition 2.2.3 *Let $F = (f_1, \dots, f_n)$ be an $\mathcal{A}$-automorphism of $\mathcal{A}[\underline{x}]$ with 1 as Jacobian determinant, and $G = (g_1, \dots, g_n)$ be its inverse. Then for any $i = 1, \dots, n$ we have:*

$$\exp(t\mathcal{X}_{f_1,\dots,f_{n-1}}).x_i = g_i(f_1, \dots, f_{n-1}, t + f_n).$$

Proof. If we let $g_i(x) = \sum_j a_{i,j}(x_1, \dots, x_{n-1})x_n^j$, then we have the identity

$$\sum_j a_{i,j}(f_1, \dots, f_{n-1})f_n^j = x_j.$$

Applying $\mathcal{X}_{f_1,\dots,f_{n-1}}$ to the last equation we get

$$\mathcal{X}_{f_1,\dots,f_{n-1}}(x_i) = (\partial_{x_n} g_i)(f_1, \dots, f_n),$$

and by induction we easily prove that

$$\mathcal{X}^k_{f_1,\dots,f_{n-1}}(x_i) = (\partial^k_{x_n^k} g_i)(f_1, \dots, f_n)$$

for any k. Taking into account these relations we get

$$\exp(t\mathcal{X}_{f_1,\dots,f_{n-1}}).x_i = \sum_k \frac{1}{k!}(\partial^k_{x_n^k} g_i)(f_1, \dots, f_n)t^k.$$

The right hand side of the last equation is nothing other than the Taylor expansion of $g_i(f_1, \dots, f_{n-1}, t + f_n)$ around f_n. ∎

2.2.2 The question of younger mate

The aim of this section is to show that the coordinate's mate computed in Theorem 2.2.1 is a younger mate of the given polynomial. First let us begin with the following lemmas which will be needed.

Lemma 2.2.4 *Let $\mathcal{A}$ be a domain and $f, g \in \mathcal{A}[t]$ be two polynomials such that* $\deg(f) = p$, $\deg(g) = q$ *and* $\min(p, q) \geq 2$. *Let* $\mathrm{Res}_t(f - x, g - y)$ *be the resultant of* $f(t) - x$ *and* $g(t) - y$ *with respect to* t. *Then* $\deg_x(\mathrm{Res}_t(f - x, g - y)) = q$, $\deg_y(\mathrm{Res}_t(f - x, g - y)) = p$ *and* $\mathrm{Res}_t(f - x, g - y)$ *is monic with respect to both* x *and* y.

Proof. Let us write $f = c_p t^p + \ldots + c_0$ and $g = d_q t^q + \ldots + d_0$. Let $\mathrm{Sylv}(f(t) - x, g(t) - y) = (a_{j,k})$ be the Sylvester matrix of $f(t) - x$ and $g(t) - y$. The coefficients $a_{j,k}$ are either constants or $c_0 - x$ or $d_0 - y$. Moreover, the number of times $c_0 - x$ (resp. $d_0 - y$) appears in $\mathrm{Sylv}(f(t) - x, g(t) - y)$ is q (resp. p). On the other hand $\mathrm{Res}_t(f - x, g - y)$ is the determinant of the Sylvester matrix, so that the bounds

$$\deg_x(\mathrm{Res}_t(f - x, g - y)) \leq q, \quad \deg_y(\mathrm{Res}_t(f - x, g - y)) \leq p.$$

To prove that these bounds are equalities, we need to be little bit more precise, and give the exact subscripts j, k whose corresponding coefficient is $c_0 - x$ (resp. $d_0 - y$). In fact we have $a_{j,k} = d_0 - y$ if and only if $j \geq q + 1$ and $k = j$. Let us write

$$\mathrm{Res}_t(f - x, g - y) = \sum_{\sigma \in \mathcal{S}_{p+q}} \varepsilon(\sigma) a_{1,\sigma(1)} \cdots a_{p+q,\sigma(p+q)}.$$

In order that a given σ generates a term of the type $c(d_0 - y)^p$ it should satisfy $\sigma(j) = j$ for any $j \geq q + 1$. This means that $\sigma(j) \leq q$ for any $j \leq q$. Therefore, the coefficient of the monomial $(d_0 - y)^p$ in $\mathrm{Res}_t(f - x, g - y)$ is $\det(A_{q,q})$, where $A_{q,q}$ is the $q \times q$ principal submatrix of $\mathrm{Sylv}(f(t) - x, g(t) - y)$. Clearly, $A_{q,q}$ is upper triangular and its diagonal entries are equal to c_p. Thus, we have

$$\mathrm{Res}_t(f - x, g - y) = c_p^q (d_0 - y)^p + r(x, y)$$

with $\deg_y(r) < p$. Similar arguments show that $\mathrm{Res}_t(f - x, g - y)$ is monic of degree q with respect to x. ∎

Lemma 2.2.5 *Let* (f, g) *be an automorphism of* $\mathcal{K}[x, y]$ *and assume that* $\deg(f) > \deg(g)$. *Let* (f_1, g_1) *be the inverse of* (f, g) *and write* $f_1 = a_m y^m + a_{m-1}(x) y^{m-1} + \ldots + a_0(x)$ *and* $g_1 = b_q y^q + b_{q-1}(x) y^{q-1} + \ldots + b_0(x)$. *Then the coefficients* $a_{m-1}(x)$ *and* $b_{q-1}(x)$ *are constant.*

Proof. Even if it means replacing (f, g) by $(f \circ \ell, g \circ \ell)$, where ℓ is a suitable linear transformation, we may assume that $\deg_y(f) = \deg(f)$ and $\deg_y(g) = \deg(g)$. Indeed, such change of coordinates does not affect the condition $\deg(g) < \deg(f)$. Moreover, since the inverse of $(f \circ \ell, g \circ \ell)$ is $\ell^{-1} \circ (f_1, g_1)$, the claimed conclusion will not be modified.

Let u, v be indeterminates. Since (f, g) is an automorphism and according to [41, Theorem 3.3.1], the resultant of $f - u$ and $g - v$ with respect to y writes as

$$\mathrm{Res}_y(f - u, g - v) = \alpha(x - f_1(u, v)).$$

If we let $m = \deg_y(f)$ and $n = \deg_y(g)$, then by Lemma 2.2.4, $f_1(u, v)$ is a polynomial of degree m with respect to v and of degree n with respect to u and its leading coefficients with respect to both u and v are constants. Since the degree of the inverse (f_1, g_1) equals the degree of (f, g), we deduce that f_1 is of degree m.
Let h_m be the leading homogeneous term of f_1. Then h_m is a power of a linear form $av + bu$, and since $\deg_u(h_m) \leq \deg_u(f_1) = n < m$ then $b = 0$. This proves that $a_{m-1}(x)$ is constant. The fact that $b_{q-1}(x)$ is also constant follows immediately form the Jacobian condition. ∎

Now, we are able to give the following result.

Theorem 2.2.6 *Let $\mathcal{K}$ be a field and f be a non-triangular coordinate in $\mathcal{K}[x, y]$. Let $r_1 = \deg_{\mathcal{X}_f} x$ and $r_2 = \deg_{\mathcal{X}_f} y$. Then $(\mathcal{X}_f^{r_1}(x))^{-1}\mathcal{X}_f^{r_1-1}(x)$, as well as $(\mathcal{X}_f^{r_2}(y))^{-1}\mathcal{X}_f^{r_2-1}(y)$, is a younger mate of f.*

Proof. Let g be a younger mate of f such that $\mathrm{Jac}(f, g) = 1$ and let (f_1, g_1) be the inverse of (f, g). Let us write

$$\begin{aligned} f_1 &= a_p y^p + a_{p-1}(x)y^{p-1}, + \ldots + a_0(x) \\ g_1 &= b_q y^q + b_{q-1}(x)y^{q-1} + \ldots + b_0(x). \end{aligned}$$

By Lemma 2.2.5, the coefficients $a_{p-1}(x)$ and $b_{q-1}(x)$ are constant, and taking into account the algebraic identities in Proposition 2.2.3 we obtain the equalities

$$\begin{aligned} &\mathcal{X}_f^p(x) = p!a_p, \quad \mathcal{X}_f^{p-1}(x) = (p-1)!(pa_p g + a_{p-1}), \\ &\mathcal{X}_f^q(y) = q!b_q, \quad \mathcal{X}_f^{q-1}(y) = (q-1)!(qb_q g + b_{q-1}). \end{aligned}$$

Therefore $(\mathcal{X}_f^p(x))^{-1}\mathcal{X}_f^{p-1}(x) = g + (pa_p)^{-1}a_{p-1}$, and this proves the claimed result. ∎

2.3 The case of a UFD of characteristic zero

Recognizing coordinates over rings which are not fields is much more complicated. In [13] an algorithm of recognizing coordinates is given in the case of two variables with coefficients in a finitely generated $\mathcal{K}$-algebra. In this section we address the same problem replacing the ground field $\mathcal{K}$ by a unique factorization domain of characteristic zero $\mathcal{A}$.

2.3.1 Polynomial decomposition

In this subsection we give an efficient solution to the following problem, which will play a crucial role to make our result working in an algorithmic way.

Problem : Let $\mathcal{A}$ be a UFD and a be a nonzero element of $\mathcal{A}$. Let $f, g \in \mathcal{A}[x, y]$. How to check whether $g = h(f) \mod(a)$, where h is a polynomial in $\mathcal{A}[t]$?

In the sequel, $\operatorname{Rem}(g, f; y)$ will stand for the Euclidean remainder of g by f with respect to the variable y. The following lemma is the master piece of the solution we give to this problem.

Lemma 2.3.1 *Let $\mathcal{A}$ be a domain and f, g two elements of $\mathcal{A}[x, y]$. Then $g = h(f)$ if and only if* $\operatorname{Rem}(g, f - t; y) = h(t)$, *where h is a polynomial in $\mathcal{A}[t]$.*

Proof. $\Leftarrow$) Assume that $\operatorname{Rem}(g, f - t; y) = h(t)$ then $g = h(t) \mod(f - t)$ and by substituting f to t we get $g = h(f)$.
$\Rightarrow$) If $g = h(f)$ then $g - h(t) = h(f) - h(t) = (f - t)P$, where P a polynomial in $\mathcal{A}[x, y]$. Since $\deg(h) < deg(f)$, then $\operatorname{Rem}(g, f - t; y) = h(t)$. ∎

Let $\mathcal{A}$ be a UFD, f, g be polynomials in $\mathcal{A}[x, y]$ and a be an element of $\mathcal{A}$. Write $a = a_1^{m_1} \dots a_r^{m_r}$, where the a_i's are irreducible. By using Euclidean division over the domain $\mathcal{A}/(a_1)[x, t]$, we let

$$h_{1,1}(y) = \operatorname{Rem}(g, f - t; y) \mod(a_1), \quad g_{1,1} = a_1^{-1}(g - h_{1,1}(f)),$$

and then for $j = 2, \dots, m_1$ we let

$$h_{1,j}(t) = \operatorname{Rem}(g_{1,j-1}, f - t; y) \mod(a_1), \quad g_{1,j} = a_1^{-1}(g_{1,j-1} - h_{1,j}(f)).$$

We repeat the same process for $a_2, a_3, \dots, a_r$ by letting for any $i = 2, \dots, r$

$$h_{i,j}(t) = \operatorname{Rem}(g_{i,j-1}, f - t; y) \mod(a_i),$$
$$g_{i,j} = a_i^{-1}(g_{i,j-1} - h_{i,j}(f)),$$

where $j = 1, \dots, m_i$ and $g_{i,0} = g_{i-1,m_{i-1}}$.

The solution of the above problem is stated in the following theorem.

Theorem 2.3.2 *Let $\mathcal{A}$ be a UFD, f, g be two polynomials in $\mathcal{A}[x, y]$ and a be a nonzero element of $\mathcal{A}$. Then the following assertions are equivalent:*
i) $g = h(f) \mod(a)$ for some $h \in \mathcal{A}[t]$,
ii) all $h_{i,j}$'s are elements of $\mathcal{A}[t]$.
In this case, the polynomial $h = \sum_{i=1}^{r} \sum_{j=1}^{m_i} a_i^{j-1} h_{i,j}(t)$ satisfies $g = h(f) + a g_{r,m_r}$.

Proof. $i) \Rightarrow ii)$ This is a direct consequence of the routine described above and Lemma 2.3.1.
$ii) \Rightarrow i)$ By induction on the size $m = m_1 + \dots + m_r$ of $a = a_1^{m_1} \dots a_r^{m_r}$. If $m = 1$, the element a is irreducible, so the result follows from lemma 2.3.1. Assume now that the result has been proved for the size less than m and let a be with size $m + 1$, Let a_1 be a prime factor of a. By using Euclidean division over the domain $\mathcal{A}/(a_1)[x, t]$, we have $g = h_{1,1}(f) + a_1 g_{1,1}$, and applying the induction hypothesis to $g_{1,1}$ and $a_1^{-1}a$, we get $g_{1,1} = h_0(f) \mod (a_1^{-1}a)$ for some $h_0 \in \mathcal{A}[t]$. Therefore, $g = h(f) \mod (a)$, where $h(t) = h_{1,1}(t) + a_1 h_0(t)$. ∎

2.3.2 Characterization of coordinates over a UFD

The following result produces an algorithmic characterization of coordinates over a unique factorization domain.

Theorem 2.3.3 *Let $\mathcal{A}$ be a UFD of characteristic zero and f be a non-triangular polynomial in $\mathcal{A}[x, y]$. Then f is a coordinate if and only if the three following conditions hold:*

i) the derivation $\mathcal{X}_f$ is locally nilpotent,

ii) $r_1 = \deg_{\mathcal{X}_f} x \geq 2$ and $\mathcal{X}_f^{r_1}(x)$ is constant.

iii) $\mathcal{X}_f^{r_1-1}(x) = h(f) \mod(\mathcal{X}_f^{r_1}(x))$, where $h \in \mathcal{A}[t]$.

In this case, $(\mathcal{X}_f^{r_1}(x))^{-1}(\mathcal{X}_f^{r_1-1}(x) - h(f))$ is a coordinate's mate of f.

Proof. $\Rightarrow$) The conditions i) and ii) can be checked in the same way as in the proof of Theorem 2.2.1, so the only thing that remains to prove is the condition iii). Let g be a coordinate's mate of f such that $\mathcal{X}(g) = 1$. Then

$$\mathcal{X}(\mathcal{X}^{r_1-1}(x) - \mathcal{X}^{r_1}(x)g) = 0,$$

and so $\mathcal{X}^{r_1-1}(x) - \mathcal{X}^{r_1}(x)g = h(f)$ by Theorem 2.1.3.
$\Leftarrow$) By Theorem 2.1.3 it is enough to prove that $\mathcal{X}_f$ has a slice. Since $\mathcal{X}_f^{r_1-1}(x) = h(f) \mod(\mathcal{X}_f^{r_1}(x))$, there exists a polynomial g in $\mathcal{A}[x, y]$ such that $\mathcal{X}_f^{r_1-1}(x) = h(f) + (\mathcal{X}_f^{r_1}(x))g$, which implies that $\mathcal{X}_f(g) = 1$. ∎

The algorithm of this case is giving as follow

Algorithm 2: Coordinate's algorithm over UFD

Input : A polynomial $f \in \mathcal{A}[x, y]$, where $\mathcal{A}$ is a UFD.
Output : Either a message that f is not coordinate or a mate with minimum degree $g \in \mathcal{A}[x, y]$ of f.

1: By using algorithm 1 check if $\mathcal{X}_f$ is locally nilpotent, a local slice is then given by $g = \mathcal{X}_f^{r_1-1}(x)$
2: **if** $\mathcal{X}_f^{r_1}(x) \in \mathcal{A}$ **then**
3: Put $a = \mathcal{X}_f^{r_1-1}(x)$ and compute $h_{i,j}$ as in theorem 2.3.2
4: **if** $h_{i,j} \in \mathcal{A}[t]$ **then**
5: f is coordinate and $(\mathcal{X}_f^{r_1}(x))^{-1}(\mathcal{X}_f^{r_1-1}(x) - h(f))$ is a coordinate's mate of f, where $h = \sum_{i=1}^{r} \sum_{j=1}^{m_i} a_i^{j-1} h_{i,j}(t)$.
6: **else**
7: f is not coordinate
8: **else**
9: f is not coordinate
10: **end if**
11: **end if**

2.4 Implementation

In this section we give a pseudo-code description of the algorithm studied in the previous sections. The algorithm takes as input a polynomial f in two variables with coefficients in a UFD of characteristic zero and checks whether it is a coordinate, and if so, it computes a coordinate's mate. Moreover, it produces a mate of f of minimal degree.

2.4.1 Description of the coordinate algorithm

For a given polynomial f, the algorithm performs the following steps:

Step 1: It is well known that the leading homogeneous form of f should be a power of a linear form. Thus, in this step we test if f satisfies this condition.

Step 2: We test if the derivation $\mathcal{X}_f$ is locally nilpotent, by computing the iterates $\mathcal{X}_f^i(x)$ and $\mathcal{X}_f^i(y)$ up to $d = \deg(f)$. At the same time we check whether $\mathcal{X}_f^{r_1}(x)$ is constant, where $r_1 = \deg_{\mathcal{X}_f}(x)$. Notice that according to the relation (2.5) the degree of the i-th iterate should be bounded by $\min(d(d-1), i(d-2)+1)$. The computation is stopped if the degree of $\mathcal{X}_f^i(x)$ exceeds this bound. If $\mathcal{X}_f^{r_1}(x)$ divides $\mathcal{X}_f^{r_1-1}(x)$, the polynomial $(\mathcal{X}_f^{r_1}(x))^{-1}\mathcal{X}_f^{r_1-1}(x)$ is a younger mate of f. Otherwise, the algorithm returns the polynomial $\mathcal{X}_f^{r_1-1}(x)$ and the constant $\mathcal{X}_f^{r_1}(x)$.

Step 3: We check the condition $iii)$ of Theorem 2.3.3 by computing the $h_{i,j}$ which corresponds to the routine described in Theorem 2.3.2.

Step 4: In case a coordinate's mate is computed in step 3, we transform it into a mate of minimal degree by using the following algorithm.

Algorithm 3: Reduction's algorithm

Input : Two polynomials f and g such that $\deg_y(f)$ divides $\deg_y(g)$.
Output : A polynomial $h \in \mathcal{A}[t]$ and $\tilde{g}$ of minimal degree such that $g = h(f) + \tilde{g}$.

$\tilde{g} = g$
if $\frac{\deg_y g}{\deg_y f} \in \mathbb{N}^*$ **then**
  for i to $\deg f - 1$ **do**
    - Compute the coefficients $C_{\tilde{g}}$ and C_f of $y^{(d-i)\deg_y f}$ in, respectively, $\tilde{g}$ and f^{d-i}.
    - Write $C_{\tilde{g}} = \alpha C_f + \beta$
    if α and β are polynomial and content of α is integer **then**
      $\tilde{g} := \tilde{g} - \alpha f^{d-i}$
      $h := h + \alpha t^{d-i}$
    else
      return g
    end if
  end for
else

return g
end if
return $\tilde{g}$,h

2.4.2 Examples

In this subsection we present some examples of coordinates in two variables. For experimentations, we have used the Computer Algebra System Maple.

1) Let us consider the first component of the well-known Nagata automorphism over $\mathbb{Z}[z][x, y]$:

$$f(x, y) := y + z^2x + zy^2.$$

By applying algorithm 1, we get that $\mathcal{X}_f$ is locally nilpotent and has $1 + 2zy$ as a local slice with its image $-2z^3$ which is not a unit of $\mathbb{Z}[z]$.
Using algorithm 2, we get $h = 1 + 2zt - 2z^2t^2$ which is an element of $\mathbb{Z}[z][t]$. So f is coordinate and a coordinate's mate of minimal degree is

$$g(x, y) := x - 2\,yzx - 2\,y^3 - z^3x^2 - 2\,z^2xy^2 - zy^4.$$

It is also of minimal degree over $\mathcal{Q}$. Since $\deg(g) > \deg(f)$, we deduce that the Nagata automorphism is not tame in $\mathcal{Q}[z][x, y]$.

2) In the ring $\mathbb{Z}[\sqrt{2}][x, y]$, we consider the polynomial defined by

$$f(x, y) := x - 2\,y\left(\sqrt{2}x - y^2\right) + \sqrt{2}\left(\sqrt{2}x - y^2\right)^2 - \sqrt{2}\left(y - \sqrt{2}\left(\sqrt{2}x - y^2\right)\right)^4.$$

Applying algorithm 2, we show that it is a coordinate and it has a mate of minimal degree

$$g(x, y) := -y - \sqrt{2}y^2 + 2\,x.$$

3) Consider the polynomial in $\mathbb{Z}[z][x, y]$ defined by

$$f(x, y) := -z^4y^{12} + \left(3\,xz^3 - 5\,z^5\right)y^8 + \left(-3\,x^2z^2 + 10\,z^4x\right)y^4 + 5\,y + 3 + zx^3 - 5\,z^3x^2.$$

The algorithm 1 shows that the derivation $\mathcal{X}_f$ has a local slice

$$37422000000000z^5x - 62370000000000z^7 - 37422000000000y^4z^6$$

and by algorithm 2, we state that f is not a coordinate in $\mathbb{Z}[z][x, y]$. It is, however, a coordinate in the ring $\mathbb{Q}[z][x, y]$, and a coordinate's mate is

$$g(x, y) := -1/3\,z^2 - 1/5\,zy^4 + 1/5\,x.$$

Chapter 3

The rank's characterization of locally nilpotent derivations

Let $\mathcal{K}[\underline{x}]$ be the polynomial ring over $\mathcal{K}$ and $\mathcal{X}$ be a derivation of $\mathcal{K}[\underline{x}]$. As defined in [50] the co-rank of $\mathcal{X}$, denoted by $corank(\mathcal{X})$, is the unique nonnegative integer r such that $\mathcal{K}[\underline{x}]^{\mathcal{X}}$ contains a system of coordinates of length r and no system of coordinates of length greater than r. The rank of $\mathcal{X}$, denoted by $rank(\mathcal{X})$, is defined by $rank(\mathcal{X}) = n - corank(\mathcal{X})$. Intuitively, the rank of $\mathcal{X}$ is the minimal number of partial derivatives needed for expressing $\mathcal{X}$. The unique derivation of rank 0 is the zero derivation. Any derivation of rank 1 is of the form $p(f_1, \ldots, f_n)\partial_{f_n}$, where $f_1, \ldots, f_n$ is a coordinate system, such a derivation is locally nilpotent if and only if p does not depend on f_n.

For such a derivation, let c be the gcd of $\mathcal{X}(x_1), \ldots, \mathcal{X}(x_n)$. We say that $\mathcal{X}$ is irreducible if c is a constant of $\mathcal{K}^\star$. It is well known that $\mathcal{X}(c) = 0$ and $\mathcal{X} = c\mathcal{Y}$, where $\mathcal{Y}$ is an irreducible locally nilpotent derivation. Moreover, this decomposition is unique up to a unit, i.e., if $\mathcal{X} = c_1\mathcal{Y}_1$, where $\mathcal{Y}_1$ is irreducible, then there exists a constant $\mu \in \mathcal{K}^\star$ such that $c_1 = \mu c$ and $\mathcal{Y} = \mu\mathcal{Y}_1$.

Given any irreducible locally nilpotent derivation of $\mathcal{K}[\underline{x}]$ and any $c \neq 0$ such that $\mathcal{X}(c) = 0$, the derivations $\mathcal{X}$ and $c\mathcal{X}$ have the same rank. Thus, for rank computation we may reduce, without loss of generality, to irreducible derivations.

3.1 Minimal local slice

This section concerns minimal local slices of locally nilpotent derivations on polynomial rings. We show that for a unique factorization domain, minimal local slices always exist.

3.1.1 Existence of minimal local slices

Let $\mathcal{A}$ be a ring and $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{A}$. A local slice s of $\mathcal{X}$ called minimal if for any local slice v such that $\mathcal{X}(v)/\mathcal{X}(s)$ we have

$$\mathcal{X}(v) = \mu\mathcal{X}(s),$$

where μ is a unit of $\mathcal{A}$.

The following lemma is the master key of the existence of minimal local slices.

Lemma 3.1.1 *Let $\mathcal{A}$ be a domain and $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{A}$. Let s be a local slice of $\mathcal{X}$, p be a factor of $\mathcal{X}(s) = c$ and write $c = pc_1$. Then there exists $s_1 \in \mathcal{A}$ such that $\mathcal{X}(s_1) = c_1$ if and only if the ideal $p\mathcal{A}$ contains an element of the form $s + a$ where $a \in \mathcal{A}^{\mathcal{X}}$.*

Proof. $\Rightarrow$) Assume that there exists a local slice s_1 of $\mathcal{X}$ such that $\mathcal{X}(s_1) = c_1$. Then $\mathcal{X}(ps_1 - s) = 0$ and so $ps_1 - s = a$, where a is a constant of $\mathcal{X}$. This proves that $p\mathcal{A}$ contains $s + a$.
$\Leftarrow$) Assume now that the ideal $p\mathcal{A}$ contains an element of the form $s + a$, where a is a constant of $\mathcal{X}$, and write $s + a = ps_1$. Then $\mathcal{X}(s) = p\mathcal{X}(s_1)$ and so $\mathcal{X}(s_1) = c_1$. ∎

For the case of a unique factorization domain, the following result states the existence of minimal local slices.

Proposition 3.1.2 *Let $\mathcal{A}$ be a UFD, $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{A}$. Then for any local slice s of $\mathcal{X}$ there exists a minimal local slice s_0 of $\mathcal{X}$ such that $\mathcal{X}(s_0)/\mathcal{X}(s)$,*

Proof. i) Let s be a local slice of $\mathcal{X}$ and write $\mathcal{X}(s) = \mu p_1^{m_1} \dots p_r^{m_r}$, where μ is a unit and the p_i's are primes, and set $m = \sum_i m_i$. We will prove the result by induction on m.
For $m = 0$, $\mathcal{X}(s) = \mu$, and so $\mu^{-1}s$ is a slice of $\mathcal{X}$. This shows that s is a minimal local slice of $\mathcal{X}$. Let us now assume that the result holds for $m - 1$ and let s be a local slice of $\mathcal{X}$, with $\mathcal{X}(s) = \mu p_1^{m_1} \dots p_r^{m_r}$ and $\sum_i m_i = m$. Two cases are then possible:

- Case 1: for any $i = 1, \dots, r$ the ideal $p_i\mathcal{A}$ does not contain any element of the form $s + a$ with $\mathcal{X}(a) = 0$. In this case s is a minimal local slice of $\mathcal{X}$ by Lemma 3.1.1.

- Case 2: there exists i such that $p_i\mathcal{A}$ contains an element of the form $s + a$, with $\mathcal{X}(a) = 0$. Without loss of generality, we may assume that $i = 1$. If we write $s+a = p_1 s_1$ then $\mathcal{X}(s_1) = p^{m_1-1}p_2^{m_2}, \dots, p_r^{m_r}$, and using induction hypothesis we get a minimal local slice s_0 of $\mathcal{X}$ such that $\mathcal{X}(s_0)/\mathcal{X}(s_1)$. The conclusion follows from the fact that $\mathcal{X}(s_1)/\mathcal{X}(s)$. ∎

3.1.2 Computation of minimal local slices

The main question to be addressed, if we want to have an algorithmic version of Proposition 3.1.2, is to check, for a given prime p of $\mathcal{A}$, whether $p\mathcal{A} \cap \mathcal{A}^{\mathcal{X}}[s]$ contains a monic polynomial of degree one with respect to s. In case $\mathcal{A}$ is an affine ring over a computable field $\mathcal{K}$ this problem, may be solved by using Gröbner bases theory, see e.g. [5, 9, 20]. We only treat here the case of when $\mathcal{A}$ and $\mathcal{A}^{\mathcal{X}}$ are polynomial rings over a field since this fits our need.

Proposition 3.1.3 *Let $\mathcal{I}$ be an ideal of $\mathcal{K}[\underline{x}]$ and $\underline{h} = h_1, \dots, h_t$ be a list of algebraically independent polynomials of $\mathcal{K}[\underline{x}]$. Let $\underline{u} = u_1, \dots, u_t$ be a list of new variables and $\mathcal{J}$ be the ideal of $\mathcal{K}[\underline{u}, \underline{x}]$ generated by $\mathcal{I}$ and $h_1 - u_1, \dots, h_t - u_t$. Let $\mathcal{G}$ be a Gröbner*

basis of $\mathcal{J}$ with respect to the lexicographic order $u_1 \prec \ldots \prec u_t \prec x_1 \prec \ldots \prec x_n$, and $\{g_1, \ldots, g_v\} = \mathcal{G} \cap \mathcal{K}[\underline{u}]$. Then:
i) $\{g_1, \ldots, g_v\}$ is a Gröbner basis of $\mathcal{J} \cap \mathcal{K}[\underline{u}]$ with respect to the lexicographic order $u_1 \prec \ldots \prec u_t$,
ii) the $\mathcal{K}$-isomorphism $u_i \in \mathcal{K}[\underline{u}] \longmapsto h_i \in \mathcal{K}[\underline{h}]$ maps $\mathcal{J} \cap \mathcal{K}[\underline{u}]$ onto $\mathcal{I} \cap \mathcal{K}[\underline{h}]$.

In our case, we have $\mathcal{I} = p\mathcal{K}[x, y, z]$ for some polynomial p, and $\mathcal{K}[\underline{h}] = \mathcal{K}[f, g, s]$ where f, g is a generating system of $\mathcal{K}[x, y, z]^{\mathcal{X}}$ and s is a local slice of $\mathcal{X}$. Let u_1, u_2, u_3 be new variables and $\mathcal{J}$ be the ideal of $\mathcal{K}[u_1, u_2, u_3, x, y, z]$ generated by $p, f - u_1, g - u_2, s - u_3$. Let $\mathcal{G}$ be a Gröbner basis of $\mathcal{J}$ with respect to the lexicographic order $u_1 \prec u_2 \prec u_3 \prec x \prec y \prec z$ and $\mathcal{G}_1 = \mathcal{G} \cap \mathcal{K}[u_1, u_2, u_3]$. By Proposition 3.1.3, the ideal $p\mathcal{K}[x, y, z] \cap \mathcal{K}[f, g, s]$ contains a polynomial of the form $s + a(f, g)$ if and only if $\mathcal{G}_1$ contains a monic polynomial $\ell(u_1, u_2, u_3)$ of degree 1 with respect to u_3. In this case, the polynomial we are looking for is $\ell(f, g, s)$.

3.2 The plinth ideal

In this section we focus our attention on the case of polynomial rings in three variables over a field. We give an algorithm to compute a generator of the plinth ideal of a locally nilpotent derivation of $\mathcal{K}[x, y, z]$. Besides Theorem 3.2.1, our algorithm strongly depends on the fact that $\mathcal{K}[x, y, z]^{\mathcal{X}}$ is finitely generated. Since we do not have at disposal an algorithmic version of Miyanishi theorem 1.1.12, we assume a generating system of $\mathcal{K}[x, y, z]^{\mathcal{X}}$ to be available
Let $\mathcal{A}$ be a ring, $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{A}$ and let

$$\mathcal{S}^{\mathcal{X}} := \{\mathcal{X}(a)/\mathcal{X}^2(a) = 0\}.$$

It is easy to see that $\mathcal{S}^{\mathcal{X}}$ is an ideal of $\mathcal{A}^{\mathcal{X}}$, called the plinth ideal of $\mathcal{X}$. This is clearly an invariant of $\mathcal{X}$, i.e., $\mathcal{S}^{\sigma\mathcal{X}\sigma^{-1}} = \sigma(\mathcal{S}^{\mathcal{X}})$ for any automorphism σ of $\mathcal{A}$. In case $\mathcal{A} = \mathcal{K}[x, y, z]$, we have the following result which is a direct consequence of faithful flatness of $\mathcal{K}[x, y, z]$ over $\mathcal{K}[x, y, z]^{\mathcal{X}}$, see [28].

Theorem 3.2.1 *Let $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{A} = \mathcal{K}[x, y, z]$. Then the plinth ideal $\mathcal{S}^{\mathcal{X}}$ is principal.*

The following result gives a generator of the plinth ideal in case it is principal.

Proposition 3.2.2 *Let $\mathcal{A}$ be a UFD, $\mathcal{X}$ be a locally nilpotent derivation of $\mathcal{A}$ and s be a local slice of $\mathcal{X}$. If $\mathcal{S}^{\mathcal{X}}$ is principal ideal, then it is generated by $\mathcal{X}(s)$ for any minimal local slice s of $\mathcal{X}$.*

Proof. Assume that $\mathcal{S}^{\mathcal{X}}$ is principal and let c be a generator of this ideal, with $c = \mathcal{X}(s_0)$. Let s be a minimal local slice of $\mathcal{X}$. Since $\mathcal{X}(s) \in S^{\mathcal{X}}$ we may write $\mathcal{X}(s) = c_1\mathcal{X}(s_0)$. The fact that s is minimal implies that c_1 is a unit of $\mathcal{A}^{\mathcal{X}}$, and so $\mathcal{X}(s)$ generates $\mathcal{S}^{\mathcal{X}}$. ∎

At least in the case we are concerned with, the ideal $\mathcal{S}^{\mathcal{X}}$ is principal according to Theorem 3.2.1. So if we restrict to the case of derivations of $\mathcal{K}[x, y, z]$ represented in a jacobian form, the following algorithm gives the main steps to be performed in order to compute a minimal local slice of a given locally nilpotent derivation.

Algorithm 4: Minimal local slice Algorithm

Input : A locally nilpotent derivation $\mathcal{X}$ of $\mathcal{K}[x, y, z]$ and a generating system f, g of $\mathcal{K}[x, y, z]^{\mathcal{X}}$.
Output : A minimal local slice s of $\mathcal{X}$.

```
Compute a local slice s_0 of X.
Write X(s_0) = p_1^{m_1} ... p_r^{m_r}, where the p_i's are primes.
s = s_0.
for i to r do
  for j to m_i do
    Let G be a Gröbner basis of I(p, f−u_1, g−u_2, s−u_3) with respect to the lex-order
    u_1 ≺ u_2 ≺ u_3 ≺ x ≺ y ≺ z, and G_1 = G ∩ K[u_1, u_2, u_3].
    if G_1 contains a monic polynomial of degree 1 with respect to u_3, say u_3+a(u_1, u_2)
    then
      Write s + a(f, g) = p_i s_1.
      s = s_1.
    else
      Break.
    end if
  end for
end for
```

This algorithm may easily be modified to work for any locally nilpotent derivation of $\mathcal{K}[x_1, \ldots, x_n]$, provided we have at disposal a finite generating system of its $\mathcal{K}$-algebra of constants.

Remark 3.2.3 *In [29] it is proved that if f is a basic element in $\mathcal{K}[x, y, z]$ then for any locally nilpotent derivation such that $f \in \mathcal{K}[x, y, z]^{\mathcal{X}}$ there exists a polynomial g that satisfies $\mathcal{K}[x, y, z]^{\mathcal{X}} = \mathcal{K}[f, g]$ and a generator of the plinth ideal $S^{\mathcal{X}}$ is of the form $a(f)g^n$ for some $a \in \mathcal{K}[f]$ and $n \in \{o, 1\}$.*

3.3 The rank in three variables

In this section we show that the plinth ideal holds a crucial information to give a characterization of the rank of locally nilpotent derivations in dimension three. As a by-product, we give an algorithm for computing the rank.

3.3.1 The main result

It is well-known that the only derivation of rank 0 is the zero derivation. An irreducible locally nilpotent derivation of $\mathcal{K}[\underline{x}]$ is of rank one if and only if $\mathcal{K}[\underline{x}]^{\mathcal{X}} = \mathcal{K}^{[n-1]}$ and $\mathcal{X}$ has a slice, see [50]. In dimension 3, and taking into account Theorem 1.1.12, an irreducible locally nilpotent derivation is of rank one if and only if Algorithm 4 produces a slice. Therefore, we only need to characterize derivations of rank two.

Now, we are ready to announce the main theorem in this section.

Theorem 3.3.1 *Let $\mathcal{X}$ be an irreducible locally nilpotent derivation of $\mathcal{K}[x, y, z]$ and assume $rank(\mathcal{X}) \neq 1$. Let us write $\mathcal{K}[x, y, z]^{\mathcal{X}} = \mathcal{K}[f, g]$ and $\mathcal{S}^{\mathcal{X}} = c\mathcal{K}[f, g]$. Then the following are equivalent:*
i) $rank(\mathcal{X}) = 2$,
ii) $c = \ell(u)$, where ℓ is a univariate polynomial and u is a coordinate of $\mathcal{K}[f, g]$,
iii) $c = \ell(u)$, where u is a coordinate of $\mathcal{K}[x, y, z]$.

Proof. *i)* $\Rightarrow$ *ii)* Assume that $rank(\mathcal{X}) = 2$ and let u, v, w be a coordinate system such that $\mathcal{X}(u) = 0$. The derivation $\mathcal{X}$ is therefore a $\mathcal{K}[u]$-derivation of $\mathcal{K}[u][v, w]$, and since $\mathcal{K}[u]$ is UFD, there exists $p \in \mathcal{K}[x, y, z]$ such that $\mathcal{K}[f, g] = \mathcal{K}[u, p]$. This proves that u is a coordinate of $\mathcal{K}[f, g]$.
Let us now view $\mathcal{X}$ as $\mathcal{K}(u)$-derivation of $\mathcal{K}(u)[v, w]$. By Theorem 1.2.1, $\mathcal{X} = \alpha(v')\partial_{w'}$ for some $v', w' \in \mathcal{K}(u)[v, w]$ and $\alpha \in \mathcal{K}(u)[v']$. Since $\mathcal{X}$ is irreducible, then $\alpha \in \mathcal{K}(u)$ which means that $\mathcal{X}$ have a slice s in $\mathcal{K}(u)[v, w]$. Let us write $s = k(u)^{-1}h(u, v, w)$, then $\mathcal{X}(h) = k(u)$. Let c be a generator of $\mathcal{S}^{\mathcal{X}}$. Then c divides $k(u)$, and since $\mathcal{K}[u]$ is factorially closed in $\mathcal{K}[u, v, w]$, we have $c = \ell(u)$ for some univariate polynomial ℓ.

ii) $\Rightarrow$ *iii)*Assume that $c = \ell(u)$, where u is a coordinate of $\mathcal{K}[f, g]$ and write $\mathcal{K}[f, g] = \mathcal{K}[u, p]$. Let s be such that $\mathcal{X}(s) = c$. If we view $\mathcal{X}$ as $\mathcal{K}(u)$-derivation of $\mathcal{K}(u)[x, y, z]$ then $\mathcal{K}(u)[x, y, z]^{\mathcal{X}} = \mathcal{K}(u)[p]$ and $\mathcal{X}(c^{-1}s) = 1$. By applying Proposition 1.1.7 we get $\mathcal{K}(u)[x, y, z] = \mathcal{K}(u)[p, s]$. From the observation after Theorem 1.4.2, we deduce that u is a coordinate of $\mathcal{K}[x, y, z]$.

iii) $\Rightarrow$ *i)* Since $rank(\mathcal{X}) \neq 1$ the polynomial ℓ is nonconstant. Then we have $\mathcal{X}(c) = \ell'(u)\mathcal{X}(u) = 0$, and so $\mathcal{X}(u) = 0$. On the other hand, since u is assumed to be a coordinate of $\mathcal{K}[x, y, z]$, we have $rank(\mathcal{X}) \leq 2$. By assumption $rank(\mathcal{X}) \neq 1$ and so $rank(\mathcal{X}) = 2$. ∎

The conditions of *ii)* in Theorem 3.3.1 is in fact algorithmic. Indeed, it is algorithmically possible to check whether a given polynomial in two variables is a coordinate, see chapter 2 or [1, 13, 95]. Here we will use this step as a black box, but it is worth mentioning that from the complexity point of view, the algorithm given in [95] is the most efficient as reported in [96]. On the other hand, condition $c = \ell(u)$ may be checked by using a special case, called uni-multivariate decomposition, of functional decomposition of polynomials, see e.g. [56]. It is important to notice here that uni-multivariate decomposition is essentially unique. Namely, if $c = \ell(u) = \ell_1(u_1)$, where u and u_1, are undecomposable, then there exist $\mu \in \mathcal{K}^*$ and $\nu \in \mathcal{K}$ such that $u_1 = \mu u + \nu$. Taking into account the particular nature of our decomposition problem, it seems more convenient to use the following proposition.

Proposition 3.3.2 *Let $c(\underline{x}) \in \mathcal{K}[\underline{x}]$ be nonconstant and $\underline{u} = u_1, \ldots, u_n$ be a list of new variables. Then the following are equivalent:*
i) $c(\underline{x}) = \ell(y_1(\underline{x}))$, where ℓ is a univariate polynomial and y_1 is a coordinate of $\mathcal{K}[\underline{x}]$,
ii) $y_1(\underline{x}) - y_1(\underline{u})/c(\underline{x}) - c(\underline{u})$ and y_1 is a coordinate of $\mathcal{K}[\underline{x}]$.

Proof. *i)* $\Rightarrow$ *ii)* Let ℓ be a univariate polynomial and t, t_0 be variables. Then we have $t - t_0/\ell(t) - \ell(t_0)$. This shows that $y_1(\underline{x}) - y_1(\underline{u})/\ell(\underline{x}) - \ell(\underline{u})$.

ii) $\Rightarrow$ *i)* Let $y_2, \ldots, y_n$ be polynomials such that $\underline{y} = y_1, \ldots, y_n$ is a coordinate system of $\mathcal{K}[\underline{x}]$, and let $v_i = y_i(\underline{u})$. Then $\underline{v} = v_1, \ldots, v_n$ is a coordinate system of $\mathcal{K}[\underline{u}]$.
Let us write $c(\underline{x}) - c(\underline{u}) = (y_1(\underline{x}) - y_1(\underline{u}))A(\underline{u}, \underline{x})$ and $c(\underline{x}) = \ell(\underline{y})$. Then we have

$$\ell(\underline{y}) - \ell(\underline{v}) = (y_1 - v_1)B(\underline{v}, \underline{y}). \tag{3.1}$$

Let us now write $\ell(\underline{y}) = \sum_\alpha a_\alpha y_2^{\alpha_2} \ldots y_n^{\alpha_n}$. After substituting y_1 to v_1 in the relation 3.1 and taking into account the fact that $v_2, \ldots, v_n, y_2, \ldots, y_n$ are algebraically independent over $\mathcal{K}[y_1]$, we get $a_\alpha = 0$ for any $\alpha \neq 0$. This proves that $\ell(\underline{y})$ is a polynomial in terms of y_1.

3.3.2 The rank algorithm

Before implementing algorithms for locally nilpotent derivations of $\mathcal{K}[x, y, z]$ we must first specify how such objects are to be concretely represented. Any chosen representation should address the two following problems.

Recognition problem: Given a derivation $\mathcal{X}$ of $\mathcal{K}[x, y, z]$, check whether $\mathcal{X}$ is locally nilpotent.

Kernel problem: Given a locally nilpotent derivation $\mathcal{X}$ of $\mathcal{K}[x, y, z]$, compute f, g such that $\mathcal{K}[x, y, z]^{\mathcal{X}} = \mathcal{K}[f, g]$.

Usually, a derivation $\mathcal{X}$ of $\mathcal{K}[x, y, z]$ is written as a $\mathcal{K}[x, y, z]$-linear combination of the partial derivatives $\partial_x, \partial_y, \partial_z$. However, with such a representation, the recognition and kernel problems are nowhere near completely solved. To our knowledge, only the weighted homogeneous case of the recognition problem is solved, see [44]. One way to go round this hurdle is to opt for another representation. The Jacobian representation gives another alternative to represent locally nilpotent derivations. Indeed, by Proposition 1.2.3, any locally nilpotent derivation of $\mathcal{K}[x, y, z]$ is, up to a nonzero constant in $\mathcal{K}[x, y, z]^{\mathcal{X}}$, equal to $\mathrm{Jac}(f, g, .)$. According to Theorem 1.1.6 and in order to check whether a Jacobian derivation $\mathcal{X} = \mathrm{Jac}(f, g, .)$ is locally nilpotent, it suffices to check that $\mathcal{X}^{d+1}(x) = \mathcal{X}^{d+1}(y) = \mathcal{X}^{d+1}(z) = 0$, where $d = \deg(f)\deg(g)$. However, it is still not clear how such a representation could help in solving the kernel problem. Nevertheless, we may always check whether this ring of constants is generated over $\mathcal{K}$ by f, g by using van den Essen's kernel algorithm [41]. Due to the above discussed issues, we have restricted our implementation to the case of derivations of $\mathcal{K}[x, y, z]$ represented in a Jacobian form, say $\mathrm{Jac}(f, g, .)$, and whose ring of constants is generated by f, g.

Now the algorithm for computing the rank of a locally nilpotent derivation in dimension 3 is.

Algorithm 5: Rank Algorithm

Input : A locally nilpotent derivation $\mathcal{X}$ of $\mathcal{K}[x,y,z]$ and a generating system f,g of $\mathcal{K}[x,y,z]^{\mathcal{X}}$.
Output : The rank of $\mathcal{X}$.

Write $\mathcal{X} = a_1\partial_x + a_2\partial_y + a_3\partial_z$. Compute $c_1 = gcd(a_1,a_2,a_3)$ and write $\mathcal{X} = c_1\mathcal{Y}$. By using Algorithm 4, compute a minimal local slice s of $\mathcal{Y}$. A generator of $\mathcal{S}^{\mathcal{Y}}$ is then given by $c = \mathcal{Y}(s)$.
if c is a unit **then**
  $rank(\mathcal{X}) = 1$
else
  Compute a factorization of $c(f,g) - c(t_1,t_2)$ in $\mathcal{K}[f,g,t_1,t_2]$where t_1,t_2 are new variables.
  if no factor of $c(f,g) - c(t_1,t_2)$ is of the form $u(f,g) - u(t_1,t_2)$ **then**
    $rank(\mathcal{X}) = 3$
  else
    if u is a coordinate of $\mathcal{K}[f,g]$ for a factor of the form $u(f,g)-u(t_1,t_2)$ of $c(f,g)-c(t_1,t_2)$ **then**
      $rank(\mathcal{X}) = 2$
    else
      $rank(\mathcal{X}) = 3$
    end if
  end if
end if

In case $rank(\mathcal{X}) = 2$, this algorithm produces a coordinate u which belongs to $\mathcal{K}[x,y,z]^{\mathcal{X}}$ but does not produce any coordinate system which contains u. This is due to the fact that we do not know any algorithmic version of Kaliman's result [60].

3.3.3 Examples

Example 1: Let us take, in the first example, the well-known example established by Freudenburg [51] for a derivation of rank 3. So let

$f = xz + y^2$
$g = zf^2 + 2x^2yf - x^5.$

By using algorithm 4 we compute the minimal local slice of the Jacobian derivation $\mathcal{X}_{f,g}$, we get that

$$s = 2(xz + y^2)(-x^3 + yxz + y^3)$$

and its image which is a generator of the plinth ideal $S^{\mathcal{X}_{f,g}}$ is given as

$c = -2zy^8 - 8z^2y^6x - 12z^3y^4x^2 - 4y^7x^2 - 12y^5x^3z - 12y^3x^4z^2 - 8z^4x^3y^2 - 4z^3yx^5 - 2z^5x^4 + 2x^5y^4 + 4x^6y^2z + 2x^7z^2.$

Viewing c as an element of the polynomial ring $\mathcal{K}[f,g]$ and using algorithm 5 we obtain that $c = f^2g$, which is not a coordinate in $\mathcal{K}[f,g]$. So as consequence of Theorem 3.3.1, we deduce that the derivation is of rank three.

Example 2: Consider the derivation $\mathcal{X}$ defined by polynomials

$f_1 = -x - 5yz - 14x^2z - 28xyz^2 - 14y^2z^3 + 2y^2 + 2z^2 + 2yx + 2y^2z - 2xz - 2yz^2 + 2x^2 + 4xyz + 2y^2z^2$

and

$f_2 = 7x^2z + 14xyz^2 + 7y^2z^3 - y^2 + 2yz - z^2 - yx - y^2z + xz + yz^2 - x^2 - 2xyz - y^2z^2$

In the first step, applying the algorithm 4, we show that the minimal local slice of $\mathcal{X}$ is given as

$s = 2x + 2y - 2z + 10yz - 4y^2z + 4xz + 4yz^2 + 28x^2z + 28y^2z^3 - 4y^2z^2 + 56xyz^2 - 8xyz - 4x^2 - 4y^2 - 4z^2 - 4yx$

Its image, which is a generator of $S^{\mathcal{X}}$, is

$$c = 28xyz + 14y^2z^2 + 14x^2.$$

So as a consequence of this step, $\mathcal{X}$ is not of rank 1.

By the algorithm 5 we get that the derivation is of rank two, so the obtained result shows that the polynomial c is of the form $14u^2$ with $u = x + zy$, and that u is a coordinate in $\mathcal{A}^{\mathcal{X}}$ with its coordinate's mate given as $p := f_2$.

As we showed in this chapter, the plinth ideal of a locally nilpotent derivations contains crucial information about this derivation. In the next chapter we will show that it also holds more other information which can be used to give a characterization of triangulable derivations in three variables case.

Chapter 4

Triangulable locally nilpotent derivations in dimension three

All over this chapter, $\mathcal{K}$ is a field of characteristic zero. Let $\mathcal{X}$ be a derivation of $\mathcal{K}[\underline{x}]$. We say that $\mathcal{X}$ is triangulable, if there exists an $\mathcal{K}$-automorphism σ of $\mathcal{K}[\underline{x}]$ such that $\sigma\mathcal{X}\sigma^{-1}(x_1) \in \mathcal{K}$ and for $i \geq 2$ $\sigma\mathcal{X}\sigma^{-1}(x_i) \in \mathcal{K}[x_1, \ldots, x_{i-1}]$. A natural question, when studying derivations, is to decide whether a given locally nilpotent derivation is triangulable. The case of two variables was algorithmically solved by Rentschler's theorem 1.2.1. For the case $n \geq 3$, the first example of non-triangulable G_a-action in dimension 3 is given in [7]. Then the construction of this example was generalized by V. L. Popov in [85] to obtain non-triangulable G_a-actions in any dimension $n \geq 3$.

A necessary condition of triangulability, based on the structure of the variety of fixed points, is also given in [85]. It is proven that the set of fixed points of a triangulable derivation must be cylindrical, i.e., isomorphic to $\mathcal{K}.\mathcal{V}$, where $\mathcal{V}$ is an algebraic variety of $\mathcal{K}^2$. However, this condition is not sufficient as proved in [21]. Other criteria of triangulability in dimension 3 are given in [50, 21, 49, 23]. Whereas, it is nowhere near obvious to make all of these methods work in an algorithmic manner.

This chapter deals with the triangulability of locally nilpotent derivations in three dimensional case. By using results obtained in Chapter 3, we will show a new criterion for the triangulability in three variables and as by-product an efficient algorithm will be produced. In case the given derivation is triangulable, this algorithm produces a coordinate system in which it exhibits a triangular form.

4.1 Basic facts

The following proposition gives a necessary condition for the triangulability of derivations.

Proposition 4.1.1 *Triangulable derivations $\mathcal{X}$ of $\mathcal{K}[\underline{x}]$ are of rank at most $n-1$.*

Proof. Without loss of generality, we may assume that $\mathcal{X}$ is triangular in the coordinate system $(x_1, \ldots, x_n)$. Suppose that $n \geq 2$ and assume that $\mathcal{X}(x_1) = \alpha \in \mathcal{K}$. If $\alpha = 0$, we are done. Otherwise, let $g \in \mathcal{K}[x_1]$ such that $\mathcal{X}(x_2) = \partial_{x_1} g(x_1)$. Then if we let $y_2 = \alpha x_2 + g(x_1)$, it is clear that y_2 is a coordinate and since $\mathcal{X}(y_2) = 0$ we claim the result. ∎

As defined in [21], a derivation $\mathcal{X}$ of rank r of $\mathcal{K}[\underline{x}]$ is called rigid if for any coordinate systems $y_1, \ldots, y_n$ and $z_1, \ldots, z_n$ such that $\mathcal{K}[y_1, \ldots, y_{n-r}] = \mathcal{K}[\underline{x}]^{\mathcal{X}}$ and $\mathcal{K}[z_1, \ldots, z_{n-r}] = \mathcal{K}[\underline{x}]^{\mathcal{X}}$, we have $\mathcal{K}[y_1, \ldots, y_{n-r}] = \mathcal{K}[z_1, \ldots, z_{n-r}]$. The main result behind the triangulability criterion given in [21] is that locally nilpotent derivations in three variables are rigid. In general, derivations of rank $0, 1$ and n are obviously rigid, only the rank two case is nontrivial. The characterization *ii)* of rank two derivations given in Theorem 3.3.1 gives, in fact, more precise information. Indeed, it tells that if a coordinate of $\mathcal{K}[x, y, z]$ belongs to $\mathcal{K}[x, y, z]^{\mathcal{X}}$, then it may be found by decomposing the generator of the plinth ideal $\mathcal{S}^{\mathcal{X}}$. The fact that rank two derivations are rigid is then an obvious consequence of the uniqueness property of uni-multivariate decomposition. On the other hand, a rank 1 locally nilpotent derivation is obviously triangulable. This shows that, in dimension 3, we only need to deal with rank 2 derivations.

Let $\mathcal{X}$ be a rank two locally nilpotent derivation of $\mathcal{K}[x, y, z]$ such that $\mathcal{X}(x) = 0$. Then for any coordinate system x_1, y_1, z_1 such that $\mathcal{X}(x_1) = 0$, we have $\mathcal{K}[x] = \mathcal{K}[x_1]$, see [21]. This could also be easily deduced from the uniqueness property of uni-multivariate decomposition. This proves that if $\mathcal{X}$ has a triangular form in a coordinate system x_1, y_1, z_1, then x_1 is essentially unique and may be extracted from a generator of the plinth ideal $\mathcal{S}^{\mathcal{X}}$. Also, this shows that if $\mathcal{X}$ is triangulable and $\mathcal{X}(a) = 0$, then $a\mathcal{X}$ is triangulable if and only if $a \in \mathcal{K}[x]$.

In the following lemma we construct a new derivation which will play a crucial role in Theorem 4.4.2.

Lemma 4.1.2 *Let $\mathcal{X}$ be an irreducible locally nilpotent derivation of $\mathcal{K}[x, y, z]$ of rank 2, u be a coordinate of $\mathcal{K}[x, y, z]$ such that $\mathcal{X}(u) = 0$, and s be a minimal local slice of $\mathcal{X}$. Then the $\mathcal{K}[u]$-derivation $\mathcal{Y} = \mathrm{Jac}_{(x,y,z)}(u, s, .)$ is locally nilpotent irreducible and $\mathcal{K}[x, y, z]^{\mathcal{Y}} = \mathcal{K}[u, s]$. Moreover, $\mathcal{X}\mathcal{Y} = \mathcal{Y}\mathcal{X}$.*

Proof. Without loss of generality, we may assume that $u = x$. Let us write $\mathcal{K}[x, y, z]^{\mathcal{X}} = \mathcal{K}[x, p]$ and by Theorem 3.3.1 let $\mathcal{X}(s) = c(x)$. Then $\mathcal{K}[x]_c[y, z] = \mathcal{K}[x]_c[p, s]$ according to Proposition 1.1.7. Given $a \in \mathcal{K}[x, y, z]$, we may therefore write $a = \frac{h(x,p,s)}{c(x)^n}$. This gives

$$\mathcal{Y}(a) = -c^{-n}(\partial_z s \partial_y p - \partial_y s \partial_z p)\partial_p h,$$

and since, by the observation following Theorem 1.2.1, $\mathcal{X}(s) = -\partial_z s \partial_y p + \partial_y s \partial_z p = c(x)$, we get $\mathcal{Y}(a) = c(x)^{-n+1}\partial_p h$. By induction, we get $\mathcal{Y}^{d+1}(a) = 0$, where $d = \deg_p(h)$, and this proves that $\mathcal{Y}$ is locally nilpotent.
Let $g(x, y, z) = \gcd(\partial_y s, \partial_z s)$. Since $\mathcal{Y}(p) = -c(x)$, then $g \mid c(x)$ and so we may write $c(x) = g(x)c_1(x)$. Then $s(x, y, z) = g(x)s_1(x, y, z) + a(x)$, and this gives $\mathcal{X}(s_1) = c_1(x)$. Since s is a minimal local slice of $\mathcal{X}$, then $c(x) \mid c_1(x)$, and so $g \in \mathcal{K}^{\star}$. This shows that $\mathcal{Y}$ is irreducible.
Let us write $\mathcal{K}[x, y, z]^{\mathcal{Y}} = \mathcal{K}[x, s_0]$ and $s = \ell(x, s_0)$. Then

$$\mathcal{Y} = \partial_{s_0}\ell(x, s_0)(\partial_z s_0 \partial_y - \partial_y s_0 \partial_z).$$

Since $\mathcal{Y}$ is irreducible, $\partial_{s_0}\ell(x, s_0)$ is a unit, and so $s = \mu s_0 + a(x)$ with $\mu \in \mathcal{K}$. This proves that $\mathcal{K}[x, s_0] = \mathcal{K}[x, s]$. The fact that $\mathcal{X}$ and $\mathcal{Y}$ commute is clear. ■

4.2 Reduction of the triangular form

The main purpose of this section is to reduce the triangular form of a given triangular derivation, i.e., for any triangular derivation $\mathcal{X}$ of $\mathcal{K}[x, y, z]$ we can find a new coordinate system (u, v, w) in which the derivation has the triangular form $\mathcal{X}(u) = 0$, $\mathcal{X}(v) = c(u)$ and $\mathcal{X}(w) = b(u, v)$, where $c(u)$ is a generator of the plinth ideal of the derivation $\mathcal{X}$.

The following lemma is the key for that.

Lemma 4.2.1 *Let $\mathcal{X}$ be a rank two irreducible triangulable derivation of $\mathcal{K}[x, y, z]$ and let u, v, w be a coordinate system of $\mathcal{K}[x, y, z]$ such that*

$$\mathcal{X}(u) = 0, \quad \mathcal{X}(v) = d(u), \quad \mathcal{X}(w) = q(u, v).$$

Let $c(u)$ be a generator of the ideal $\mathcal{S}^{\mathcal{X}}$. Then $d(u) = c(u)e(u)$, $\gcd(c(u), e(u)) = 1$ and $\mathcal{I}(e(u), q(u, v)) = \mathcal{K}[u, v]$.

Proof. Since $\mathcal{X}$ is of rank 2, we must have $d(u) \neq 0$, and so v is a local slice of $\mathcal{X}$. This proves that $c(u) \mid d(u)$. On the other hand, let us consider

$$p = d(u)w - q_1(u, v), \tag{4.1}$$

where $\partial_v q_1 = q$. Then $\mathcal{X} = \partial_w p \partial_v - \partial_v p \partial_w$, and the fact that $\mathcal{X}$ is irreducible implies that $\gcd(\partial_v p, \partial_w p) = 1$. This shows that $\mathcal{K}[u, v, w]^{\mathcal{X}} = \mathcal{K}[u, p]$.

Let us write $d(u) = c(u)e(u)$, and notice that the result obviously holds if we have $\deg_u(e(u)) = 0$. Thus, we assume in the sequel that $\deg_u(e(u)) > 0$.

Let α be a root of $e(u)$ in an algebraic closure $\overline{\mathcal{K}}$ of $\mathcal{K}$ and let us prove that $q(\alpha, v)$ is a nonzero constant. Using proposition 3.1.2 we may write $\mathcal{X}(s) = c(u)$ for some minimal local slice of $\mathcal{X}$. Hence $v - e(u)s \in \mathcal{K}[u, v, w]^{\mathcal{X}}$. So

$$v = e(u)s(u, v, w) + \ell(u, p(u, v, w)), \tag{4.2}$$

By substituting α to u in the relation (4.2) we get $v = \ell(\alpha, p(\alpha, v, w))$, and by doing so for (4.1) we get $p(\alpha, v, w) = -q_1(\alpha, v)$. This yields $v = \ell(\alpha, -q_1(\alpha, v))$. By comparing degrees in both sides of this equality we get $\deg(q_1(\alpha, v)) = 1$. This proves that $\deg(q(\alpha, v)) = 0$ and so $q(\alpha, v)$ is a nonzero constant. By the Hilbert's Nullstellensatz, we have $\mathcal{I}(e(u), q(u, v)) = \mathcal{K}[u, v]$. To prove that $\gcd(c, e) = 1$, we only need to show that $q(\alpha, v)$ is nonconstant for any root α of $c(u)$.

Let $a(u)$ be a prime factor of $c(u)$. First, notice that the assumption $q(u, v) = 0 \mod a(u)$ would imply that $a(u) \mid \mathcal{X}(h)$ for any h and contradicts the fact that $\mathcal{X}$ is irreducible. Assume, towards contradiction, that $q(u, v)$ is a nonzero constant modulo $a(u)$. Then $\mathcal{X}$ has no fixed points in the surface $a(u) = 0$. If we write $c(u) = a(u)^m c_1(u)$, with $\gcd(c_1, a) = 1$, and view $\mathcal{X}$ as $\mathcal{K}[u]_{c_1}$-derivation of $\mathcal{K}[u]_{c_1}[v, w]$, then it is fixed point free and so it has a slice s according to Theorem 1.2.2. If we write $s = \frac{h(u,v,w)}{c_1^n}$ then $\mathcal{X}(h) = c_1^n$. But c_1^n is not a multiple of c, and this contradicts the fact that c is a generator of $\mathcal{S}^{\mathcal{X}}$. ■

The following lemma shows that it is possible to get rid of the factor $e(u)$.

Lemma 4.2.2 *Let $\mathcal{X}$ be a rank two irreducible triangulable locally nilpotent derivation of $\mathcal{K}[x,y,z]$, and write $\mathcal{K}[x,y,z]^{\mathcal{X}} = \mathcal{K}[u,p]$ where u is a coordinate of $\mathcal{K}[x,y,z]$. Let s be a minimal local slice of $\mathcal{X}$ and write $\mathcal{X}(s) = c(u)$. Then there exist v, w such that u, v, w is a coordinate system and*

$$\mathcal{X}(u) = 0,\ \mathcal{X}(v) = c(u),\ \mathcal{X}(w) = q(u,v).$$

Proof. Let u_1, v_1, w_1 be a coordinate system such that $\mathcal{X}(u_1) = 0, \mathcal{X}(v_1) = d(u_1)$ and $\mathcal{X}(w_1) = q_1(u_1, v_1)$. Without loss of generality, we may assume that $u_1 = u$, and according to Lemma 4.2.1, let us write $d(u) = c(u)e(u)$ with $\gcd(c(u), e(u)) = 1$.

Without loss of generality, we may choose $p = c(u)e(u)w_1 - Q_1(u, v_1)$, where $\partial_{v_1} Q_1 = q_1$, and $v_1 = e(u)s + \ell_1(u,p)$. This gives the relation

$$p = c(u)e(u)w_1 - Q_1(u, e(u)s + \ell_1(u,p)). \tag{4.3}$$

If we write $a(u)c(u) + b(u)e(u) = 1$, then we get

$$Q_1(u, e(u)s + \ell_1(u,p)) = Q_1(u, e(u)(s + b(u)\ell_1(u,p)) + c(u)a(u)\ell_1(u,p)),$$

and by Taylor expanding we get

$$Q_1(u, e(u)s + \ell_1(u,p)) = Q_1(u, e(u)(s + b(u)\ell_1(u,p))) + c(u)Q_2(u,p,s). \tag{4.4}$$

Now, let $\ell(u,p) = b(u)\ell_1(u,p)$, $v = s + \ell(u,p)$, $Q(u,v) = Q_1(u, e(u)v)$ and let $w = e(u)w_1 - Q_2(u,p,s)$. According to the relations (4.3) and (4.4), we have

$$p + Q(u,v) = c(u)w. \tag{4.5}$$

Let us consider the $\mathcal{K}[u]$-derivation $\mathcal{Y} = -\mathrm{Jac}(u,v,.)$. By Lemma 4.1.2, $\mathcal{Y}$ is locally nilpotent and $\mathcal{K}[x,y,z]^{\mathcal{Y}} = \mathcal{K}[u,v]$. By the relation (4.5) and $\mathcal{Y}(p) = c(u)$ (see the proof of lemma 4.1.2), $\mathcal{Y}(w) = 1$, and from Proposition 1.1.7 we deduce that u, v, w is a coordinate system of $\mathcal{K}[x,y,z]$. Moreover, $\mathcal{X}(u) = 0, \mathcal{X}(v) = c(u)$ and $\mathcal{X}(w) = \partial_v Q(u,v)$. ∎

4.3 Criterion for triangulability

Let $\mathcal{A}$ be a ring and $\mathcal{X}$ a locally nilpotent derivation of $\mathcal{A}$. Let $\mathcal{A}^{\mathcal{X}}[s\ ;\ \mathcal{X}(s) \in \mathcal{S}^{\mathcal{X}}]$ be the subring of $\mathcal{A}$ generated over $\mathcal{A}^{\mathcal{X}}$ by all the local slices of $\mathcal{X}$. This is another invariant of the derivation $\mathcal{X}$. Let $(c_i)_{i\in I}$ be a generating system of $\mathcal{S}^{\mathcal{X}}$ and let s_i be such that $\mathcal{X}(s_i) = c_i$. Given any local slice s of $\mathcal{X}$ we have $\mathcal{X}(s) \in \mathcal{S}^{\mathcal{X}}$, and so there exist a finite subset J of I and a family $(u_i)_{i\in J}$ in $\mathcal{A}^{\mathcal{X}}$ such that $\mathcal{X}(s) = \sum_i u_i \mathcal{X}(s_i)$. Then $\mathcal{X}(s - \sum_i u_i s_i) = 0$ and so $s \in \mathcal{A}^{\mathcal{X}}[s_i, i \in I]$. This proves that the ring $\mathcal{A}^{\mathcal{X}}[s\ ;\ \mathcal{X}(s) \in \mathcal{S}^{\mathcal{X}}] = \mathcal{A}^{\mathcal{X}}[s_i, i \in I]$.

Assume that $\mathcal{A}$ to be a UFD and $\mathcal{S}^{\mathcal{X}}$ is principal and generated by $c = \mathcal{X}(s)$. For any factor q of c, we let $\mathcal{I}_q^{\mathcal{X}} = q\mathcal{A} \cap \mathcal{A}^{\mathcal{X}}[s]$. The ideals $\mathcal{I}_q^{\mathcal{X}}$ are in fact invariants of the derivation and we will see in the sequel that they hold the essential information needed to decide whether $\mathcal{X}$ is triangulable.

The following result gives a criterion of the triangulability.

Theorem 4.3.1 *Let $\mathcal{X}$ be a rank two irreducible locally nilpotent derivation of the ring $\mathcal{K}[x,y,z]$ and write $\mathcal{K}[x,y,z]^{\mathcal{X}} = \mathcal{K}[u,p]$ where u is a coordinate of $\mathcal{K}[x,y,z]$. Let s be a minimal local slice of $\mathcal{X}$ and write $\mathcal{X}(s) = c(u)$. Then the following are equivalent:*
i) the derivation $\mathcal{X}$ is triangulable,
ii) the ideal $\mathcal{I}_c^{\mathcal{X}}$ contains a polynomial of the form $H = p + Q(u, s + \ell(u,p))$.

In this case, if we let $v = s + \ell(u,p)$ and $H = c(u)w$, then u, v, w is a coordinate system of $\mathcal{K}[x,y,z]$ which satisfies

$$\mathcal{X}(u) = 0,\ \mathcal{X}(v) = c(u),\ \mathcal{X}(w) = \partial_v Q(u,v).$$

Proof. *i)* ⇒ *ii)* Let u, v, w be a coordinate system such that $\mathcal{X}(u) = 0, \mathcal{X}(v) = d(u)$ and $\mathcal{X}(w) = q(u,v)$. By Lemma 4.2.2 we may choose our coordinate system in such a way that $d(u) = c(u)$. In this case we have $v = s + \ell(u,p)$ and we may choose $p = c(u)w - Q(u,v)$, where $\partial_v Q(u,v) = q(u,v)$. If we let $H = p + Q(u,v)$, then clearly $H \in \mathcal{I}_c^{\mathcal{X}}$.

ii) ⇒ *i)* Let $v = s + \ell(u,p)$ and $\mathcal{Y} = -\mathrm{Jac}(u,v,.)$. Notice that $\mathcal{Y}$ is locally nilpotent and $\mathcal{K}[x,y,z]^{\mathcal{Y}} = \mathcal{K}[u,v]$ according to Lemma 4.1.2. By assumption we have $H = p + Q(u,v) \in \mathcal{I}_c^{\mathcal{X}}$, so let us write $H = c(u)w$. Since $\mathcal{Y}(H) = \mathcal{Y}(p) = c(u)$, then $\mathcal{Y}(w) = 1$. According to Proposition 1.1.7, u, v, w is a coordinate system of $\mathcal{K}[x,y,z]$, $\mathcal{X}(u) = 0, \mathcal{X}(v) = c(u)$, and $\mathcal{X}(w) = \partial_v Q(u,v)$. ∎

By the following corollary we may reduce the problem to the case c^n, where c is irreducible.

Corollary 4.3.2 *Let $\mathcal{X}$ be a rank two irreducible locally nilpotent derivation of $\mathcal{K}[x,y,z]$ and write $\mathcal{K}[x,y,z]^{\mathcal{X}} = \mathcal{K}[u,p]$ where u is a coordinate of $\mathcal{K}[x,y,z]$. Let s be a minimal local slice of $\mathcal{X}$ and write $\mathcal{X}(s) = c(u) = c_1^{n_1} \cdots c_r^{n_r}$, where the c_i's are irreducible and pairwise distinct. Then the following are equivalent:*
i) the derivation $\mathcal{X}$ is triangulable,
ii) for any $i = 1, \ldots, r$ the ideal $\mathcal{I}_{c_i^{n_i}}^{\mathcal{X}}$ contains a polynomial H_i such that $H_i = p + Q_i(u, s + \ell_i(u,p)) \bmod c_i^{n_i}$.

Proof. *i)* ⇒ *ii)* This is an obvious consequence of Theorem 4.3.1.
ii) ⇒ *i)* By the Chinese remainder Theorem, let $Q(u,v)$ and $\ell(u,p)$ be such that $Q = Q_i \bmod c_i^{n_i}$ and $\ell = \ell_i \bmod c_i^{n_i}$. A straightforward computation shows that $p + Q(u, s + \ell(u,p)) = c(u)w$, and so $\mathcal{X}$ is triangulable by Theorem 4.3.1. ∎

4.4 Computation of a triangulating coordinate system

Let $\mathcal{X}$ be an irreducible triangulable locally nilpotent derivation of $\mathcal{K}[x,y,z]$ and write $\mathcal{K}[x,y,z]^{\mathcal{X}} = \mathcal{K}[u,p]$, where u is a coordinate of $\mathcal{K}[x,y,z]$. Let s be a minimal local slice of $\mathcal{X}$, with $\mathcal{X}(s) = c(u) = c_1^{n_1}\cdots c_r^{n_r}$ and the c_i's are prime and pairwise distinct. According to Corollary 4.3.2, it suffices to find a polynomial of the form $p+Q_i(u, s+\ell_i(u,p))$ in each ideal $\mathcal{I}^{\mathcal{X}}_{c_i^{n_i}}$. It is trivial to see that such a polynomial is a coordinate of $\mathcal{K}[u,p,s]$, and as by-product it is a coordinate when viewed as polynomial of $\mathcal{K}[u]/c_i^{n_i}[p,s]$. We are thus led to deal with the problem of finding a polynomial in $\mathcal{I}_{c_i^{n_i}}$ which is a coordinate of $\mathcal{K}[u]/c_i^{n_i}[p,s]$. In fact, taking into account Theorem 1.4.1, we only need to deal with the case of $\mathcal{K}[u]/c_i[p,s]$. In this section we solve such a problem, and we show how this allows to compute a coordinate system of $\mathcal{K}[x,y,z]$ in which $\mathcal{X}$ exhibits a triangular form.

Lemma 4.4.1 *Let $\mathcal{X}$ be a rank two irreducible locally nilpotent derivation of the ring $\mathcal{K}[x,y,z]$, and write $\mathcal{K}[x,y,z]^{\mathcal{X}} = \mathcal{K}[u,p]$ where u is a coordinate of $\mathcal{K}[x,y,z]$. Let s be a minimal local slice of $\mathcal{X}$ and write $\mathcal{X}(s) = c(u)$. Then for any prime factor c_1 of c the following hold:*

i) there exists a monic polynomial h_1 with respect to s such that $\mathcal{I}^{\mathcal{X}}_{c_1} = (c_1, h_1)$. Moreover, c_1, h_1 is the reduced Gröbner basis of $\mathcal{I}^{\mathcal{X}}_{c_1}$ with respect to the lex-order $u \prec p \prec s$,

ii) the ideal $\mathcal{I}^{\mathcal{X}}_{c_1}$ contains a coordinate of $\mathcal{K}[u]/c_1[p,s]$ if and only if h_1 is a coordinate of $\mathcal{K}[u]/c_1[p,s]$. Moreover, any polynomial $h \in \mathcal{I}^{\mathcal{X}}_{c_1}$ which is a coordinate of $\mathcal{K}[u]/c_1[p,s]$ satisfies $h = \mu(u)h_1$, where μ is a unit of $\mathcal{K}[u]/c_1$.

Proof. $i)$ Let v, w be such that u, v, w is a coordinate system of $\mathcal{K}[x,y,z]$. The derivation $\mathcal{X}$ induces a $\mathcal{K}[u]/c_1$-derivation $\overline{\mathcal{X}}$ of the ring $\mathcal{K}[x,y,z]/c_1 = \mathcal{K}[u]/c_1[v,w]$ which is locally nilpotent. Since $\mathcal{X}$ is assumed to be irreducible, then $\overline{\mathcal{X}} \neq 0$, and by Theorem 1.2.1, there exists $\vartheta \in \mathcal{K}[u]/c_1[v,w]$ such that

$$\mathcal{K}[u]/c_1[v,w]^{\overline{\mathcal{X}}} = \mathcal{K}[u]/c_1[\vartheta].$$

Clearly, $\mathcal{K}[u,p,s]/\mathcal{I}^{\mathcal{X}}_{c_1}$ is a $\mathcal{K}[u]/c_1$-subalgebra of $\mathcal{K}[u]/c_1[v,w]$ and we have $\overline{\mathcal{X}}(p) = \overline{\mathcal{X}}(s) = 0$ in $\mathcal{K}[u]/c_1[v,w]$. This proves that $\mathcal{K}[u,p,s]/\mathcal{I}^{\mathcal{X}}_{c_1}$ is in fact a $\mathcal{K}[u]/c_1$-subalgebra of $\mathcal{K}[u]/c_1[\vartheta]$, and as a consequence there exist polynomials $a(t), b(t) \in \mathcal{K}[u]/c_1[t]$ such that $p = a(\vartheta)$ and $s = b(\vartheta)$ in $\mathcal{K}[u]/c_1[\vartheta]$. To prove that $a(t)$ is nonconstant we will prove that $\mathcal{K}[u,p] \cap \mathcal{I}^{\mathcal{X}}_{c_1} = (c_1)$. Let $k(u,p) \in \mathcal{K}[u,p] \cap \mathcal{I}^{\mathcal{X}}_{c_1}$ and write $k(u,p) = c_1(u)p_1(u,v,w)$. Since $\mathcal{K}[u,p]$ is factorially closed in $\mathcal{K}[u,v,w]$(cf. Proposition 1.1.4), then $p_1(u,v,w) = p_2(u,p)$, and so $k(u,p) = c_1(u)p_2(u,p)$.

Now, if $a(t)$ is constant, say $a_0(u)$, then $p - a_0(u) = 0$ in $\mathcal{K}[u]/c_1[v,w]$ and so $p - a_0(u) \in \mathcal{K}[u,p] \cap \mathcal{I}^{\mathcal{X}}_{c_1}$. This contradicts the fact that $\mathcal{K}[u,p] \cap \mathcal{I}^{\mathcal{X}}_{c_1} = (c_1(u))$.

The fact $\mathcal{K}[u,p] \cap \mathcal{I}^{\mathcal{X}}_{c_1} = (c_1)$ implies that the polynomial algebra $\mathcal{K}[u]/c_1[p]$ is a $\mathcal{K}[u]/c_1$-subalgebra of $\mathcal{K}[u]/c_1[v,w]$. Let us write $a(t) = a_m(u)t^m + \cdots + a_0(u)$ with $m \geq 1$ and a_m a unit of $\mathcal{K}[u]/c_1$. The fact that $a(\vartheta) - p = 0$ in $\mathcal{K}[u]/c_1[v,w]$ implies that

ϑ is integral over $\mathcal{K}[u]/c_1[p]$. From $s = b(\vartheta)$ in $\mathcal{K}[u]/c_1[v,w]$, we deduce that s is integral over $\mathcal{K}[u]/c_1[p]$ as well. Since $\mathcal{K}[u]/c_1[p]$ is a UFD and $\mathcal{K}[u]/c_1[v,w]$ is a domain there exists a unique irreducible polynomial $h_1(u,p,t)$ which is monic with respect to t such that $h_1(u,p,s) = 0$ in $\mathcal{K}[u]/c_1[v,w]$. Moreover, any other polynomial $h(u,p,t)$ such that $h(u,p,s) = 0$ in $\mathcal{K}[u]/c_1[v,w]$ is a multiple of h_1. This means exactly that $c_1\mathcal{K}[u,v,w] \cap \mathcal{K}[u,p,s] = (c_1,h_1)$ and that h_1 is unique, up to a multiplication by a constant in $\mathcal{K}[u]/c_1$, when viewed as a polynomial in $\mathcal{K}[u]/c_1[p,s]$.

Now, let $a \in \mathcal{I}_{c_1}^{\mathcal{X}}$, and notice that in this case reducing a by h_1, with respect to the lex-order $u \prec p \prec s$, is the same as performing the Euclidean division of a by h_1 with respect to s. We may thus write $a = qh_1 + r$, with $\deg_s(r) < \deg_s(h_1)$. Since $r \in \mathcal{I}_{c_1}^{\mathcal{X}}$ we may write $r = b_1h_1 + b_2c_1$, and even if it means reducing b_2 by h, we may assume that $\deg_s(b_2) < \deg_s(h_1)$. By comparing degrees with respect to s in both sides of the last equality, we get $r = b_2c_1$, and so a reduces to 0 by using h_1, c_1. This means exactly that c_1, h_1 is a Gröbner basis of $\mathcal{I}_{c_1}^{\mathcal{X}}$ with respect to the lex-order $u \prec p \prec s$.

ii) Let $h \in \mathcal{I}_{c_1}^{\mathcal{X}}$ be a coordinate of $\mathcal{K}[u]/c_1[p,s]$, and write $h = ac_1 + bh_1$. Then over $\mathcal{K}[u]/c_1$, we have $h = bh_1$, and the fact that h is a coordinate of $\mathcal{K}[u]/c_1[p,s]$ implies that it is irreducible. This shows that b is a unit of $\mathcal{K}[u]/c_1[p,s]$, and so a nonzero element of the field $\mathcal{K}[u]/c_1$. It follows that, h_1 is a coordinate of $\mathcal{K}[u]/c_1[p,s]$. The converse is clear. ∎

Theorem 4.4.2 *Let $\mathcal{X}$ be a rank two irreducible locally nilpotent derivation of the ring $\mathcal{K}[x,y,z]$, and let $\mathcal{K}[x,y,z]^{\mathcal{X}} = \mathcal{K}[u,p]$, where u is a coordinate of $\mathcal{K}[x,y,z]$. Let s be a minimal local slice of $\mathcal{X}$ and write $\mathcal{X}(s) = c(u) = c_1^{n_1}\cdots c_r^{n_r}$, where the c_i's are irreducible and pairwise distinct. Then $\mathcal{X}$ is triangulable if and only if for any $i = 1,\dots,r$ the following hold:*

i) the reduced Gröbner basis of $\mathcal{I}_{c_i}^{\mathcal{X}}$ with respect to the lex-order $u \prec p \prec s$ is c_i, h_i, where $h_i = Q_i(u, s+\ell_i(u,p)) + \mu_i(u)p \mod c_i$ and $\mu_i(u)$ is a unit $\mathrm{mod}\ c_i$,

ii) if $\ell(u,p)$ is such that $\ell(u,p) = \ell_i(u,p)) \mod c_i$, and $v = s + \ell(u,p)$ then u, v is a system of coordinates of $\mathcal{K}[x,y,z]$.

In this case, the ideal $\mathcal{I}_c^{\mathcal{Y}}$, where $\mathcal{Y} = \mathrm{Jac}_{(x,y,z)}(u,v,.)$, contains a polynomial of the form $p + Q(u, s+\ell(u,p))$ and if we let $p + Q(u,s+\ell(u,p)) = c(u)w$, then u,v,w is a coordinate system of $\mathcal{K}[x,y,z]$ which satisfies

$$\mathcal{X}(u) = 0,\ \mathcal{X}(v) = c(u),\ \mathcal{X}(w) = \partial_v Q(u,v).$$

Proof. $\Rightarrow$) By Theorem 4.3.1, the ideal $\mathcal{I}_c^{\mathcal{X}}$ contains a polynomial $h^\star$ of the form $p + Q^\star(u, s+\ell^\star(u,p))$ and if we let $v^\star = s + \ell^\star(u,p)$ and $h^\star = c(u)w^\star$, then $u, v^\star, w^\star$ is a coordinate system of $\mathcal{K}[x,y,z]$.

For any $i = 1,\dots,r$, let $h_i^\star, Q_i^\star, \ell_i^\star$ be respectively the reductions modulo c_i of $h^\star, Q^\star, \ell^\star$. The fact that reduction modulo c_i is a $\mathcal{K}$-algebra homomorphism implies that $h_i^\star = p + Q_i^\star(u, s+\ell_i^\star(u,p)) \mod c_i$.

Since $h^\star$ is a coordinate of $\mathcal{K}[u][p,s]$, it is a coordinate of $\mathcal{K}[u]/c_i[p,s]$ according to Theorem 1.4.1. By Lemma 4.4.1 *i*) let c_i, h_i be the reduced Gröbner basis of $\mathcal{I}_{c_i}^{\mathcal{X}}$ with respect to the lex-order $u \prec p \prec s$. According to Lemma 4.4.1 *ii*), there exists a unit ν_i modulo c_i such that $h_i^\star = \nu_i(u)h_i$. If we let $\mu_i(u)$ be such that $\mu_i\nu_i = 1 \mod c_i$, then we have $h_i = Q_i(u, s + \ell_i^\star(u,p)) + \mu_i(u)p$, where $Q_i \in \mathcal{K}[u,t]$.

Now, let $\ell(u,p)$ be such that $\ell(u,p) = \ell_i^\star(u,p) \mod c_i$ for any $i = 1,\dots,r$. Since $\ell_i^\star(u,p) = \ell^\star(u,p) \mod c_i$ we also have $\ell(u,p) = \ell^\star(u,p) \mod c_i$. We claim that $v = s + \ell(u,p)$ is a $\mathcal{K}[u]$-coordinate of $\mathcal{K}[u,v^\star,w^\star]$. Indeed, according to Theorem 1.4.1, it suffices to show that v is a coordinate of $\mathcal{K}[u]/d(u)[v^\star,w^\star]$ for any irreducible polynomial $d(u) \in \mathcal{K}[u]$. Depending on $d(u)$, we have the two following cases.

– For some $i = 1,\dots,r$, $d(u)$ and $c_i(u)$ are associate. In this case, we have $v = v^\star$ in $\mathcal{K}[u]/d(u)[v^\star,w^\star]$, and so v is a coordinate in $\mathcal{K}[u]/d(u)[v^\star,w^\star]$.

– For any $i = 1,\dots,r$, $\gcd(d,c_i) = 1$. In this case, $c(u)$ is a unit of $\mathcal{K}[u]/d(u)$. Let $\overline{\mathcal{X}}$ be the $\mathcal{K}[u]/d(u)$-derivation of $\mathcal{K}[u]/d(u)[v^\star,w^\star]$ induced by $\mathcal{X}$. Then $\overline{\mathcal{X}}(c^{-1}v) = 1$, which proves, according to Theorem 1.2.1, that v is a coordinate of $\mathcal{K}[u]/d(u)[v^\star,w^\star]$.

$\Leftarrow$) Assume that *i*) and *ii*) hold and let $\mathcal{Y} = \mathrm{Jac}(u,v,.)$. By Lemma 4.1.2, $\mathcal{Y}$ is locally nilpotent and $\mathcal{K}[u,v^\star,w^\star]^{\mathcal{Y}} = \mathcal{K}[u,v]$. Moreover, $\mathcal{Y}(p) = -c(u)$ and the fact that v is a coordinate of $\mathcal{K}[u][v^\star,w^\star]$ implies that $\mathcal{Y}$ has a slice w. We therefore have $\mathcal{Y}(p+c(u)w) = 0$, and so $p + c(u)w = Q(u,v)$. The fact that u,v,w is a coordinate system of $\mathcal{K}[x,y,z]$ follows immediately from Proposition 1.1.7, and a direct computation shows that $\mathcal{X}$ has a triangular form in the coordinate system u,v,w. ∎

Remark 4.4.3 *Let $\mathcal{X}$ be a triangular derivation and write*

$$\mathcal{X}(x) = 0,\ \mathcal{X}(y) = c(x),\ \mathcal{X}(z) = q(x,y),$$

and let $p = c(x)z - Q(x,y)$ where $q = \partial_y Q$. From Theorem 4.4.2 ii) we deduce that any $v = y + d(x)\ell(x,p)$, where $d(x)$ is the maximal square-free factor of $c(x)$, is a coordinate and gives rise to another coordinate system x,v,w in which $\mathcal{X}$ has a triangular form with a different polynomial Q. Thus, a triangulable derivation has many, actually infinitely many, triangular forms. It is also not clear whether there exists a distinguished form which could serve as a "normal form". Nevertheless, it should be noticed that all the triangular forms and their corresponding coordinate systems are built out of invariants of $\mathcal{X}$, namely $\mathcal{S}^{\mathcal{X}}$ and the ideals $\mathcal{I}_{c_i}^{\mathcal{X}}$ where the c_i's are the primes factors of $c(u)$.

4.5 The algorithm

Let us now discuss how to computationally check the conditions *i*) and *ii*) of Theorem 4.4.2. Assume that condition *i*) holds and that we have found a polynomial of the form $p + Q_i(u, s + \ell_i(u,p))$ in each ideal $\mathcal{I}_{c_i}^{\mathcal{X}}$. The computation of $\ell(u,p)$ is then just a matter of Chinese remaindering. On the other hand, from Lemma 4.1.2 we know that $\mathcal{Y} = \mathrm{Jac}_{(x,y,z)}(u,v,.)$, where $v = s+\ell(u,p)$, is locally nilpotent and $\mathcal{K}[x,y,z]^{\mathcal{Y}} = \mathcal{K}[u,v]$. Thus, v is a coordinate if and only if $\mathcal{Y}$ has a slice. This may be checked by computing a minimal local slice starting from the local slice p, which reduces to compute a reduced Gröbner basis G of $c(u)\mathcal{K}[x,y,z] \cap \mathcal{K}[u,v,p]$ with respect to the lex-order $u \prec v \prec p$.

In more explicit terms, v is a coordinate if and only if the computed Gröbner basis is of the form $c(u), p + Q(u, v)$. Notice that in case v is a coordinate, G also furnishes a polynomial w, with $p+Q(u, v) = c(u)w$, which completes u, v into a coordinate system and the polynomial Q which is involved in the triangular form of $\mathcal{X}$.

The condition *i)* is a matter of functional decomposition of polynomials, and the fact that we are here dealing with monic polynomials with respect to s makes it almost trivial.

Lemma 4.5.1 *Let $c(u)$ be an irreducible polynomial of $\mathcal{K}[u, v, w]$, n be a positive integer and $h \in \mathcal{K}[u, v, w]$ be monic with respect to w and write*

$$h = w^d + h_{d-1}(u, v)w^{d-1} + \cdots + h_0(u, v).$$

Then the following are equivalent:
i) $h = Q(u, w + \ell(u, v))$ in $\mathcal{K}[u]/c^n[v, w]$, with $\ell \in \mathcal{K}[u]/c^n[v]$ and $Q \in \mathcal{K}[u]/c^n[w]$,
ii) $h(u, v, w - \frac{h_{d-1}}{d})$, viewed in $\mathcal{K}[u]/c^n[v, w]$, is a polynomial of $\mathcal{K}[u]/c^n[w]$.

In this case, we may choose $\ell = \frac{h_{d-1}}{d}$ and $Q = h(u, v, w - \ell)$.

Proof. *i)* $\Rightarrow$ *ii)* Let us write $Q = w^d + q_{d-1}(u)w^{d-1} + \cdots + q_0(u)$. By expanding $Q(u, w + \ell(u, v))$ an comparing its coefficients with respect to w to those of h we get $h_{d-1}(u, v) = d\ell(u, v) + q_{d-1}(u)$. Therefore, $h(u, w - \frac{h_{d-1}}{d}) = Q(u, w - \frac{q_{d-1}(u)}{d})$ and this clearly shows that $h(u, w - \frac{h_{d-1}}{d}) \in \mathcal{K}[u]/c^n[w]$.

ii) $\Rightarrow$ *i)* Let us write $h(u, v, w - \frac{h_{d-1}}{d}) = Q(u, w)$. Then $Q(u, w + \frac{h_{d-1}}{d}) = h$ and we have the required decomposition. ∎

The following algorithm gives the main steps to check the triangulability and in the affirmative case produce the triangular form.

Algorithm 6: Triangulability Algorithm

Input : A locally nilpotent derivation $\mathcal{X}$ of $\mathcal{K}[x, y, z]$ and a generating system f, g of $\mathcal{K}[x, y, z]^{\mathcal{X}}$.
Output : Check whether $\mathcal{X}$ is triangulable. If so, compute a coordinate system u, v, w such that $\mathcal{X}$ has a triangular form in u, v, w.

1: Write $\mathcal{X} = a_1\partial_x + a_2\partial_y + a_3\partial_z$. Compute $c_1 = gcd(a_1, a_2, a_3)$ and write $\mathcal{X} = c1\mathcal{Y}$.
2: By using Algorithm 4, compute a minimal local slice $s$of $\mathcal{Y}$. A generator of $\mathcal{S}^{\mathcal{Y}}$ is then given by $c = \mathcal{Y}(s)$.
3: By using Algorithm 5, compute the rank of $\mathcal{X}$.
4: **if** $rank(\mathcal{X}) = 3$ **then**
5: $\mathcal{X}$ is not triangulable.
6: **end if**
7: **if** $rank(\mathcal{X}) = 1$ **then**

f, g, s is a coordinate system, and $\mathcal{X}$ has the triangular form

$$\mathcal{X}(f) = 0, \quad \mathcal{X}(g) = 0, \quad \mathcal{X}(s) = c_1(f, g).$$

end if
if $rank(\mathcal{X}) = 2$ **then**
  Let $c = c(u) = c_1^{n_1}, \ldots, c_r^{n_r}$, where u is a coordinate of $\mathcal{K}[x, y, z]$, and let p be such that $\mathcal{K}[f, g] = \mathcal{K}[u, p]$.
  for i to r **do**
    Let t_1, t_2, t_3 be new indeterminates, and compute a Gröbner basis $\mathcal{G}_i$ of the ideal $\mathcal{I}(c_i, u - t_1, p - t_2, s - t_3)$ with respect to the lexicographic order $t_1 \prec t_2 \prec t_3 \prec x \prec y \prec z$. Let $\mathcal{G}_{i,c_i} = \mathcal{G}_i \cap \mathcal{K}[t_1, t_2, t_3]$.
    if $\mathcal{G}_{i,c_i}$ is not of the form $\{c_i(t_1), h_i(t_1, t_2, t_3)\}$ **then**
      $\mathcal{X}$ is not triangulable.
    else if $h_i = Q_i(t_1, t_3 + \ell_i(t_1, t_2)) + \mu_i(t_1)t_2 \mod c_i(t_1)$ with $\mu_i(t_1)$ is unit $\mod c_i(t_1)$ **then**
      Let $v_i = s + \ell_i(u, p)$.
    else
      $\mathcal{X}$ is not triangulable.
    end if
  end for
  Find ℓ such that $\ell = \ell_i \mod c_i$, for $i = 1..r$
  Put $v = s + \ell$ and compute a Gröbner basis $\mathcal{G}$ of the ideal $\mathcal{I}(c, u - t_1, p - t_2, v - t_3)$ with respect to the lexicographic order $t_1 \prec t_3 \prec t_2 \prec x \prec y \prec z$.
  Let $\mathcal{G}_c = \mathcal{G} \cap \mathcal{K}[t_1, t_2, t_3]$.
  if $\mathcal{G}_c$ contains a polynomial of the form $t_2 + Q(t_1, t_3)$ **then**
    if we let w such that $p + Q(u, v) = wc(u)$,
    (u, v, w) is a triangulating system and $\mathcal{X}$ has the triangular form

$$\mathcal{X}(u) = 0, \quad \mathcal{X}(v) = c(u), \quad \mathcal{X}(w) = \partial_v Q(u, v).$$

  else
    $\mathcal{X}$ is not triangulable.
  end if
end if

4.6 Examples

In this section we give some examples to illustrate how our algorithm proceeds. All derivations are given in a Jacobian form, i.e., as $\mathrm{Jac}(f, g, .)$, since in such a form it is possible to check whether the given derivation is locally nilpotent and also to check whether its ring of constants in generated by f, g. For implementation, we use the Computer Algebra System Maple release 11.

Example 4.6.1 *Consider the following example from [21].*

$$f_1 = x,$$
$$g_1 = p = y + \frac{(xz + y^2)^2}{4},$$

and let the Jacobian derivation $\mathcal{X} := \mathrm{Jac}_{(x,y,z)}(f_1, g_1, .) = \partial_z g_1 \partial_x - \partial_y g_1 \partial_z$. *It is proved in [21] that* $\mathcal{X}$ *is locally nilpotent and its kernel is* $\mathcal{K}[x, p]$. *Our algorithm produces* $-x$ *as generator of the plinth ideal* $\mathcal{S}^{\mathcal{X}}$ *and* $s = -xz - y^2$ *as minimal local slice. The computation of a Gröbner basis of* $\mathcal{I}_x^{\mathcal{X}}$ *with respect to the lex-order* $x \prec g_1 \prec s$ *produces then* $x, (s^2 - 4g_1)^2 + 16s$, *and the polynomial* $(s^2 - 4g_1)^2 + 16s$ *cannot be written in the form* $\mu g_1 + Q(x, s + \ell(x, g_1))$, *where* $\mu \in \mathcal{K}^\star$. *Therefore,* $\mathcal{X}$ *is not triangulable.*

Example 4.6.2 *Consider the following polynomials*

$$f_2 = 2\,x + y + z^2 - 2\,zxy + x^2y^2,$$
$$g_2 = 3\,xy + 2\,x^2 - 2\,zx + 2\,x^2y + y^2 - yz + xy^2 + z^2y + z^2x - z^3 + 3\,z^2xy - 2\,zxy^2 - 2\,zx^2y - 3\,zx^2y^2 + x^2y^3 + x^3y^2 + x^3y^3 - z^2 + 2\,zxy - x^2y^2,$$

and let $\mathcal{Y} = \mathrm{Jac}_{(x,y,z)}(f_2, g_2, .)$. *The derivation* $\mathcal{Y}$ *is locally nilpotent and its kernel is* $\mathcal{K}[f_2, g_2]$. *Moreover, our algorithm produces* f *as a generator of the plinth ideal* $\mathcal{S}^{\mathcal{Y}}$ *and* $s = z - xy + 1$ *as a minimal local slice of* $\mathcal{Y}$. *The computation of a Gröbner basis of* $\mathcal{I}_{f_2}^{\mathcal{Y}}$ *with respect to the lex-order* $f_2 \prec g_2 \prec s$ *produces then* $f_2, s^2 - 2s + g_2 + 1$. *If we let* $u = f_2$ *and* $v = s - 1$ *then we get* $g_2 + v^2 = f_2 w$, *where* $w = -y - x + z - xy$. *This gives a coordinate system* u, v, w *such that*

$$\mathcal{Y}(u) = 0,\ \mathcal{Y}(v) = u, \mathcal{Y}(w) = 2v.$$

Chapter 5

Polynomial parametrization of nonsingular complete intersection curves

In this chapter we show a new approach to the problem of polynomial parametrization of algebraic curves using the language of locally nilpotent derivations. We give a criterion which is sufficient and necessary for the polynomial parametrization, and in the case the algebraic curve is a complete intersection, we present an algorithm which produces such a parametrization.

5.1 What is known

To parametrize a curve means to compute the birational equivalence of the curve with a projective line. This means computing an isomorphism between the function field of the curve and the function field of the projective plane. Computing a rational parametrization essentially requires an analysis of the singularities of the curve in the projective plane. This may actually be achieved either by blow-up techniques or by Puiseux expansions. It also requires to find a nonsingular point on the curve whose coordinates generate a field extension of the ground field of degree as small as possible. for more detail we refer to [3, 10, 58, 86, 90, 92, 93, 91].

Rational curve which have a polynomial parametrizations provide an interesting class of curves in so far as there are specific methods which apply to them and not to general rational curves, see e.g. [4, 34, 40, 48, 47, 46, 73]. It is therefore useful to decide whether a given space curve has a polynomial parametrization. In [98] it is proved that the condition under which an implicit algebraic curve can be parametrized using rational parametrization is that its genus must be zero. In [2] Abhyankar proved that a rational plane algebraic curve is polynomially parameterizable if and only if it has one place at infinity. A simpler characterization of such curves, together with an algorithm to compute a polynomial parametrization in case it exists, is given in [73]. However, notice that this method requires a rational parametrization of the algebraic curve to be available.

In the case of a plane curve without affine singularities, an algorithm based on the Abhyankar-Moh theorem [1] is given in [57]. Its algebraic complexity is $O(d^3 logd)$ field operations, where d is the degree of the curve. Recently, another algorithm based on Gröbner reductions [95] is given in [96], with $O(d^2 logd)$ field operations.

5.2 Algebriac curves

Let $\mathcal{K}$ be a field of characteristic zero and $\overline{\mathcal{K}}$ be its algebraic closure. Let $\mathcal{I}$ be an ideal of $\mathcal{K}[\underline{x}]$ and $\mathcal{C} \subseteq \overline{\mathcal{K}}^n$ be the algebraic set defined by $\mathcal{I}$. We will say in this case that $\mathcal{C}$ is defined over $\mathcal{K}$. The ideal of $\mathcal{C}$, namely the set of all polynomials which vanish on $\mathcal{C}$, will be denoted by $\mathcal{I}_{\mathcal{K}}(\mathcal{C})$ and its coordinate ring $\mathcal{K}[x]/\mathcal{I}_{\mathcal{K}}(\mathcal{C})$ by $\mathcal{K}[\mathcal{C}]$. When the ideal $\mathcal{I}_{\mathcal{K}}(\mathcal{C})$ is equi-dimensional of dimension 1, we call $\mathcal{C}$ an algebraic curve. An algebraic curve is called absolutely irreducible if the ideal $\mathcal{I}_{\overline{\mathcal{K}}}(\mathcal{C})$ is prime.

Given an algebraic curve $\mathcal{C}$, there exists a positive integer d such that a generic affine hyperplane $\mathcal{H}$ of $\overline{\mathcal{K}}^n$ intersects $\mathcal{C}$ at d points. Moreover, if a hyperplane $\mathcal{H}$ does not contain the curve, the intersection $\mathcal{H} \cap \mathcal{C}$ contains at most d points. The integer d is called the degree of the curve and is denoted by $\deg(\mathcal{C})$.

An algebraic curve $\mathcal{C}$ is called an ideal theoretically complete intersection, or complete intersection for short, if $I_{\mathcal{K}}(\mathcal{C})$ is generated by $n-1$ polynomials $f_1, \ldots, f_{n-1}$. In this case, $\deg(\mathcal{C}) \leq \prod_i \deg(f_i)$ by Bézout theorem, and equality holds if the hypersurfaces $f_i = 0$ have only finitely many intersection points in the hyperplane at infinity of the projective space $\mathbb{P}^n(\overline{\mathcal{K}})$.

The following result characterizes the nilpotency of derivations on coordinate ring of nonsingular algebraic curves.

Theorem 5.2.1 *Let $\mathcal{C}$ be an n-space nonsingular algebraic curve of degree d defined over $\mathcal{K}$ and let $\mathcal{X}$ be a derivation of $\mathcal{K}[\mathcal{C}]$. Then the following are equivalent:*
i) the derivation $\mathcal{X}$ is locally nilpotent,
ii) for any $i = 1, \ldots, n$, $\mathcal{X}^{d+1}(x_i) = 0$ in $\mathcal{K}[\mathcal{C}]$.

Proof. *i)* $\Rightarrow$ *ii)* Let $\mathcal{I}_{\overline{\mathcal{K}}}(\mathcal{C})$ be the ideal of the curve $\mathcal{C}$ in $\overline{\mathcal{K}}[x]$, and recall that $\mathcal{I}_{\overline{\mathcal{K}}}(\mathcal{C})$ is radical. Let us write $\mathcal{I}_{\overline{\mathcal{K}}}(\mathcal{C}) = \mathcal{P}_1 \cap \ldots \cap \mathcal{P}_r$ where the $\mathcal{P}_i$'s are prime, and let $\mathcal{C}_i$ be the curve defined by $\mathcal{P}_i$. Then $\mathcal{C} = \cup \mathcal{C}_i$, and the fact that $\mathcal{C}$ is nonsingular implies that $\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$ for $i \neq j$. By the Hilbert Nullstellensatz, we have $\mathcal{P}_i + \mathcal{P}_j = (1)$ for $i \neq j$. According to the Chinese remainder theorem, the $\overline{\mathcal{K}}$-algebra $\overline{\mathcal{K}}[\mathcal{C}]$ is isomorphic to $\prod_i \overline{\mathcal{K}}[\mathcal{C}_i]$. As by product, the derivation $\mathcal{X}$ can be identified through this isomorphism to $(\mathcal{X}_1, \ldots, \mathcal{X}_r)$, where $\mathcal{X}_i$ is a derivation of $\overline{\mathcal{K}}[\mathcal{C}_i]$. On the other hand, since $\deg(\mathcal{C}_i) \leq \deg(\mathcal{C})$, it suffices to prove the bound for every $\mathcal{X}_i$. Thus, without loss the generality, we may assume that $\mathcal{C}$ is absolutely irreducible.

Let v be a local slice of $\mathcal{X}$ and let $c = \mathcal{X}(v)$. The fact that $\overline{\mathcal{K}}[\mathcal{C}]$ is of transcendence degree 1 over $\overline{\mathcal{K}}$ and v is transcendent over $\overline{\mathcal{K}}[\mathcal{C}]^{\mathcal{X}}$ implies that $\overline{\mathcal{K}}[\mathcal{C}]^{\mathcal{X}}$ is algebraic over $\overline{\mathcal{K}}$, and so $\overline{\mathcal{K}}[\mathcal{C}]^{\mathcal{X}} = \overline{\mathcal{K}}$ since $\overline{\mathcal{K}}$ is algebraically closed. In particular, c is a unit of $\overline{\mathcal{K}}[\mathcal{C}]$ and therefore $s = c^{-1}v$ is a slice of $\mathcal{X}$.

By Proposition 1.1.7, we may write $\overline{\mathcal{K}}[\mathcal{C}] = \overline{\mathcal{K}}[s]$, and we have $\mathcal{X} = \partial_s$. Let us write $x_i = \sum a_{i,j} s_j$, and let $\deg_s(x_i) = d_i$. Clearly, $\mathcal{X}^{d_i+1}(x_i) = 0$. It remains to prove that $d_i \leq d$ for any i. The case of $x_i(s)$ being constant is trivial, so let us assume that $x_i(s)$ is nonconstant and for any $a \in \overline{\mathcal{K}}$ let $\mathcal{V}_{i,a}$ be the intersection of the curve $\mathcal{C}$ with the hyperplane $x_i = a$. Then $\mathcal{V}_{i,a} = \{\alpha \in \overline{\mathcal{K}}^n / \alpha = (x_1(s), \ldots, x_n(s)), x_i(s) = a\}$. Let us choose a in such a way that the roots of $x_i(s) - a$ are all simple. Moreover, since $\mathcal{C}$ is nonsingular, then two distinct roots of $x_i(s) - a$ give distinct points of $\mathcal{V}_{i,a}$, and so $|\mathcal{V}_{i,a}| = d_i$. On the other hand, $|\mathcal{V}_{i,a}| \leq d$ since $\mathcal{C}$ and the hyperplane $x_i = a$ may intersect in the hyperplane at infinity of the projective space $\mathbb{P}^n\overline{\mathcal{K}}$. Therefore, $d_i \leq d$.
ii) $\Rightarrow$ *i)* Since $x_1, \ldots, x_n$ generate $\mathcal{K}[\mathcal{C}]$ and $\mathcal{X}_f^{d+1}(x_i) = 0$, the derivation $\mathcal{X}_f$ is locally nilpotent. ∎

5.3 Polynomial parametrization of algebraic curves

In this section we give the main theoretical results which are at the basis of our method. The main idea behind our method is that if an absolutely irreducible nonsingular curve $\mathcal{C}$ has a polynomial parametrization $x(t)$, then this parametrization is in fact a solution of an ordinary differential equation $\dot{x} = p(x)$, where the components of p are polynomials. Moreover, this differential equation has no fixed points on the curve $\mathcal{C}$. In algebraic terms this means that the derivation corresponding to this differential equation is locally nilpotent and generates the module $\mathcal{D}_{\overline{\mathcal{K}}}(\overline{\mathcal{K}}[\mathcal{C}])$. It turns out that we always may choose a derivation with coefficients in the ground field $\mathcal{K}$, and this is the main reason behind the fact that we can find a parametrization with coefficients in $\mathcal{K}$.

The following lemma will be needed.

Lemma 5.3.1 *Let $\mathcal{C}$ be a nonsingular affine n-space algebraic curve defined over $\mathcal{K}$, and $\mathcal{K}[\mathcal{C}]$ be its coordinate ring. Assume that $\mathcal{C}$ is absolutely irreducible and has a polynomial parametrization. Then the units of $\mathcal{K}[\mathcal{C}]$ are the elements of $\mathcal{K}^*$.*

Proof. Let $f_1, \ldots, f_r$ be a generating system of the ideal $\mathcal{I}_{\mathcal{K}}(\mathcal{C})$. Since $\mathcal{I}_{\mathcal{K}}(C)$ is radical, the f_i's also generate $\mathcal{I}_{\overline{\mathcal{K}}}(\mathcal{C})$. The fact that $\mathcal{C}$ is absolutely irreducible, nonsingular and has a polynomial parametrization implies that $\overline{\mathcal{K}}[\mathcal{C}] \cong_{\overline{\mathcal{K}}} \overline{\mathcal{K}}^{[1]}$. As by product, the units of $\overline{\mathcal{K}}[\mathcal{C}]$ are the elements of $\overline{\mathcal{K}}^*$. Now, let $g \in \mathcal{K}[x]$ which is a unit in $\mathcal{K}[\mathcal{C}]$, and write

$$g = u + \sum a_i(x) f_i(x),$$

with $u \in \overline{\mathcal{K}}^*$ and $a_i \in \overline{\mathcal{K}}[x]$. Let $\mathcal{F}$ be the field generated over $\mathcal{K}$ by u and the coefficients of the a_i's, and write $\mathcal{F} = \mathcal{K}[\mu]$ according to the primitive element theorem. The above relation may then be rewritten as

$$g = \sum u_j \mu^j + \sum f_i \sum a_{i,j} \mu^j,$$

where $u_i \in \mathcal{K}$ and $a_{i,j} \in \mathcal{K}[x]$. Since $\mathcal{K}[\mu]$ and $\mathcal{K}[x]$ are linearly disjoint over $\mathcal{K}$, we get $g = u_0 + \sum a_{i,0} f_i$, and so $g = u_0$ in $\mathcal{K}[\mathcal{C}]$. ∎

Now, we give the main result of this section

Theorem 5.3.2 *Let $\mathcal{C}$ be an affine n-space algebraic curve defined over $\mathcal{K}$. Then the following are equivalent:*

i) the curve $\mathcal{C}$ is absolutely irreducible, nonsingular and has a polynomial parametrization with coefficients in a field extension of $\mathcal{K}$,

ii) $\mathcal{D}_{\mathcal{K}}(\mathcal{K}[\mathcal{C}])$ is free of rank 1, any generator $\mathcal{X}$ is locally nilpotent and $\mathcal{K}[\mathcal{C}]^{\mathcal{X}} = \mathcal{K}$. In this case, $\mathcal{X}$ has a slice s and a parametrization of $\mathcal{C}$ is given by

$$x_i(s) = \sum_j \frac{1}{j!} \xi_{-s}(\mathcal{X}^j(x_i)) s^j, \qquad i = 1, \ldots, n. \tag{5.1}$$

In particular, $\mathcal{C}$ has a polynomial parametrization with coefficients in $\mathcal{K}$.

Proof. $i) \Rightarrow ii)$ Let us write $\overline{\mathcal{K}}[\mathcal{C}] = \overline{\mathcal{K}}[s]$. Then the derivation defined by $\mathcal{X}(s) = 1$ is clearly locally nilpotent and generates $\mathcal{D}_{\overline{\mathcal{K}}}(\overline{\mathcal{K}}[\mathcal{C}])$. Now, we need to show that $\mathcal{X}$, or another generator, restricts to a derivation of $\mathcal{K}[\mathcal{C}]$. Since $\mathcal{X}$ is not trivial, we may assume that $\mathcal{X}(x_1) \neq 0$. Let us write $\mathcal{X}(x_1) = \sum_\alpha a_\alpha x^\alpha$ where the monomials x^α with $a_\alpha \neq 0$ are linearly independent, in $\overline{\mathcal{K}}[\mathcal{C}]$, over $\overline{\mathcal{K}}$. Then one, at least, of the coefficients a_α, say a_0, is nonzero, and even if it means dividing by it, we may assume $a_0 = 1$.

Let us prove that $\mathcal{X}(x_i) \in \mathcal{K}[\mathcal{C}]$ for any $i = 1, \ldots, n$. For this, we let σ be a $\mathcal{K}$-automorphism of $\overline{\mathcal{K}}$ and we extend it to a $\mathcal{K}[\underline{x}]$-automorphism of $\overline{\mathcal{K}}[\underline{x}]$ by letting $\sigma(x_i) = x_i$. The fact that $\mathcal{I}_{\overline{\mathcal{K}}}(\mathcal{C})$ is generated by polynomials in $\mathcal{K}[x]$ implies that

$$\sigma(\mathcal{I}_{\overline{\mathcal{K}}}(\mathcal{C})) = \mathcal{I}_{\overline{\mathcal{K}}}(\mathcal{C})$$

so σ induces a $\mathcal{K}[\mathcal{C}]$-automorphism of $\overline{\mathcal{K}}[\mathcal{C}]$ which we also denoted by σ. Since $\sigma\mathcal{X}\sigma^{-1} \in \mathcal{D}_{\overline{\mathcal{K}}}(\overline{\mathcal{K}}[\mathcal{C}])$, we have $\sigma\mathcal{X}\sigma^{-1} = a\mathcal{X}$, with $a \in \overline{\mathcal{K}}[\mathcal{C}]$. On the other hand, the fact that σ is a $\mathcal{K}[\mathcal{C}]$-automorphism of $\overline{\mathcal{K}}[\mathcal{C}]$ implies that $\sigma\mathcal{X}\sigma^{-1}$ also generated $\mathcal{D}_{\overline{\mathcal{K}}}(\overline{\mathcal{K}}[\mathcal{C}])$. This gives $\mathcal{X} = b.\sigma\mathcal{X}\sigma^{-1}$, and hence $ab = 1$. Therefore, $a \in \overline{\mathcal{K}}^*$. Since $\sigma^{-1}(x_1) = x_1$, then $\sigma\mathcal{X}\sigma^{-1}(x_1) = \sigma\mathcal{X}(x_1)$, and so

$$\sum \sigma(a_\alpha) x^\alpha = a \sum a_\alpha x^\alpha$$

According to the linear independence of the x^α's over $\overline{\mathcal{K}}$ and the fact that $a_0 = 1$ we get $a = 1$, and hence $\sigma\mathcal{X}\sigma^{-1} = \mathcal{X}$. From classical Galois theory, we deduce that $\mathcal{X}(x_i) \in \mathcal{K}[\mathcal{C}]$ for any i, and so $\mathcal{X}$ restricts to a derivation of $\mathcal{K}[\mathcal{C}]$. In the rest of the proof, we also denote by $\mathcal{X}$ the restriction of $\mathcal{X}$ to $\mathcal{K}[\mathcal{C}]$.

Let us now prove that $\mathcal{X}$ generates $\mathcal{D}_{\mathcal{K}}(\mathcal{K}[\mathcal{C}])$. Given any $\mathcal{Y} \in \mathcal{D}_{\mathcal{K}}(\mathcal{K}[\mathcal{C}])$, we may write $\mathcal{Y} = a\mathcal{X}$ with $a \in \overline{\mathcal{K}}[\mathcal{C}]$. Applying any $\mathcal{K}[\mathcal{C}]$-automorphism of $\overline{\mathcal{K}}[\mathcal{C}]$ to this relation we get $\mathcal{Y} = \sigma(a)\mathcal{X}$, and so $a = \sigma(a)$. This proves that $a \in \mathcal{K}[\mathcal{C}]$, and hence $\mathcal{X}$ generates $\mathcal{D}_{\mathcal{K}}(\mathcal{K}[\mathcal{C}])$.

Let $c \in \mathcal{K}[\mathcal{C}]$ be such that $\mathcal{X}(c) = 0$, and assume that $c \neq 0$. The fact that $\mathcal{K}[\mathcal{C}]$ is of transcendence degree 1 over $\mathcal{K}$ and $\mathcal{X} \neq 0$ implies, according to the equality (1.3) , that $\mathcal{K}[\mathcal{C}]^{\mathcal{X}}$ is of transcendence degree zero over $\mathcal{K}$, hence it is algebraic over $\mathcal{K}$, and so c is algebraic over $\mathcal{K}$.

Since c is algebraic over $\mathcal{K}$ and $c \neq 0$, it is a unit of $\mathcal{K}[\mathcal{C}]$, and by Lemma 5.3.1 $c \in \mathcal{K}$. This proves that $\mathcal{K}[\mathcal{C}]^{\mathcal{X}} = \mathcal{K}$. On the other hand, if v is a local slice of $\mathcal{X}$ then $\mathcal{X}(v) = c \neq 0$ and $\mathcal{X}(c) = 0$. Therefore, $c \in \mathcal{K}^*$ and so $s = c^{-1}v$ is a slice of $\mathcal{X}$. By the relation (1.2) we get a parametrization of $\mathcal{C}$ in the form (5.1), which clearly has its coefficients in the ground field $\mathcal{K}$.

ii) $\Rightarrow$ *i)* The fact that $\mathcal{C}$ is absolutely irreducible and nonsingular follows immediately from the fact that $\mathcal{C}$ is isomorphic to $\overline{\mathcal{K}}$. ∎

Given an algebraic curve $\mathcal{C}$ and $\mathcal{I}_{\mathcal{K}}(\mathcal{C})$ its defining ideal, an algorithmic realization of Theorem 5.3.2 would mainly consist of the following steps:

P_1. Check whether $\mathcal{D}_{\mathcal{K}}(\mathcal{K}[\mathcal{C}])$ is free of rank 1, and if so, find a generator.

P_2. In case a generator $\mathcal{X}$ of $\mathcal{D}_{\mathcal{K}}(\mathcal{K}[\mathcal{C}])$ is found, check whether it is locally nilpotent.

P_3. In case $\mathcal{X}$ is locally nilpotent, compute a slice. For this, choose x_i in such a way that $\mathcal{X}(x_i) \neq 0$. Let $a_j = \mathcal{X}^j(x_i)$ and r be the biggest integer such that $a_r \neq 0$. If $a_r \notin \mathcal{K}$ then $\mathcal{K} \subsetneq \mathcal{K}[\mathcal{C}]^{\mathcal{X}}$. Otherwise, $s = a_r^{-1}\, a_{r-1}$ is a slice of $\mathcal{X}$.

P_4. If a slice is found, compute a generating system of $\mathcal{K}[\mathcal{C}]^{\mathcal{X}}$ by using Lemma 1.1.8, and check whether $\mathcal{K} = \mathcal{K}[\mathcal{C}]^{\mathcal{X}}$. If so, compute a parametrization by using the identity (1.2).

The steps P_3 and P_4 can clearly be achieved by using Gröbner bases and normal forms, and the step P_2 is also a matter of normal form computation due to Theorem 5.2.1, but the first one need more work. We will see in what follow that step P_1 has an easy solution in the case of a complete intersection nonsingular curve.

5.4 Nonsingular complete intersection curves

Let $\mathcal{C}$ be a complete intersection curve, and let $f = f_1, \ldots, f_{n-1}$ be a list of polynomials in $\mathcal{K}[x]$ which generates the ideal $\mathcal{I}_{\mathcal{K}}(\mathcal{C})$. Let $\mathrm{Jac}(f)$ be the Jacobian matrix of f. This is an $n-1$ by n matrix, and so it has exactly n principal minors. Recall that a point of $\mathcal{C}$ is singular if and only if all the principal minors of $\mathrm{Jac}(f)$ vanish at that point. Let $\mathcal{X}_f$ be the derivation of $\mathcal{K}[x]$ defined by $\mathcal{X}_f(h) = \det\mathrm{Jac}(f,h)$. It is obvious to see that $\mathcal{X}_f(f_i) = 0$ for any $i = 1, \ldots, n-1$, and therefore $\mathcal{X}_f$ induces a derivation of $\mathcal{K}[\mathcal{C}]$. By abuse of notation we also use $\mathcal{X}_f$ to denote such a derivation.

The following lemma gives an answer to the problem of finding a generator of the module $\mathcal{D}_{\mathcal{K}}(\mathcal{K}[\mathcal{C}])$.

Lemma 5.4.1 *Let $\mathcal{C}$ be a nonsingular complete intersection curve, and let $f = f_1, \ldots, f_{n-1}$ be a list of polynomials in $\mathcal{K}[x]$ such that $\mathcal{I}_{\mathcal{K}}(\mathcal{C}) = \mathcal{I}_{\mathcal{K}}(f)$. Then $\mathcal{D}_{\mathcal{K}}(\mathcal{K}[\mathcal{C}])$ is a free $\mathcal{K}[\mathcal{C}]$-module of rank 1 generated by $\mathcal{X}_f$.*

Proof. Let $m_1, \ldots, m_n$ be the principal minors of $\mathrm{Jac}(f)$, and notice that $\mathcal{X}_f = \sum_i (-1)^{i+n} m_i \partial_{x_i}$. The fact that $\mathcal{I}_{\mathcal{K}}(\mathcal{C}) = \mathcal{I}_{\mathcal{K}}(f)$ and $\mathcal{C}$ is nonsingular implies that the m_i's do not have common zeros in $\mathcal{C}$, and so we have $\sum a_i m_i = 1$ with $a_i \in \mathcal{K}[\mathcal{C}]$.

Let $\mathcal{X} = \sum g_j \partial_{x_j}$ be a derivation of $\mathcal{K}[\mathcal{C}]$. Then for any $i = 1, \ldots, n-1$, we have $\sum_j g_j \partial_{x_j} f_i = 0$. Moreover, if we let $\sum_j (-1)^{j+n} g_j a_j = p$, then we get a linear system

$$A.g = (0, \ldots, 0, p)^t,$$

where $g = (g_1, \ldots, g_n)^t$ and $A = (a_{i,j})$ is defined by

$$a_{i,j} = \begin{cases} \partial_{x_j} f_i & i \leq n-1, \\ (-1)^{j+n} a_j & i = n \end{cases}$$

By expanding the determinant of A with respect to its last line we get $\det(A) = \sum_j a_j m_j = 1$, and so A is invertible. This implies that $g = A^{-1}.(0, \ldots, 0, p)$, and so to get the g_i's, we just need to compute the entries in the last column of A^{-1}. Since A^{-1} is the transpose of the adjoint of A, the entry (i, n) of A^{-1} is $(-1)^{i+n}\det(A_{n,i})$, where $A_{n,i}$ is the matrix obtained form A by removing the line n and the column i. Clearly, $\det(A_{n,i}) = m_i$, and so $g_i = (-1)^{i+n} m_i p$. This finally gives $\mathcal{X} = p \sum_i (-1)^{i+n} m_i \partial_{x_i} = p\mathcal{X}_f$. ∎

In the case of a nonsingular complete intersection curve, we have the following reformulation of Theorem 5.3.2.

Theorem 5.4.2 *Let $f = f_1, \ldots, f_{n-1}$ be a list a polynomials in $\mathcal{K}[x]$ and let $\mathcal{C}$ be the algebraic set defined by f. Then the following are equivalent:*

i) $\mathcal{C}$ is an absolutely irreducible nonsingular curve having a polynomial parametrization and $\mathcal{I}_{\mathcal{K}}(\mathcal{C}) = \mathcal{I}_{\mathcal{K}}(f)$,

ii) For any $i = 1, \ldots, n$ we have $\mathcal{X}_f^{d+1}(x_i) = 0$ in $\mathcal{K}[x]/\mathcal{I}(f)$, with $d = \prod \deg(f_k)$, and the ring of constants of $\mathcal{X}_f$ is $\mathcal{K}$.

Proof. *i)* $\Rightarrow$ *ii)* We have $\mathcal{I}_{\mathcal{K}}(\mathcal{C}) = \mathcal{I}_{\mathcal{K}}(f)$, and so $\mathcal{K}[x]/\mathcal{I}_{\mathcal{K}}(f) = \mathcal{K}[\mathcal{C}]$. By Lemma 5.4.1 the derivation $\mathcal{X}_f$ generates $\mathcal{D}_{\mathcal{K}}(\mathcal{K}[\mathcal{C}])$. The fact that $\mathcal{C}$ is absolutely irreducible, nonsingular and has a polynomial parametrization implies, by Theorem 5.3.2, that the generator $\mathcal{X}_f$ is locally nilpotent and its ring of constants is $\mathcal{K}$. On the other hand, since $\deg(\mathcal{C}) \leq \prod \deg(f_k)$, then $\mathcal{X}_f^{d+1}(x_i) = 0$ by Theorem 5.2.1.
ii) $\Rightarrow$ *i)* Let v be a local slice of $\mathcal{X}_f$ and write $\mathcal{X}_f(v) = c \neq 0$. Since c is a constant of $\mathcal{X}_f$, then $c \in \mathcal{K}^*$, and so $s = c^{-1}v$ is a slice of $\mathcal{X}_f$. By Proposition 1.1.7, we have $\mathcal{K}[x]/\mathcal{I}_{\mathcal{K}}(f) = \mathcal{K}[s]$. This proves that $\mathcal{C}$ is isomorphic to $\mathcal{K}$, and so $\mathcal{C}$ is absolutely irreducible, nonsingular and has a polynomial parametrization. The fact that $\mathcal{K}[s]$ is a domain implies that $\mathcal{I}_{\mathcal{K}}(\mathcal{C})$ is prime, and so $\mathcal{I}_{\mathcal{K}}(\mathcal{C}) = \mathcal{I}_{\mathcal{K}}(f)$ by the Hilbert Nullstellensatz. ∎

5.5 Parametrization algorithm

The following algorithm gives the main steps to compute the polynomial parametrization of an algebraic curve

---

Algorithm 7: Polynomial parametrization.

Input : A list $f = f_1, \ldots, f_{n-1}$ of polynomials in $\mathcal{K}[x]$. We let $\mathcal{C}$ be the algebraic set defined by f.
Output : A polynomial parametrization of $\mathcal{C}$ in case $\mathcal{C}$ is a nonsingular curve, $\mathcal{I}_{\mathcal{K}}(\mathcal{C}) = \mathcal{I}_{\mathcal{K}}(f)$ and such a parametrization exists.

1: Compute a Gröbner basis G of $\mathcal{I}_{\mathcal{K}}(f)$. Any monomial order will do the job since no projection is needed.
2: Check whether $\mathcal{X}_f$ is locally nilpotent. If so, compute a slice and check whether the ring of constants of $\mathcal{X}_f$ is $\mathcal{K}$.

- For any $i = 1, \ldots, n$ compute incrementally $\mathcal{X}_f^j(x_i)$, compute its normal form $a_{i,j}$ with respect to G and stop if $a_{i,j} = 0$ or $j = d+1$, with $d = \prod \deg(f_k)$. If the sequence $(a_{i,j})$ does not reach 0 for some i then $\mathcal{X}_f$ is not locally nilpotent.
- Check whether for any i the last nonzero element a_{i,r_i} in the sequence $(a_{i,j})$ is an element of $\mathcal{K}$. If it is not the case we have $\mathcal{K} \subsetneq (\mathcal{K}[x]/\mathcal{I}_{\mathcal{K}}(f))^{\mathcal{X}_f}$.
- Choose i in such a way that $r_i \geq 1$ (if no such i exists then this means that $\mathcal{X}_f = 0$), and let $s = a_{i,r_i}^{-1} a_{i,r_i-1}$. Then s is a slice of X_f .
- Compute a generating system $c_1, \ldots, c_n$ of $(\mathcal{K}[x]/\mathcal{I}_{\mathcal{K}}(f))^{\mathcal{X}_f}$ by using lemma 5.4.1 and normal forms with respect to G. If one, a least, of the c_i's is not in $\mathcal{K}$, then $\mathcal{K} \subsetneq (\mathcal{K}[x]/\mathcal{I}_{\mathcal{K}}(f))^{X_f}$.

3: Compute a parametrization of $\mathcal{C}$ using the identity (1.2).

5.5.1 Comparison to projection methods

Projection based algorithms for computing a parametrization of a space curve mainly consist of the two following steps.

S_1. Find a birational projection of $\mathcal{C}$ onto a plane curve $\mathcal{C}_h$ given by a bivariate polynomial h, and compute the birational inverse of the projection. To simplify, we assume that the projection is $x \longmapsto (x_1, x_2)$.

S_2. Compute a parametrization of the plane curve $\mathcal{C}_h$, and deduce from it a parametrization of $\mathcal{C}$ by using the birational inverse of the projection.

The first step S_1 can for example be achieved by Gröbner basis of $\mathcal{I}_{\mathcal{K}}(\mathcal{C})$ with respect to an elimination order, say the lexicographic order $x_1 \prec x_2 \prec \ldots \prec x_n$. The Gröbner basis contains the equation $h(x_1, x_2)$ of the plane projection, and also enough information to compute the inverse of the projection. Indeed, since the projection is birational, the Gröbner basis contains for each $i \geq 3$ a polynomial in $\mathcal{K}[x_1, \ldots, x_i]$ which is of degree 1 with respect to x_i. In case $\mathcal{C}$ is nonsingular in the projective space, and under some genericity conditions on the projection, it is shown in [10] that the computed Gröbner basis also contains information on the adjoint curves to $\mathcal{C}_h$, which helps a lot for its parametrization. In the case of a complete intersection curve in the

3-dimensional space, one can use pseudo-remainder sequences instead of Gröbner bases [3].

For the step S_2, several algorithms exist so far [10, 58, 86, 90, 91, 92, 93] and they consist of two major steps. The first one is a fine analysis of the singularities, in the projective plane, of the projection $\mathcal{C}_h$. This is in fact tightly bound to the computation of a nonsingular model of $\mathcal{C}_h$, and one feels it is redundant to do so if the original curve $\mathcal{C}$ is nonsingular. The second step is to find a nonsingular point on the curve. A parametrization of $\mathcal{C}_h$ is obtained by computing a rational function which has a pole of multiplicity 1 at the chosen point and no other poles.

The choice of the point is important in so far as the resulting parametrization has its coefficients in the field extension generated by the coordinates of the chosen point. Therefore, one needs to find a point on the curve which generates a field extension of degree as small as possible, and this is quite involved [92]. It is also important to notice that if the point is chosen in the affine plane then the resulting parametrization has rational functions, and not polynomials, as components even in the case where the curve has a polynomial parametrization. This is due to the fact that the chosen point is a pole of the computed birational map from $\mathcal{C}$ into $\mathbb{P}^1\overline{\mathcal{K}}$. In this case a re-parametrization of the curve is needed, see e.g. [73].

Let $\mathcal{C}$ be an affine nonsingular complete intersection curve having a polynomial parametrization. A generic plane projection $\mathcal{C}_h$ of $\mathcal{C}$ has only nodes as singularities in the affine plane. Nevertheless, $\mathcal{C}_h$ always has one place at infinity, and if $\deg(\mathcal{C}) \geq 4$ this place is centered at a big singular point which could be rather complicated [2]. In our method, once a Gröbner basis of the ideal of the curve is computed, we only need to perform normal form computation to solve for a parametrization. In contrast to projection based methods, we do not need to deal with the singular point at infinity or to find a nonsingular point on the curve. Notice also that we have much more flexibility in the choice of the monomial order. This is important since Gröbner basis computation is very sensitive to the chosen order and elimination orders, which are needed in projection based methods, are reputed to be very costly compared to other orders such as the graded reverse lexicographic order.

5.5.2 Examples

In this section we give some computational examples, and compare the performance of our method with the projection based one.

Example 1: Consider the 3-space curve $\mathcal{C}$ given implicitly by
$f = -x^6 + x - z^2 + 2zx^3 - 2zy^2 + 2y^2x^3 - y^4$,
$g = -1/2x^9 + y - 3/2xz + 1/2z^3 - 3/2x^3z^2 + 3/2z^2y^2 + 3/2zx^6 - 3x^3zy^2 + 3/2zy^4 + 3/2x^3 + 3/2y^2x^6 - 3/2x^3y^4 - 3/2xy^2 + 1/2y^6$.

Applying algorithm 7, we get the following parametrization in 1.151 seconds.

$x(t) = t^2$,
$y(t) = t^3 - 3/2t^6 + 3/2t^8$,
$z(t) = t + 3t^9 - 3t^{11} - 9/4t^{12} + 9/2t^{14} - 9/4t^{16}$.

By projecting the curve $\mathcal{C}$ into the (x, y)-plane we get a curve whose parametrization, using the *Maple package Algcurves* , requires 9.864 seconds. The resulting parametrization has rational components, which means that a re-parametrization step is needed.

Example 2: Another example of 3-space curve is defined by

$$f = 5x - 5z + 3y^3z + 3y^4 + 18y^2xz + 18y^3x + 36yx^2z + 36y^2x^2 + 24x^3z + 24x^3y + 7,$$
$$g = -13y + 2x - 10xz + 5z^2 - 10xy - 6y^3z^2 - 12y^4z - 6y^5 - 36y^2xz^2 - 72y^3xz - 36y^4x - 72yx^2z^2 - 144y^2x^2z - 72y^3x^2 - 48x^3z^2 - 96x^3yz - 48x^3y^2 - 14z - 5y^2 + 1.$$

Using our method, the resulting parametrization of this curve is

$$x(t) = 2/5 + 8t + 125t^2 - 1125t^3 + 140625t^5 - 5859375t^7,$$
$$y(t) = -9/5 - 16t - 125t^2 + 2250t^3 - 281250t^5 + 11718750t^7,$$
$$z(t) = 9/5 + 11t + 125t^2 - 2250t^3 + 281250t^5 - 11718750t^7,$$

and the running time is 1.011 seconds. On the other hand, using the projection onto the (x, y)-plane, the parametrization of the resulting curve is achieved in 90.240 seconds. If we choose the projection onto the (y, z)-plane, we get a parametrization in 13.690 seconds. The obtained parametrization in this example have rational components with huge coefficients.

We have also tested our method in several other examples, and it compares very favorably to the projection based method. In fact, our method is even faster than the parametrization step of the plane projection in the projection based method.

Bibliography

[1] S. S. Abhyankar and T. T. Moh, Embeddings of the line in the plane. *J. Reine Angew. Math.*, 276(1975),148–166.

[2] S. S. Abhyankar, What is the difference between a parabola and a hyperbola. *The Mathematical Intelligencer*, 4(10)(1988),36–43.

[3] S. S. Abhyankar and C. L. Bajaj, Automatic parameterization of rational curves and surfaces, iv: algebraic space curves. *ACM Trans. Graphics*, 8(1989),325–334.

[4] S. S. Abhyankar, *Algebraic geometry for scientists and engineers*, volume 35. Mathematical Surveys and monographs, AMS, 1990.

[5] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, volume 3 of Graduate Texts in Mathematics. AMS, 1994.

[6] T. Bandman and L.Makar-Limanov, Affine surfaces with $AK(S) = (C)$, *Michigan Math. J.*, 49(2001,) 567-582.

[7] H. Bass, A non-triangulable action of G_a on $\mathbb{A}^3$. *J. Pure Appl. Algebra*, 33(1984),1–5.

[8] H. Bass, F. connel and D. Wright, The Jacobian conjecture: reduction of degree and formal expansion of the inverse, *Bull. Amer. Math. Soc.*, 7(1982),287-330.

[9] T. Becker and S. Weispfenning, *Gröbner Basis, A Computational Approach to Commutative Algebra.* Springer-Verlag, Berlin and New York, 1993.

[10] T. G. Berry, Parametrization of algebraic space curves. *J. Pure Appl. Algebra*, 117(1997),81–95.

[11] J. Berson, A. van den Essen and S. Maubach, Derivations having divergence zero on $R[x, y]$. *Israel J. Math.*, 124(2001),115-124.

[12] J. Berson, J. W. Bikker and A. van den Essen, Adapting coordinates. *J. Pure Appl. Algebra*, 184(2003),165–174.

[13] J. Berson and A. van den Essen, An algorithm to find a coordinate's mate. *J. of Symbolic Computation*, 36(2003),835–843.

[14] J. Berson, *Polynomial coordinates and their behavior in higher dimensions.* PhD thesis, University of Nijmegen, 2004.

[15] S. M. Bhatwadekar and A. K. Dutta, On residual variables and stably polynomial algebras. *Comm. Algebra*, 21(2)(1993),635–645.

[16] S. M. Bhatwadekar and A. K. Dutta, Kernel of locally nilpotent $\mathcal{R}$-derivations of $\mathcal{R}[x, y]$. *Trans. Amer. Math. Soc.*, 349 (8) (1997),3303-3319.

[17] A. Campbell and J-T. Yu, Two dimensional coordinate polynomials and dominant maps. *Comm. Algebra*, 28(5)(2000),2297–2301.

[18] J. Chadzyński and T. Krasiński, On the Lojasiewicz exponent at infinity for polynomial mappings of $\mathbb{C}^2$ into $\mathbb{C}^2$ and components of polynomial automorphisms of $\mathbb{C}^2$. *Ann. Pol. Math. Soc.*, 57(3)(1992),291–302.

[19] C. C. Cheng, J. H. McKay, and S. S-S. Wang, Younger mates and the jacobian conjecture. *Proc. Amer. Math. Soc.*, 123(10)(1995),2939–2947.

[20] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms.* Springer-Verlag, second edition, 1998.

[21] D. Daigle, A necessary and sufficient condition for triangulability of derivations of $k[X, Y, Z]$. *J. Pure Appl. Algebra*, 113(3)(1996),297–305.

[22] D. Daigle, On some properties of locally nilpotent derivations. *J. Pure Appl. Algebra*, 114(3)(1997),221–230.

[23] D. Daigle and G. Freudenburg, Locally nilpotent derivations over a UFD and an application to rank two locally nilpotent derivations of $k[X_1, \cdots, X_n]$. *J. Algebra*, 204(2)(1998),353–371.

[24] D. Daigle and G. Freudenburg, A counterexample to Hilbert's fourteenth problem in dimension five. *J. Algebra*, 221(1999),528–535.

[25] D. Daigle, On locally nilpotent derivations of $\mathcal{K}[x_1, x_2, y]/(\phi(y) - x_1x_2)$. *J. Pure Appl. Algebra*, 181(2003),181-208.

[26] D. Daigle, Locally nilpotent derivations and Danielewski surfaces. *Osaka J. Math.*, 41(2004),37-80.

[27] D. Daigle, Classification of homogeneous locally nilpotent derivations of $\mathcal{K}[x, y, z]$. *Available at http://aix1.uottawa.ca/~ddaigle/*.

[28] D. Daigle and S. Kaliman, A note on locally nilpotent derivations and variables of k[X,Y,Z]. *to appear in Canadian Bull. Math.*

[29] D. Daigle, On polynomials in three variables annihilated by two locally nilpotent derivations. *J. Algebra*, 310(1)(2007),303–324.

[30] H. Derksen, The kernel of derivation. *J. Pure Appl. Algebra*, 84(1993),13–16.

[31] A. Dubouloz, Completions of normal affine surfaces with a trivial Makar-Limanov invariant. *Michigan Math. J.*, 52(2004),289-308.

[32] E. Edo and S. Vénéreau, Lenght 2 variables and transfer. *Ananales Polonici Mathematici*, 76(2001),67–76.

[33] M. El Kahoui, Constants of derivations in polynomial rings over unique factorization domains. *Proc. Amer. Math. Soc* , 132(9)(2004),2537–2541.

[34] M. El Kahoui, D-resultants and subresultants. *Proc. Amer. Math. Soc*, 133(2005),2193–2199.

[35] M. El Kahoui, UFD's with commuting linearly independent locally nilpotent derivations. *J. Algebra*, 289(2005),446–452.

[36] A. van den Essen, A criterion to decide if a polynomial map is invertible and to compute the inverse. *Comm. Algebra*, 18(10)(1990),3183–3186.

[37] A. van den Essen, An algorithm to compute the invariant ring of a G_a-action on an affine variety. *J. Symbolic Computation*, 16(1993),551–555.

[38] A. van den Essen, Locally nilpotent derivations and their applications III. *J. Pure Appl. Algebra*, 98(1995),15–23.

[39] A. van den Essen and J. Janssen, The Kernels of elementary derivations. *Report No 9584, University of Nijmegen, Nijmegen, The Netherlands*, 1995.

[40] A. van den Essen and J-T. Yu, The D-resultant, singularities and the degree of unfaithfulness. *Proc. Amer. Math. Soc*, 125(3)(1997)689-695.

[41] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, *Progr. in Math.,*Vol. 190, Birkhäuser Verlag, Basel, 2000.

[42] A. van den Essen and P. van Rossum, Triangular derivations related to problems on affine n-space, *Proc. Amer. Math. Soc.* 130 (2001), 1311-1322.

[43] A. van den Essen and P. van Rossum, Coordinates in two variables over a $\mathbb{Q}$-algebra. *Trans. Amer. Math. Soc.*, 356(5)(2004)1691–1703.

[44] A. van den Essen and D. Holtackers, On the recognition problem of quasi-homogeneous locally nilpotent derivations in dimension three. *J. Pure Appl. Algebra*, 194(3)(2004)273–279.

[45] A. van den Essen, Three-variable stable coordinates are coordinates. *Report No 0503, University of Nijmegen, Nijmegen, The Netherlands*, 2005.

[46] R. T. Farouki, Pythagorean-hodograph curves. *In Handbook of Comput. Aided Geom. Des.*, (2002) 405–427. North-Holland, Amsterdam.

[47] R. T. Farouki, M. Al Kandari, and T. Sakkalis, Structural invariance of spatial pythagorean hodographs. *Comput. Aided Geom. Des.*, 19(6)(2002),395–407.

[48] R. T. Farouki, C. Y. Han, C. Manni, and A. Sestini, Characterization and construction of helical polynomial space curves. *J. Computational Appl. Math.*, 162(2)(2004),365–392.

[49] D. R. Finston and S. Walcher, Centralizer of locally nilpotent derivations. *J. Pure Appl. algebra*, 120(1)(1997),39–49.

[50] G. Freudenburg, Triangulability criteria for additive group actions on affine space. *J. Pure Appl. Algebra*, 105(1995),267–275.

[51] G. Freudenburg. Actions of G_a on $\mathbb{A}^3$ defined by homogeneous derivations. *J. Pure Appl. Algebra*, 126 (1998)169–181.

[52] G. Freudenburg, Local slice construction in $\mathcal{K}[x, y, z]$. *Osaka J. Math.*, 34(1997),757-767.

[53] G. Freudenburg, A counterexample of Hilbert's fourteenth problem in dimension six. *Transformation Groups*, 5(1)(2000),61–71.

[54] G. Freudenburg, *Algebraic theory of locally nilpotent derivations. Invariant theory and algebraic transformation groups VII.* Encyclopaedia of Mathematical Sciences, vol. 136,(2006).

[55] T. Fujita, On Zariski problem, *Proc. Japan Acad.*, 55A(1979),106-110.

[56] J. van zur Gathen, Functional decomposition of polynomials: the tame case. *J. Symbolic computation*, 9(3)(1990)281–299.

[57] J. Gutierrez, R. Rubio, and J. Schicho. Polynomial parametrization of curves without affine singularities. *Comput. Aided Geom. Des.*, 19(2002),223–234.

[58] A.van Hoeij, Rational parametrizations of algebraic curves using canonial divisor. *J. Symbolic Computation*, 23(1997),209–227.

[59] H. W. E. Jung, Über ganze birational Transformationen der Ebene. *J. Reine Angew. Math.*, 184(1942),161–174.

[60] S. Kaliman, Polynomial with general $\mathbb{C}^2$-fibres are variables. *Pacific J. Math.*, 203(1)(2002),161–190.

[61] S. Kaliman, Free $\mathbb{C}^+$-actions on $\mathbb{C}^3$ are translations. *Invent. Math.*, 156(2004),163-173.

[62] T. Kambayashi, On the absence of nontrivial separable forms of the affine plane. *J. Algebra*, 35(1975),449-456.

[63] O. Keller, Ganze Cremona-Transformationen. *Monatsh, Mat. Phys.*, 47 (1939), 299-306.

[64] H. Kojima and M. Miyanishi, On Roberts' counterexample to the fourteenth problem of Hilbert. *J. Pure Appl. Algebra*, 122(1997),247-268.

[65] H. Kraft, Challenging problems on affine n-space, *Sém. Bourbaki, 17ème annéee* 802 (1994-l995),295-317.

[66] W. van der Kulk, On polynomial rings in two variables. *Nieuw Arch. Wisk.*, 1(3)(1953),33–41.

[67] S. Kuroda, A condition for finite generation of the kernel of a derivation. *J. Algebra*, 262(2)(2003),391–400.

[68] S. Kuroda, A counterexample to the fourteenth problem of Hilbert in dimension four. *J. Algebra*, 279(2004),126–134.

[69] S. Kuroda, Fields defined by locally nilpotent derivations and monomials. *J. Algebra*, 293(2)(2005),395–406.

[70] L. Makar Limanov, Locally nilpotent derivations, a new ring invariant and applications. *Available at* http://www.math.wayne.edu/~lml/.

[71] L. Makar-Limanov, On the hypersurface $x + x^2y + z^2 + t^3 = 0$ in $\mathbb{C}^4$ or a $\mathbb{C}^3$-like threefold which is not $\mathbb{C}^3$, *Israel J. Math.* 96 (1996) 419-429.

[72] L. Makar-Limanov, Locally nilpotent derivation of affine domains. *MPIM Preprint series 2004-92. Available at* www.mpim-bonn.mpg.de.

[73] D. Manocha and J. F. Canny, Rational curves with polynomial parametrization. *Comput. Aided Des.*, 23(9)(1991),645–652.

[74] K. Masuda, Torus actions and kernels of locally nilpotent derivations with slices. *Preprint*,2005, 10 pages.

[75] S. Maubach. An algorithm to compute the kernel of a derivation up to a certain degree. *J. Symbolic Computation*, 29(6)(2000),959–970.

[76] S. Maubach, Triangular monomial derivations on $k[x_1, x_2, x_3, x_4]$ have kernel generated by at most four elements. *J. Pure Appl. Algebra*, 153(2000),165–170.

[77] S. Maubach, The Commuting Derivations Conjecture, J. Pure Appl. Algebra 179 (1-2) (2003), 159-168.

[78] J. H. McKay and S. S-S. Wang, An elementary proof of the automorphism theorem for the polynomial ring in two variables. *J. Pure Appl. Algebra*, 52(1-2)(1988),91–102.

[79] Michiel de Bondt and A. van den Essen The Jacobian Conjecture, Linear triangularization for homogeneous polynomial maps in dimension three, *J. of Algebra* 294, no. 1 (2005), 294-306.

[80] M. Miyanishi and T. Sugie, Affine surfaces containing cylinderlike open sets. *J. Math. Kyoto U.*, 20(1980),11-42.

[81] M. Miyanishi, Normal affine subalgebra of a polynomial ring. *Algebra and Topological Theories–to the memory of Dr. Takehiko MIYATA,Kinokuniya*, (1985), 37–51.

[82] M. Nagata and A. Nowicki, Rings of constants for k-derivations in $k[x_1, \ldots, x_n]$. *J. Math. Kyoto Univ.*, 28(1)(1988),111–118.

[83] A. Nowicki, *Polynomial derivations and their rings of constants.* Uniwersytet Mikolaja Kopernika, Toruń, 1994.

[84] A. Nowicki and J.M. Strelcyn, Generators of rings of constants for some diagonal derivations in polynomial rings. *J. Pure Appl. Algebra*, 101(1995),207–212.

[85] V. L. Popov, On actions of $\mathbf{G}_a$ on $\mathbf{A}^n$. In *Algebraic groups Utrecht 1986*, volume 1271 *Springer, Berlin, Lecture Notes in Math.*, (1987),237–242 .

[86] T. Recio and J. R. Sendra, Real reparametrizations of real curves. *J. Symbolic Computation*, 2-3(23) (1997),241–254.

[87] R. Rentschler, Opérations du groupe additif sur le plan affine. *C. R. Acad. Sci. Paris Ser. A*, 267(1968),384–387.

[88] P. Roberts, An infinitely generated symbolic blow-up in a power series ring and new counterexample to Hilbert's fourtheenth problem. *J. Algebra*, 132(1990),461-473.

[89] K. P. Russell On Affine-Ruled Rational Surfaces, *Math. Annalen* 255 (1981), 287-302.

[90] J. Schicho, On the choice of pencils in the parametrization of curves. *J. Symbolic Computation*, 14(6)(1992),557–576.

[91] J. R. Sendra and F. Winker, Symbolic parametrization of curves. *J. Symbolic Computation*, 12(1991),607–631.

[92] J. R. Sendra and F. Winker, Parametrization of algebraic curves over optimal field extension. *J. Symbolic Computation*, 23(2-3)(1997),191–208.

[93] J. R. Sendra and F. Winker, Tracing index of rational curve parametrizations. *Comput.Aided Geom. Des.*, 18(8)(2001),771–795.

[94] I. P Shestakov and U. U. Umirbaev, The tame and wild automorphisms of polynomial rings in three variables. *J. Amer. Math. Soc.*, 17(1)(2004),197–227.

[95] V. Shpilrain and J-T. Yu, Polynomial automorphisms and Gröbner reductions. *J. Algebra*, 197(1997),546–558.

[96] V. Shpilrain, C.M Lam and J.T Yu, Recognizing and parametrizing curves isomorphic to a line. *J. Symbolic Computation*, 42(7)(2007),751–756.

[97] S. Smale, Mathematical problems for the next century. *Math. Intellingencer*, 20(2)(1998), 7-15.

[98] R. Walter, *Algebraic curves.* Dover Publication, 1949.

[99] D. L. Wright, On the Jacobian Conjecture. *Illinois J. Math*, 25(3)(1981),423–440.

[100] D. Wright, Cancellation of variables of the form $bT^n - a$, *J. Algebra*, 52 (1978) 94-100.

[101] A. Yagzhev, *On Keller's problem.* Siberian Math. J. 21(1980) 747-754.

[102] G. Zariski, Interpretations algebrico-geometriques du quatorziéme problème de Hilbert. *Bull. Sci. Math.*, 78(1954),155-168.

Résumé

Les dérivations localement nilpotentes sur les anneaux des polynômes sont des objets de grande importance dans beaucoup de domaines de mathématiques. Durant la dernière décennie, elles ont connu un véritable progrès et sont devenues un élément essentiel pour la compréhension de la géométrie algébrique affine et d'algèbre commutative. Cette importance est due au fait que certains problèmes classiques dans ces domaines, telles que la conjecture jacobienne, le problème d'élimination, le problème de plongement et le problème de linéarisation, ont été reformulés dans la théorie des dérivations localement nilpotentes. Cette thèse porte sur l'étude algorithmique des problèmes liés aux dérivations localement nilpotentes et leurs applications aux automorphismes polynomiaux de l'espace affine. Elle a pour objectif de présenter, d'une part, quelques problèmes dans lesquels les dérivations localement nilpotentes jouent un rôle crucial, à savoir le problème des coordonnées et le problème de paramétrisation polynomial des courbes algébriques dans l'espace affine. Et d'autre part, de donner quelques algorithmes qui peuvent contribuer à la compréhension des dérivations localement nilpotente en dimension trois, à savoir les algorithmes du rang et de triangulabilité des dérivations localement nilpotentes

Summary

Derivations, especially locally nilpotent ones, over polynomial rings are objects of great importance in many fields of pure and applied mathematics. Nowadays, locally nilpotent derivations have made remarkable progress and became an important topic in understanding affine algebraic geometry and commutative algebra. This is due to the fact that some classic problems in these areas, such as the Jacobian conjecture, the Linearization problem and the Cancellation problem, can be reformulated in terms of locally nilpotent derivations. This thesis is about the algorithmic study of problems linked to locally nilpotent derivations and their applications to the study of polynomial automorphisms of the affine space. Its aim is to present, on one hand, some problems in which locally nilpotent derivations play a crucial role, namely, the coordinate problem and the parametrization problem. On the other hand, give some algorithms concerning locally nilpotent derivations, which may contribute in understanding locally nilpotent derivations in three dimensional case, namely, rang and triangulability algorithms of locally nilpotent derivations.