Contribution à l'algorithmique en algèbre différentielle

François Lemaire



Contribution à l'algorithmique en algèbre différentielle

THÈSE

présentée et soutenue publiquement le 22 Janvier 2002

pour l'obtention du

Doctorat de l'Université des Sciences et Technologies de Lille

(spécialité informatique)

par

François Lemaire

Composition du jury

Président :	Sophie TISON	LIFL, Université de Lille 1
Rapporteurs :	Daniel LAZARD	LIP6, Université de Paris 6
	Greg REID	ORCCA, University of Western Ontario, London
Examinateurs :	François BOULIER	LIFL, Université de Lille 1
	Anne DUVAL	AGAT, Université de Lille 1
Directeur :	Gérard JACOB	LIFL, Université de Lille 1

UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE
Laboratoire d'Informatique Fondamentale de Lille — UPRESA 8022
U.F.R. d'I.E.E.A. – Bât. M3 – 59655 VILLENEUVE D'ASCQ CEDEX
Tél. : +33 (0)3 20 43 47 24 – Télécopie : +33 (0)3 20 43 65 66 – email : direction@lifl.fr

Mis en page et composé avec LaTeX et la classe thlifl. Version du 14 mars 2002.

Remerciements

Lors de mon arrivée dans l'équipe de Calcul Formel, je me réjouissais à l'idée de me consacrer pleinement à des disciplines que j'affectionne depuis toujours, à savoir l'informatique et les mathématiques. Quatre ans plus tard, je suis heureux d'avoir concrétisé mon travail par l'écriture de ce manuscrit, qui a mobilisé toute mon énergie et toute ma volonté.

Mes premiers remerciements vont à Gérard Jacob pour m'avoir accueilli dans son équipe et accordé une grande liberté dans mon travail.

Je remercie grandement François Boulier qui m'a proposé mon sujet et m'a encadré durant quatre ans. C'est grâce à ses nombreuses explications et à tout le temps qu'il m'a consacré que j'ai pu mener à bien cette thèse.

Je remercie Daniel Lazard (LIP6, université de Paris VI) et Greg Reid (ORCCA, university of Western Ontario, Canada) d'avoir accepté d'être rapporteurs. Merci à Daniel Lazard pour la rigueur avec laquelle il a relu mon manuscrit et merci à Greg Reid d'avoir relu mon texte rédigé en français.

Je remercie Anne Duval (AGAT, université de Lille I) et Sophie Tison (LIFL, université de Lille I) de m'avoir fait l'honneur de participer à ce jury.

Je remercie également les autres membres de l'équipe. Marc Moreno Maza pour m'avoir souvent aidé sur les systèmes triangulaires et pour avoir organisé de nombreux pots (particulièrement bienvenus) au sein de l'équipe. Michel Petitot pour ses nombreuses discussions scientifiques aussi éclairantes et qu'intéressantes. Hoang Minh pour son dynamisme et sa bonne humeur. Nour-Eddine pour sa sérénité et ses conseils avisés. Enfin, mes deux homologues Michael Bigotte (docteur) et Sylvain Neut (futur docteur) avec qui j'ai pu partager mes impressions de doctorant.

Je remercie vivement ma famille et mes amis pour tous les moments inoubliables passés avec eux.

Introduction

Les équations différentielles se retrouvent dans des domaines aussi variés que la mécanique du solide, la mécanique des fluides, la biologie, la chimie... Lors de ma formation d'ingénieur à l'École Centrale de Lille, j'ai souvent rencontré de tels systèmes qui se traitent généralement en deux étapes. La première consiste à transformer le système pour le mettre sous une forme praticable, commode à utiliser. La seconde est la résolution même du système. Dans certains cas, on peut directement (à l'aide de méthodes classiques) déterminer la forme générale de ses solutions. Le plus souvent, on est amené soit à simplifier le système (en négligeant certains termes), soit à recourir à des techniques numériques.

Cette thèse propose des techniques de calcul formel qui visent à systématiser la première étape. Nous donnons aussi des résultats d'analyse qui relèvent de la seconde.

Nous nous intéressons aux systèmes d'équations non linéaires différentielles polynomiales dont voici un exemple :

$$\Sigma \left\{ \begin{array}{r} u_x^2 - 4u = 0 \\ u_{xy} v_y - u + 1 = 0 \\ v_{xx} - u_x = 0 \end{array} \right.$$

où u et v sont deux fonctions des variables x et y et où les dérivations sont notées en indices (par exemple u_x désigne $\frac{\partial u}{\partial x}$).

Par de simples manipulations syntaxiques (algébriques) sur le système Σ, et sans utiliser de raisonnements d'analyse, on peut obtenir des renseignements sur les solutions de Σ. C'est sur cette idée qu'est fondée l'algèbre différentielle initiée par Ritt [52] et Kolchin [28].

Une question–clé est de connaître toutes les équations qui se déduisent de Σ. Par exemple, l'équation $u_x^2 - 4u = 0$ implique, en dérivant par x, que $2u_x\, u_{xx} - 4u_x = 0$. D'autres équations sont plus difficiles à déceler comme l'équation $u_y^2 - 2u = 0$. En effet, cette «relation cachée» ne se lit pas directement sur Σ.

L'ensemble des équations conséquences de Σ forme ce qu'on appelle un idéal différentiel. Cet ensemble étant infini, il est essentiel de le représenter par un ensemble (fini) d'équations, qui soit commode à utiliser, c'est-à-dire ne contenant plus de «relations cachées».

Déterminer un tel ensemble revient à faire de l'élimination dans les idéaux différentiels. Ce problème est résolu pour les systèmes de polynômes ordinaires (i.e. sans dérivations) par les bases de Gröbner ou par les ensembles caractéristiques. En algèbre différentielle, nous disposons essentiellement des ensembles caractéristiques. Il existe un algorithme, appelé Rosenfeld–Gröbner, qui permet de calculer de tels systèmes. Cet algorithme a été

développé par François Boulier et constitue le cœur du paquetage `diffalg` disponible dans le logiciel `Maple`.

Les ensembles caractéristiques fournissent aussi un outil (basé sur des manipulations algébriques) pour calculer des solutions formelles. Ces solutions peuvent être vues comme des développements de Taylor infinis dont on ne sait pas s'ils convergent. Par exemple, l'équation $x^2 u_x = u - x$ admet la solution formelle $u(x) = \sum_{n=0}^{\infty} n! x^{n+1}$ qui diverge pour toute valeur non nulle de x. Lorsque la solution en série formelle est convergente, on dit qu'elle est analytique. La solution formelle fournit alors une solution au sens habituel du terme. Le problème de l'analycité est un problème d'analyse qui ne relève pas directement du calcul formel.

Cette thèse contient cinq résultats :

- la définition de la forme normale d'un polynôme modulo un idéal différentiel présenté par un ensemble caractéristique, et un algorithme permettant de la calculer ;
- l'algorithme regCaractéristique qui fournit une optimisation de Rosenfeld–Gröbner ;
- l'algorithme Pardi de calcul d'ensembles caractéristiques plus orienté vers la résolution de problèmes réels que Rosenfeld–Gröbner ;
- un contre-exemple à une conjecture portant sur l'analycité de solutions formelles ;
- une nouvelle preuve d'un théorème d'analycité des solutions formelles des ensembles caractéristiques.

Le premier résultat (paru dans [10]) est une méthode pour calculer la forme normale d'un polynôme modulo un idéal présenté par un ensemble caractéristique.

Les formes normales sont un outil permettant de calculer dans une algèbre présentée par générateurs (sur l'exemple les fonctions u et v) et relations (les équations de Σ). Deux expressions sont égales modulo les relations *si et seulement si* elles ont même forme normale.

Considérons par exemple les deux quantités $q_1 = u_x$ et $q_2 = 4u/u_x$. Ces deux quantités sont égales modulo les relations de Σ ; en effet, $q_1 - q_2 = u_x - (4u/u_x) = (u_x^2 - 4\,u)/u_x$ qui vaut zéro car $u_x^2 - 4\,u = 0$ est une relation de Σ. L'utilisation des formes normales (notées NF) montre que $\mathrm{NF}(q_1) = u_x = \mathrm{NF}(q_2)$.

Ainsi, pour vérifier que deux quantités sont égales modulo un idéal différentiel présenté par un ensemble caractéristique, on peut comparer leurs formes normales et nous sommes donc ramenés à une égalité syntaxique (le seul test dont on dispose en informatique).

Une propriété intéressante de ces formes normales est qu'elles forment un espace vectoriel. Une conséquence immédiate de cela est que l'on peut, par exemple, tester la dépendance linéaire de trois (ou plus) polynômes p_1, p_2 et p_3 modulo les relations de Σ en testant (sans tenir compte des relations de Σ) la dépendance linéaire de $\mathrm{NF}(p_1)$, $\mathrm{NF}(p_2)$ et $\mathrm{NF}(p_3)$. Si une telle dépendance existe, on connaît alors ses coefficients.

C'est sur cette idée que repose l'algorithme FGLM [22] de Faugère, Gianni, Lazard et Mora, qui calcule une base de Gröbner d'un idéal, pour un certain ordre, à partir d'une base de Gröbner (du même idéal) pour un autre ordre.

François Boulier a développé l'algorithme dFGLM [6] qui est l'analogue de FGLM pour le cas différentiel. Cet algorithme utilise les formes normales introduites dans cette thèse.

Le second résultat (paru dans [10]) est l'algorithme regCaractéristique *qui optimise la dernière étape de calcul de* Rosenfeld–Gröbner.

Lors de cette étape, Rosenfeld–Gröbner transforme, par un calcul de bases de Gröbner, un système d'équations A et d'inéquations S en ensembles caractéristiques. regCaractéristique effectue le même traitement en manipulant des ensembles triangulaires.

Les bases de Gröbner sont inadaptées pour les raisons suivantes. D'une part, elles ne tiennent pas compte de la structure triangulaire du système A, d'autre part, les inverses des inéquations sont explicitement calculés. Ces inverses explicites, dont le calcul peut être coûteux, sont inutiles car seule leur existence importe.

L'algorithme regCaractéristique utilise des techniques présentées dans [41] et s'inspire de l'algorithme lexTriangular [32], qui convertit une base de Gröbner en ensembles caractéristiques. Il nous a fallu adapter lexTriangular à nos besoins pour qu'il traite des systèmes d'équations et d'inéquations.

Pour l'implantation, nous nous sommes basés sur les travaux de l'équipe de Daniel Lazard, qui a développé depuis les années 1990 des méthodes manipulant des *systèmes triangulaires*. Ces méthodes sont particulièrement efficaces aussi bien en temps de calcul qu'en ce qui concerne la maîtrise du grossissement des données. On peut en particulier citer les algorithmes de Aubry [1] et de Moreno Maza [40] qui, tous deux, décomposent un système algébrique en systèmes triangulaires.

Le troisième résultat (paru dans [9]) est l'algorithme Pardi *qui est une reprise de l'algorithme* Rosenfeld–Gröbner *sous une forme moins générale, mais qui a l'avantage d'être plus adapté aux problèmes réels.*

L'algorithme Pardi nécessite des hypothèses de départ plus restrictives que Rosenfeld–Gröbner car il prend en entrée un ensemble caractéristique d'un idéal «premier» pour un certain classement (ordre sur les dérivées). L'algorithme calcule alors un nouvel ensemble caractéristique de l'idéal pour un classement différent.

Les hypothèses exigées par Pardi sont, dans la pratique, réalistes. En effet, la plupart des systèmes différentiels provenant de problèmes réels engendrent des idéaux premiers. Supposer que l'on dispose d'un ensemble caractéristique est également une hypothèse réaliste. En effet, dans le cas différentiel, il arrive souvent (par exemple pour les systèmes dynamiques en automatique non linéaire) que les équations du système initial constituent déjà un ensemble caractéristique.

Se restreindre au cas des idéaux premiers permet de décider si un polynôme est inversible (dans l'algèbre quotientée par l'idéal premier) en testant qu'il est non nul. Cette propriété permet, lors du traitement des inéquations, d'économiser des calculs parfois coûteux et d'éviter un mécanisme de type «backtracking». Lorsque des sous–problèmes algébriques sont rencontrés dans les calculs différentiels, ils sont traités par une méthode purement algébrique. Cela améliore le contrôle de la taille des coefficients et évite de nombreux calculs provenant de considérations différentielles. Cet avantage très important, par rapport à d'autres méthodes, nous a permis de traiter des problèmes jusque ici non résolus.

Des méthodes de décomposition d'idéaux quelconques (premiers ou non) en ensembles triangulaires ont aussi été formulées en termes de pgcd [26, 31, 40]. L'utilisation de ces pgcd est toutefois plus compliquée que dans Pardi. En effet, dans ces méthodes, l'idéal

modulo lequel sont calculés les pgcd évolue durant le calcul car il dépend des équations déjà calculées. Ce n'est pas le cas dans notre contexte.

L'algorithme Pardi et ses variantes Podi (pour les systèmes à une seule dérivation) et Palgie (pour les systèmes algébriques) ont été implantées : Pardi en `Maple` et en `C`, Podi en `C` et Palgie en `Maple`, `C` et `Aldor`.

Un dernier intérêt de cet algorithme est sa simplicité conceptuelle. Chacun sait que les racines communes de deux polynômes univariés sur un corps sont données par leur pgcd. Notre algorithme utilise cette propriété en remplaçant (lorsque le cas se présente) deux polynômes de même variable principale par leur pgcd au dessus du corps de fraction d'un certain anneau quotient.

Avant de présenter les deux résultats d'analycité, nous commençons par traiter l'équation de la chaleur :

$$u_{xx}(x,t) = u_t(x,t) \qquad (1)$$

où $u(x,t)$ désigne la température d'une barre à l'abscisse x et au temps t.

La forme générale de la solution formelle $u(x,t)$ est :

$$u(x,t) = u(0,0) + u_x(0,0)x + u_t(0,0)t + u_{xx}(0,0)\frac{x^2}{2} + \cdots$$

Il y a deux façons de reporter l'équation (1) dans la solution formelle : la première consiste à appliquer la règle $u_{xx} \to u_t$. Par exemple on remplace le terme $u_{xxxx}(0,0)$ par $u_{tt}(0,0)$. Une autre méthode consiste à appliquer la règle inverse, à savoir $u_t \to u_{xx}$.

Dans le premier cas, la solution $u(x,t)$ dépend uniquement des valeurs de $u_{t^p}(0,0)$ et $u_{xt^p}(0,0)$ pour p entier quelconque. Ces valeurs sont déterminées si on fixe les deux fonctions $u(0,t)$ et $u_x(0,t)$. Ces deux fonctions constituent ce qu'on appelle des conditions initiales. Dans le deuxième cas, la solution $u(x,t)$ dépend des valeurs de $u_{x^p}(0,0)$ pour p entier quelconque et ces valeurs sont déterminées si l'on fixe la fonction $u(x,0)$.

La première méthode est «meilleure» que la seconde car les variables les plus dérivées sont exprimées en fonction des variables les moins dérivées et le théorème de Cauchy–Kovalevskaya s'applique : si $u(0,t)$ et $u_x(0,t)$ sont des fonctions analytiques, la solution formelle $u(x,t)$ est elle aussi analytique.

Dans le second cas, le théorème de Cauchy–Kovalevskaya ne s'applique pas : si $u(x,0)$ est analytique, la solution formelle $u(x,t)$ n'est pas nécessairement analytique (prendre par exemple $u(x,0) = 1/(1-x)$).

Historiquement, c'est cet exemple que Sophie Kovalevskaya a utilisé au XIX$^{\text{e}}$ siècle pour montrer l'importance d'exprimer les variables les plus dérivées en fonction des variables les moins dérivées.

En s'appuyant sur cette idée–clé, on est naturellement amené à proposer la conjecture suivante :

> si C est un ensemble caractéristique pour un classement de l'ordre total (ce qui est la manière technique d'imposer que les variables les plus dérivées sont exprimées en fonction des moins dérivées) et si les conditions initiales sont données par des fonctions analytiques, alors la solution formelle est analytique.

Cette conjecture était admise comme résultat par notre équipe [11] et aussi par d'autres chercheurs. Une variante de cette conjecture était même énoncée comme vraie dans [55, théorème 7.2.1, p108].

Le quatrième résultat est le contre-exemple suivant à cette conjecture :

$$\begin{cases} u_{xx} &= u_{xy} + u_{yy} + v \\ v_{yy} &= v_{xy} + v_{xx} + u \end{cases}$$
$$u(0,y) = u_x(0,y) = e^y \text{ et } v(x,0) = v_y(x,0) = e^x$$

En effet, nous montrons que ce système admet une solution formelle *non analytique* alors que les conditions initiales (e^x et e^y) sont analytiques et que les variables les plus dérivées sont exprimées en fonction des variables les moins dérivées.

La conjecture précédente devient vraie si le classement vérifie une condition technique supplémentaire : il s'agit du théorème d'analycité démontré dans [45, page 34].

Une nouvelle preuve de ce théorème (voir th. 17, page 75) constitue le dernier résultat.

La preuve [45, page 34] s'appuie sur le théorème d'analycité de Riquier [51]. Le théorème 17 s'appuie sur le théorème 16 (page 69), qui fournit une nouvelle preuve du théorème d'analycité de Riquier. Un atout de cette preuve est qu'elle utilise un formalisme récent, ce qui en facilite la compréhension. Cela est d'autant plus appréciable que la preuve de Riquier est, selon les spécialistes, fort technique.

Tous les résultats obtenus dans cette thèse vont me permettre de faire évoluer le paquetage `diffalg`. Je pourrai y intégrer les algorithmes regCaractéristique et Pardi et aussi y ajouter de nouvelles fonctionnalités. Parmi elles, on peut citer le calcul de formes normales, ainsi qu'un critère d'analycité des solutions basé sur le théorème 17. J'espère également y intégrer une fonction d'estimation du domaine de convergence des solutions analytiques pour permettre une éventuelle simulation numérique. J'aurai l'occasion de réaliser ce travail lors de mon post-doctorat dans l'équipe ORCCA (University of Western Ontario, London, Canada), dans le cadre d'une collaboration entre l'équipe de Calcul Formel de Lille et Greg Reid, membre de l'équipe ORCCA. Nous espérons que cette collaboration entre spécialistes de l'algèbre différentielle et de la géométrie différentielle sera fructueuse.

Le premier chapitre présente des résultats d'algèbre utilisés tout au long de cette thèse. On y décrit les chaînes régulières, ainsi que des fonctions élémentaires permettant de les manipuler.

Le second chapitre présente l'algèbre différentielle de Ritt et Kolchin et notamment les ensembles caractéristiques. On y trouve trois résultats nouveaux : le calcul de formes normales, l'introduction de la notion de *chaîne différentielle régulière* et la clarification de la définition de *présentation caractéristique* donnée dans [8].

Le troisième chapitre traite de l'analycité des solutions formelles. On y retrouve le contre-exemple avec une preuve de la non analycité de sa solution, ainsi que la preuve du théorème 17.

Les quatrième et cinquième chapitres présentent respectivement les algorithmes regCaractéristique et Pardi.

Table des matières

Chapitre 1

Algèbre commutative

Sommaire

Ce chapitre rappelle les outils et les opérations nécessaires pour traiter les problèmes algébriques rencontrés dans cette thèse. Les résultats de ce chapitre sont connus et essentiellement tirés de [2], [7], [8], [31] et [43]. Ce chapitre présente, en particulier, la notion de chaîne régulière ainsi que des théorèmes d'algèbre assez techniques. L'objectif est d'amener les notions et les théorèmes de manière naturelle ; nous cherchons plus à montrer l'utilité de ces notions qu'à en donner des preuves techniques.

Le chapitre débute par le problème suivant : étant donné un système A de polynômes, trouver un algorithme effectif permettant de tester l'appartenance d'un polynôme à l'idéal engendré par le système A.

Ce problème est résolu en calculant une base de Gröbner de l'idéal (A). Une autre approche (adoptée tout au long de cette thèse) consiste à utiliser les algorithmes de réduction de Ritt. Nous verrons comment la réduction de Ritt conduit à la notion de chaîne régulière (notion définie indépendamment par Kalkbrener dans [25] et par Yang et Zhang dans [66]). D'après [2], une chaîne régulière C est un ensemble de polynômes particulier qui fournit un test d'appartenance à l'idéal I «associé à C[1]», i.e. :

$$p \text{ appartient à } I \textit{ ssi } p \text{ est réduit à 0 par } C$$

Après avoir rappelé le lien entre les chaînes régulières et les ensembles caractéristiques de Ritt (théorème 6.1 de [2]), nous étudierons les propriétés des idéaux qui leur sont associées. Nous verrons en quoi ces propriétés sont utiles d'un point de vue pratique.

De nombreux algorithmes manipulent ces chaînes régulières (on peut citer l'algorithme Decompose de Marc Moreno Maza [40] qui transforme un système de polynômes en une ou plusieurs chaînes régulières). Ces algorithmes sont assez ardus et techniques. Toutefois, dans cette thèse, nous utiliserons surtout deux fonctions conceptuellement simples : inverse et Bézout. Ces dernières calculent respectivement l'inverse d'un polynôme et une identité de Bézout modulo l'idéal associé à une chaîne régulière. L'étude de ces deux fonctions et des considérations informatiques concluent ce chapitre.

1.1 Polynômes et réduction de Ritt

Dans tout ce chapitre, R désigne l'anneau de polynômes $K[X]$ où K est un corps et X est un alphabet (éventuellement infini) ordonné.

Soit A un ensemble de polynômes.

Idéal engendré par une partie de R Si $A \subset R$, on note (A) le plus petit idéal de R contenant A, c'est–à–dire l'intersection de tous les idéaux contenant A.

Idéal Un idéal $\mathfrak{a}$ d'un anneau R est un sous–ensemble non vide de R vérifiant :

$$\begin{aligned} a, b \in \mathfrak{a} &\Rightarrow a + b \in \mathfrak{a} \\ a \in \mathfrak{a} \text{ et } b \in R &\Rightarrow a\,b \in \mathfrak{a} \end{aligned}$$

1. il s'agit de l'idéal $(C) : {I_C}^{\infty}$

Connaissant le système A, on cherche à tester l'appartenance d'un polynôme à l'idéal (A). Ce problème est résolu en calculant une base de Gröbner de l'idéal (A). Une autre méthode consiste à utiliser l'algorithme de réduction de Ritt (présenté plus loin) qui va permettre d'introduire la notion de chaîne régulière.

Soient p un polynôme non nul de R et x une indéterminée de X. Le polynôme p peut être vu comme un polynôme univarié en x à coefficients dans un anneau de polynômes et peut donc s'écrire

$$p = a_d\, x^d + \cdots + a_1\, x + a_0$$

où les polynômes a_i ne comportent pas l'indéterminée x et $a_d \neq 0$.

L'entier d est le degré de p en x et on le note $\deg(p,x)$. Le polynôme a_d est le coefficient principal de p en x et on le note $\mathrm{coeff\_principal}(p,x)$. Si p est le polynôme nul, on convient que $\deg(p,x) = -\infty$ pour toute indéterminée x ; le coefficient principal du polynôme nul n'est pas défini.

L'indéterminée principale (*leader* en Anglais) de p est la plus grande indéterminée $x \in X$ qui figure dans p. Nous la notons $\mathrm{ld}\, p$. Si x est l'indéterminée principale de p, on appelle rang de p, noté $\mathrm{rang}\, p$, le monôme x^d. On ordonne deux rangs x^d et y^e de la manière suivante : $x^d < y^e$ si $x < y$ ou $(x = y$ et $d < e)$.

le polynôme a_d est l'*initial* de p, noté i_p. Le *séparant* de p est le polynôme

$$s_p = \frac{\partial p}{\partial x} = d\, a_d\, x^{d-1} + \cdots + a_1.$$

Si $A \subset R \setminus K$ alors le rang de A est l'ensemble des rangs de ses éléments. On note $\mathrm{ld}\, A$ l'ensemble des indéterminées principales des éléments de A. On note I_A (resp. S_A) l'ensemble des initiaux (resp. des séparants) des éléments de A. On note $H_A = I_A \cup S_A$.

Pseudo-division Soient $f = f_m\, x^m + \cdots + f_1\, x + f_0$ et $g = g_n\, x^n + \cdots + g_1\, x + g_0$ deux polynômes de R vus comme des polynômes univariés en la variable x, avec $g \neq 0$. Il existe un unique couple (q, r) de polynômes de R vérifiant :

$$\begin{aligned} g_n^{m-n+1}\, f &= g\, q + r, \\ \deg(r,x) &< \deg(g,x). \end{aligned}$$

Le polynôme q (resp. r) est le pseudo–quotient (resp. pseudo–reste) de la pseudo–division de f par g. L'algorithme de pseudo–réduction est présenté dans [27, vol. 2, page 407]. On note $q = \mathsf{pquo}(f, g, x)$ et $r = \mathsf{prem}(f, g, x)$. Si l'indéterminée x n'est pas mentionnée, on suppose $x = \mathrm{ld}\, g$.

Polynôme algébriquement réduit Soient $p \in R \setminus K$ et $q \in R$ deux polynômes. Notons $\mathrm{rang}\, p = x^d$. Le polynôme q est dit *algébriquement réduit* par rapport à p si $\deg(q,x) < d$. Si $A \subset R \setminus K$, on dit que q est algébriquement réduit par rapport à A si q est algébriquement réduit par rapport à tous les polynômes de A.

Algorithme de réduction algébrique d'un polynôme par un ensemble Soient un polynôme $p \in R$ et un ensemble fini $A \subset R \setminus K$. Réduire p par A consiste à déterminer (en pseudo–divisant tant que cela est possible p par les éléments de A) deux polynômes r et h vérifiant :

1. r est algébriquement réduit par rapport à A ;
2. h est un produit d'initiaux de A ;
3. $h\,p = r \mod (A)$.

Les polynômes r et h dépendent de l'ordre dans lequel on opère les pseudo–divisions. Cette indétermination est levée dans les implantations. Le polynôme r est noté $\mathsf{prem}(p,A)$.

Saturation d'un idéal Soit $S = \{s_1, \ldots, s_t\}$ une famille finie d'éléments de R, on note $\mathfrak{a} : S^\infty$ la *saturation* de $\mathfrak{a}$ par S c'est–à–dire l'idéal

$$\mathfrak{a} : S^\infty = \{a \in R \mid \exists (e_1, \ldots, e_t) \in \mathbb{N}^t \text{ tel que } s_1^{e_1} \cdots s_t^{e_t} a \in \mathfrak{a}\}.$$

On a l'inclusion $\mathfrak{a} \subset \mathfrak{a} : S^\infty$.

Propriété 1 (Réduction par un ensemble) *Soit p un polynôme et un ensemble fini $A \subset R \setminus K$. On a :*

$$\mathsf{prem}(p,A) = 0 \implies p \in (A) : {I_A}^\infty$$

Pour obtenir un test d'appartenance, il nous reste à l'obtenir l'implication inverse qui est fausse pour un ensemble A quelconque. Voici un exemple illustrant le problème.

Exemple ▷

$$A \begin{cases} p_1 = x(y-1) \\ p_2 = x(x-1) \end{cases} \qquad y > x$$

L'idéal $I = (A) : {I_A}^\infty$ est l'idéal $(x-1, y-1)$ à cause de la saturation par l'initial x de p_1. Le polynôme $x-1$ appartient à l'idéal I mais $\mathsf{prem}(x-1,A) = x-1$. ◁

Dans l'exemple précédent, l'implication $p \in (A) : {I_A}^\infty \implies \mathsf{prem}(p,A) = 0$ pour tout p est fausse car l'initial x de p_1 est diviseur de zéro modulo l'idéal (p_2). Nous verrons dans la prochaine section des ensembles particuliers (appelés chaînes régulières) qui interdisent de tels diviseurs de zéro.

Diviseur de zéro On dit qu'un élément non nul p d'un anneau A est diviseur de zéro dans A si il existe q non nul dans A tel que $p\,q = 0$

Diviseur de zéro modulo un idéal On dit qu'un élément p d'un anneau A est diviseur de zéro modulo un idéal $\mathfrak{a}$ si p est diviseur de zéro dans l'anneau quotient $A/\mathfrak{a}$.

Élément régulier (modulo un idéal) Un élément p d'un anneau A est dit régulier (resp. modulo un idéal $\mathfrak{a}$) si p est non diviseur de zéro (resp. modulo $\mathfrak{a}$).

1.2 Chaînes régulières et ensembles caractéristiques de Ritt

Le concept de chaîne régulière a été introduit indépendamment dans [66] et [25]. On peut formuler plusieurs définitions équivalentes des chaînes régulières. La définition donnée ici s'appuie sur les diviseurs de zéro.

Ensemble triangulaire Soit un ensemble $T \subset R \setminus K$. L'ensemble T est dit *triangulaire* si les éléments de T ont deux–à–deux des indéterminées principales distinctes.

Chaîne régulière Soit $C = \{p_1, \ldots, p_n\}$ un ensemble triangulaire avec $\mathrm{ld}\, p_1 < \cdots < \mathrm{ld}\, p_n$. On dit que C est une chaîne régulière (de $K[X]$) si pour $1 \leq k < n$, $i_{p_{k+1}}$ ne divise pas zéro modulo l'idéal $(p_1, \ldots, p_k) : \{i_{p_1}, \ldots, i_{p_k}\}^\infty$

Si C est une chaîne régulière, on obtient le test d'appartenance recherché, à savoir:

$$p \in (C) : {I_C}^\infty \iff \mathsf{prem}(p, C) = 0$$

La notion de chaîne régulière est proche de celle des ensembles caractéristiques de Ritt dans le cas algébrique.

Ensemble algébriquement autoréduit L'ensemble $A \subset R \setminus K$ est dit algébriquement autoréduit si chaque polynôme p de A est algébriquement réduit par rapport à $A \setminus \{p\}$.

Nécessairement, un ensemble A algébriquement autoréduit est triangulaire.

Ensemble caractéristique Soit $A \subset R$. On suppose de plus que A ne contient pas de constantes non nulles. On dit qu'un sous–ensemble C de A est un ensemble caractéristique de A si C est algébriquement autoréduit et si A ne contient aucun élément non nul réduit par rapport à C.

Propriété 2 (Réduction par un ensemble caractéristique) *Soit C un ensemble caractéristique d'un idéal I. On a $p \in I \implies \mathsf{prem}(p, C) = 0$.*

Preuve :
Soit p un élément de I. Le polynôme $r = \mathsf{prem}(p, C)$ appartient aussi à I. Il est réduit par rapport à C et vaut donc 0 car C est un ensemble caractéristique de I. □

L'implication inverse (à savoir $\mathsf{prem}(p, C) = 0 \implies p \in I$) est en général fausse comme le montre l'exemple suivant :

Exemple ▷

$$C \left\{ \begin{array}{ll} x(y-1) = 0 & \\ y > x & \end{array} \right.$$

L'ensemble C est un ensemble caractéristique de l'idéal $I = (x(y-1))$. En effet, C est algébriquement autoréduit et inclus dans I, et tout élément de I (nécessairement de la forme $x(y-1)q$ où q est un polynôme quelconque) n'est pas réduit par rapport à C. Toutefois, $\mathsf{prem}(y-1, C) = 0$ alors que $y - 1 \notin I$. ◁

Si on suppose $I = (C) : {I_C}^\infty$, on a : $p \in I \iff \mathsf{prem}(p,C) = 0$, propriété équivalente à celle des chaînes régulières. Une chaîne régulière C et un ensemble caractéristique C de l'idéal $(C) : {I_C}^\infty$ sont deux notions équivalentes à ceci près qu'une chaîne régulière n'est pas a priori algébriquement autoréduite. En tenant compte de cette remarque, voici le théorème 6.1 de [2] reformulé en deux théorèmes[2] :

Théorème 1 *Soit C un ensemble triangulaire de $K[X]$. Les deux propriétés suivantes sont équivalentes :*

- *C est une chaîne régulière ;*
- *$p \in (C) : {I_C}^\infty \iff \mathsf{prem}(p,C) = 0$.*

Théorème 2 *Si C est une chaîne régulière (pas nécessairement algébriquement autoréduite), C a même rang que tout ensemble caractéristique[3] de $(C) : {I_C}^\infty$. Si C est un ensemble triangulaire, les deux conditions suivantes sont équivalentes :*

- *C est une chaîne régulière algébriquement autoréduite ;*
- *C est un ensemble caractéristique. de l'idéal $(C) : {I_C}^\infty$*

1.3 Propriétés des idéaux $(A) : {I_A}^\infty$ et $(A) : {S_A}^\infty$

Soit A un ensemble triangulaire. Les idéaux $(A):{I_A}^\infty$ et $(A):{S_A}^\infty$ disposent de propriétés intéressantes. Nous verrons que ces propriétés permettent de manipuler "facilement" les chaînes régulières de manière algorithmique.

Avant de formuler ces deux lemmes, nous présentons d'abord les idéaux radiciels, primaires et premiers ainsi que les théorèmes de Lasker-Nœther et Macaulay.

Idéal radiciel L'idéal $\mathfrak{a}$ est dit *radiciel* si pour tout a de R et pour tout entier positif n, $a^n \in \mathfrak{a}$ implique $a \in \mathfrak{a}$.

Radical d'un idéal Le radical d'un idéal $\mathfrak{a}$, noté $\sqrt{\mathfrak{a}}$, est l'ensemble des éléments de R dont une puissance est dans $\mathfrak{a}$. On montre que $\sqrt{\mathfrak{a}}$ est le plus petit idéal radiciel contenant $\mathfrak{a}$.

Idéal primaire L'idéal $\mathfrak{a}$ est dit *primaire* si $a\,b \in \mathfrak{a}$ et $a \notin \mathfrak{a}$ implique qu'il existe un entier n tel que $b^n \in \mathfrak{a}$.

Idéal premier L'idéal $\mathfrak{a}$ est dit *premier* si $a\,b \in \mathfrak{a}$ implique $a \in \mathfrak{a}$ ou $b \in \mathfrak{a}$.

Propriété 3 *Si $\mathfrak{a}$ est un idéal primaire, alors $\sqrt{\mathfrak{a}}$ est un idéal premier.*

2. l'article [2] introduit des ensembles caractéristiques différents de ceux présentés dans cette thèse. Ces ensembles caractéristiques ne sont pas supposés autoréduits

3. tous les ensembles caractéristiques d'un même ensemble ont même rang

Dans le cas où l'anneau R est nœtherien, on peut décomposer un idéal $\mathfrak{a}$ en une intersection d'idéaux primaires et l'idéal radiciel $\sqrt{\mathfrak{a}}$ en une intersection d'idéaux premiers.

Théorème 3 (Théorème de Lasker–Nœther) *Dans un anneau nœthérien, tout idéal est une intersection finie d'idéaux primaires*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t.$$

Toute décomposition de $\mathfrak{a}$ peut être rendue minimale en supprimant d'une part les idéaux primaires redondants (i.e. les $\mathfrak{q}_i$ inclus dans un $\mathfrak{q}_j$ où $i \neq j$) et en regroupant d'autre part les idéaux primaires dont l'intersection est elle–même un idéal primaire.

Il n'y a pas unicité de la décomposition minimale d'un idéal. Toutefois, le nombre de composantes et les radicaux des composantes primaires (appelés idéaux premiers « associés » à l'idéal) le sont : ce sont des invariants de l'idéal $\mathfrak{a}$.

Voici deux décompositions primaires minimales d'un même idéal. L'exemple est extrait de [21, page 105].

$$\mathfrak{a} = (x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x^2, xy, y^2)$$

On vérifie qu'elles ont même nombre de composantes (deux) et que les premiers associés à $\mathfrak{a}$ sont les mêmes : (x) et (x, y).

Parmi les premiers associés à un idéal $\mathfrak{a}$, on distingue les premiers « minimaux » sur $\mathfrak{a}$ (pour la relation d'inclusion entre idéaux premiers) de ceux qui ne le sont pas et qu'on nomme premiers « immergés » (parce que, dans le cas des anneaux de polynômes, la variété algébrique qui leur est associée est immergée dans celle d'un des premiers minimaux).

Sur l'exemple précédent, l'idéal (x) est minimal sur $\mathfrak{a}$ alors que (x, y) est immergé : le point $x = 0, y = 0$ est immergé dans la droite $x = 0$.

Zéro et variété d'un idéal Soit $\mathfrak{a}$ un idéal de $K[x_1, \ldots, x_n]$ où K est un corps. On appelle zéro de l'idéal $\mathfrak{a}$ tout n-uplet z de la clôture algébrique de K tel que tous les polynômes de $\mathfrak{a}$ s'annulent au point z. On désigne par $V(\mathfrak{a})$ l'ensemble des zéros de l'idéal $\mathfrak{a}$.

Le radical d'un idéal $\mathfrak{a}$ est l'intersection des premiers associés à $\mathfrak{a}$

$$\sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t.$$

Une telle décomposition peut être rendue minimale en supprimant les premiers immergés de $\mathfrak{a}$. Il ne reste plus alors que les idéaux premiers minimaux sur $\mathfrak{a}$ (ou sur $\sqrt{\mathfrak{a}}$).

Théorème 4 *Dans un anneau nœthérien, tout idéal radiciel $\mathfrak{a}$ est une intersection finie d'idéaux premiers. Toute décomposition de $\mathfrak{a}$ peut être minimalisée en supprimant les composantes redondantes. Elle est alors définie de façon unique. Ses composantes sont les idéaux premiers « minimaux » sur $\mathfrak{a}$.*

Afin de construire des chaînes régulières, le problème clef est de détecter si un polynôme est diviseur de zéro modulo l'idéal $(C) : {I_C}^{\infty}$ où C est une chaîne régulière. La propriété

qui suit montre le lien important qui existe entre les premiers associés et les diviseurs de zéro.

Propriété 4 *Un élément p appartient à un premier associé à un idéal $\mathfrak{a}$ d'un anneau R si et seulement si p est nul ou diviseur de zéro dans $R/\mathfrak{a}$.*

Ensemble paramétrique Soit $\mathfrak{p}$ un idéal premier de R. Un ensemble paramétrique est un sous–ensemble N de $\{x_1, \ldots, x_n\}$ tel que $K[N] \cap \mathfrak{p} = (0)$ et tel que $x_i \notin N$ implique $K[N \cup \{x_i\}] \cap \mathfrak{p} \neq (0)$. On montre que tous les ensembles paramétriques d'un même idéal ont même cardinal.

Nous utiliserons souvent la propriété : si N est un ensemble paramétrique d'un idéal premier $\mathfrak{p}$, alors tout polynôme de $K[N]$ est non diviseur de zéro modulo $\mathfrak{p}$.

Pour reprendre une expression imagée de Rudolf Bkouche, « dans le cas général, on peut avoir un premier immergé, c'est–à–dire une CENSURÉ ». En effet, autant les premiers minimaux ont un sens (ils correspondent aux composantes irréductibles de la variété algébrique d'un idéal) autant les premiers immergés sont plus difficiles à appréhender (le livre [21] d'Eisenbud traite de ce problème). En particulier, on pourra « capter » les premiers minimaux par des « raisonnements sur les solutions de l'idéal » mais on ne pourra pas « capter » les premiers immergés ainsi. Le théorème (difficile) de Macaulay fournit des conditions suffisantes qui assurent qu'un idéal n'a pas de premiers immergés.

Théorème 5 (Théorème de Macaulay) *Soit $\mathfrak{a} = (f_1, \ldots, f_m)$ un idéal engendré par m générateurs dans un anneau de polynômes $K[x_1, \ldots, x_n]$ en n indéterminées au–dessus d'un corps K. Si $\dim \mathfrak{a} = n - m$ alors tous les premiers associés à $\mathfrak{a}$ ont même dimension.*

En particulier, tous les premiers associés à $\mathfrak{a}$ sont minimaux sur $\mathfrak{a}$.

La *dimension* d'un idéal est par définition le maximum des dimensions de ses premiers associés. Considérons le cas d'un anneau de polynômes $R = K[x_1, \ldots, x_n]$, la dimension d'un idéal premier $\mathfrak{p}$ est égal au degré de transcendance de l'extension de corps $\mathrm{Fr}(R/\mathfrak{p})$ sur K. Elle coïncide avec le nombre de paramètres nécessaires pour décrire la variété algébrique de $\mathfrak{p}$: une variété réduite à un point est de dimension zéro, une courbe est de dimension 1, une surface de dimension 2 ... On dit d'un idéal qu'il est *équidimensionnel* si tous ses premiers associés ont même dimension.

Le théorème de Macaulay peut être adapté aux idéaux de la forme $(A) : {I_A}^\infty$ où A est un ensemble triangulaire. Une des premières utilisations du théorème de Macaulay dans ce contexte est due à Sally Morrison [42, 43] dans le cas des idéaux de la forme $(A) : {S_A}^\infty$. L'idée s'applique aux idéaux de la forme $(A) : {I_A}^\infty$. L'idée consiste à appliquer le théorème de Macaulay sur l'idéal $(A, h\,x - 1)$ où x est une nouvelle indéterminée et h désigne le produit des initiaux (ou des séparants) de A. Ce résultat, dont la preuve n'est pas immédiate, est suffisant pour justifier les preuves (publiées) de théorèmes concernant les idéaux de la forme $(A) : {I_A}^\infty$, notamment [7, Lemma 2] et [2, Theorem 5.1]. Philippe Aubry, dans sa thèse [1, page 43], fournit une autre preuve basée sur les suites régulières dans les anneaux de Cohen–Macaulay.

Lemme 1 *Soit* $\mathfrak{a} = (A) : {I_A}^\infty$ *de l'anneau de polynômes* $R = K[x_1, \ldots, x_n]$ *où* A *est un système triangulaire formé de* m *éléments. On note* $L = \{y_1, \ldots, y_m\}$ *l'ensemble des indéterminées principales des éléments de* A *et* $N = \{t_1, \ldots, t_{n-m}\}$ *l'ensemble des autres indéterminées.*

Tous les premiers associés à $\mathfrak{a}$ *ont même dimension* $n-m$*. De plus,* N *est un ensemble paramétrique pour chaque premier associé à* $\mathfrak{a}$*.*

Preuve schématique :

Supposons R nœthérien. Alors $\mathfrak{a} : S^\infty$ est l'intersection des composantes primaires de $\mathfrak{a}$ dont les premiers associés ne contiennent aucun élément de S. Ainsi, les initiaux des éléments de A n'appartiennent à aucun des premiers associés à $\mathfrak{a} = (A) : {I_A}^\infty$. Par conséquent, dans $R/\mathfrak{p}$ (où $\mathfrak{p}$ désigne un quelconque premier associé à $\mathfrak{a}$) les indéterminées principales $y_1, \ldots, y_m$ sont algébriques sur les autres (i.e. les polynômes de A ne peuvent pas dégénérer). Cela prouve que $\dim \mathfrak{p} \leq n - m$. Maintenant, il est possible, pour former une solution de $\mathfrak{a}$, de fixer des valeurs presque arbitraires aux indéterminées $t_1, \ldots, t_{n-m}$ et donc $\dim \mathfrak{a} \geq n - m$. Par conséquent, $\dim \mathfrak{a} = n - m$.

Ce raisonnement montre aussi que si $\mathfrak{p}$ est un premier associé de dimension $n - m$, alors $\mathfrak{p} \cap K[t_1, \ldots, t_{n-m}] = (0)$.

Ce raisonnement ne fournit toutefois aucune information sur les premiers immergés. Pour prouver que $\mathfrak{a}$ n'a pas de premiers immergés, on se ramène au théorème de Macaulay. Il y a correspondance bijective entre les premiers associés de $(A) : I_A^\infty$ dans $K[x_1, \ldots, x_n]$ et ceux de $\mathfrak{a}' = (A \cup \{h\, x_{n+1} - 1\})$ dans $K[x_1, \ldots, x_n, x_{n+1}]$ où h désigne le produit des initiaux de A et x_{n+1} est une nouvelle indéterminée. En particulier, $\dim \mathfrak{a}' = (n+1) - (m+1) = n - m$. Comme $\mathfrak{a}'$ est engendré par $m+1$ générateurs, le théorème de Macaulay s'applique : $\mathfrak{a}'$ n'a pas de premiers immergés. On en déduit que $\mathfrak{a}$ n'en a pas non plus. □

Ce lemme est, en pratique, d'un grand intérêt : il nous autorise à mener les calculs dans $K(N)[L]$ au lieu de $K[N,L]$. Cela revient à "faire passer" les éléments de N dans le corps des coefficients. On est alors ramené à des problèmes en dimension 0, qui se traitent facilement ; en effet, on utilise le théorème des zéros qui fait le lien entre le radical d'un idéal et sa variété et le fait que les variétés en dimension zéro sont de simples ensembles finis de points.

Théorème 6 (Théorème des zéros) *Soit* $F = \{f_1, \ldots, f_m\}$ *une famille de polynômes de* $K[x_1, \ldots, x_n]$*. Soit* $\mathfrak{a}$ *l'idéal* $(f_1, \ldots, f_m)$*. Alors, pour tout polynôme* p *de* $K[x_1, \ldots, x_n]$*, on a :*

$$p \text{ s'annule sur tous les zéros de } \mathfrak{a} \iff p \in \sqrt{\mathfrak{a}}$$

On obtient un résultat similaire au lemme 1 en saturant (A) par S_A au lieu de I_A. Ce résultat est connu sous le nom du lemme de Lazard. Ce lemme a été publié pour la première fois dans [7]. Une version plus générale a été prouvée dans [42] et une autre preuve a été donnée dans [59]. L'article [8] présente une nouvelle version de la preuve originale de [7].

Lemme 2 (Lemme de Lazard) *Soit* $\mathfrak{a} = (A) : {S_A}^\infty$ *un idéal de l'anneau de polynômes* $R = K[x_1, \ldots, x_n]$ *où* A *est un système triangulaire formé de* m *éléments. On*

note $L = \{y_1, \ldots, y_m\}$ *l'ensemble des indéterminées principales des éléments de* A *et* $N = \{t_1, \ldots, t_{n-m}\}$ *l'ensemble des autres indéterminées.*

(1) tous les premiers associés à $\mathfrak{a}$ *ont même dimension* $n - m$*. De plus,* N *est un ensemble paramétrique pour chaque premier associé à* $\mathfrak{a}$*;*

(2) $\mathfrak{a}$ *est radiciel.*

Le lemme 1 (resp. de Lazard) est encore vrai si on remplace I_A (resp. S_A) par une famille S finie contenant I_A (resp. S_A).

Preuve schématique :

Voici quelques éléments de preuve de ce lemme. La justification du point *(1)* utilise un raisonnement sur les variétés et est calquée sur celle du lemme 1. Le point *(2)* est, quant à lui, prouvé grâce à une construction (en dimension 0) communiquée en 1994 à François Boulier par Daniel Lazard montrant que l'idéal $(A) : {S_A}^\infty$ est radiciel.

Le point *(2)* s'obtient en montrant que $R/(A) : {S_A}^\infty$ n'admet pas d'élément nilpotent. D'après le point *(1)*, il suffit de montrer que $K(t_1, \ldots, t_{n-m})[y_1, \ldots, y_m]/(A) : {S_A}^\infty$ n'admet pas d'élément nilpotent.

L'anneau $K(t_1, \ldots, t_{n-m})[y_1, \ldots, y_m]/(A) : {S_A}^\infty$ se construit incrémentalement sur les y_i (indéterminée par indéterminée).

On obtient à chaque étape un produit de corps (théorème des restes chinois). Un produit de corps n'admet pas d'élément nilpotent. □

Nous terminons cette section en présentant des chaînes régulières particulières.

Chaîne régulière sans carré Une chaîne régulière C est dite *sans carré* (ou encore *séparable*), si l'idéal $(C) : {I_C}^\infty$ est radiciel.

Les chaînes régulières sans carré possèdent une propriété intéressante tirée de [23] :

Propriété 5 *Si* C *est une chaîne régulière, alors :*

$$C \text{ est une chaîne régulière sans carré} \iff (C) : {I_C}^\infty = (C) : {H_C}^\infty$$

Preuve :

La preuve de cette propriété est assez technique et se trouve dans [23, page 8]. □

Initiaux itérés Soit un polynôme p de $R[X]$. On définit l'ensemble des initiaux itérés de p, noté $\mathrm{iter}(p)$, de la manière suivante :

- si p est constant, on pose $\mathrm{iter}(p) = \emptyset$;
- sinon on pose $\mathrm{iter}(p) = \{\imath_p\} \cup \mathrm{iter}(\imath_p)$.

Ensemble triangulaire normalisé Soit $C = \{p_1, \ldots, p_m\}$ un ensemble triangulaire avec $\mathrm{ld}\, p_1 < \cdots < \mathrm{ld}\, p_m$. On note $x_i = \mathrm{ld}\, p_i$ pour $1 \leq i \leq m$. L'ensemble C est dit normalisé si pour tout $2 \leq k \leq m$, l'ensemble des indéterminées principales de $\mathrm{iter}(p_k)$ est disjoint de l'ensemble $\{x_1, \ldots, x_{k-1}\}$.

Ensemble triangulaire fortement normalisé Soit $C = \{p_1, \ldots, p_m\}$ un ensemble triangulaire avec $\mathrm{ld}\, p_1 < \cdots < \mathrm{ld}\, p_m$. On note N l'ensemble des indéterminées qui ne sont indéterminées principales d'aucun des p_i. L'ensemble C est dit fortement normalisé si tous les initiaux de C sont des polynômes de $K[N]$.

Toute ensemble triangulaire fortement normalisé est normalisé.

1.4 Inversion modulo une chaîne régulière fortement normalisée

Étant donné un polynôme a de $R = K[x_1, \ldots, x_n]$ (avec $x_1 < \cdots < x_n$) et une chaîne régulière $T = \{p_1, \ldots, p_n\}$ (avec $\mathrm{ld}\, p_i = x_i$ pour $1 \leq i \leq n$) fortement normalisée, on cherche à calculer un polynôme b de R vérifiant :

$$a\, b = 1 \mod (T)$$

L'algorithme inverse calcule un tel polynôme b (nous verrons plus loin que ce calcul peut toutefois échouer) en se basant sur une généralisation naturelle de l'algorithme d'Euclide étendu. Il s'agit d'un algorithme purement algébrique dont l'idée remonte à [31], et dont un procédé est donné dans [41]. Nous n'en rappelons que le principe.

Comme T comporte autant de polynômes que d'indéterminées, l'initial de chaque p_i est constant supposé égal à 1. L'idéal (T) est donc de dimension zéro d'après le lemme 1.

Le système T constitue une base de Gröbner de l'idéal $\mathfrak{a} = (T)$ pour l'ordre lexicographique induit par l'ordre sur l'alphabet et peut donc servir à calculer la forme normale $\mathrm{NF}(p,T)$ (au sens des bases de Gröbner) d'un polynôme quelconque $p \in R$. Cette forme normale est un polynôme équivalent à p modulo $\mathfrak{a}$. Cette forme normale coïncide d'ailleurs avec $\mathsf{prem}(p,T)$ puisque les initiaux des p_i valent 1.

La fonction inverse prend en entrée :

- un polynôme a non nul de $K[x_1, \ldots, x_i]$ algébriquement réduit par rapport à l'ensemble $\{p_1, \ldots, p_i\}$;
- l'ensemble $\{p_1, \ldots, p_i\}$.

La fonction inverse tente de calculer :

- un polynôme b de $K[x_1, \ldots, x_i]$ tel que : $a\, b = 1 \mod (p_1, \ldots, p_i)$ et b est algébriquement réduit par rapport à $\{p_1, \ldots, p_i\}$.

Lorsque le calcul aboutit, inverse renvoie le polynôme b désiré. Si le calcul de l'inverse échoue, cela signifie qu'une factorisation d'un polynôme p_k modulo $(p_1, \ldots, p_{k-1})$, avec $1 \leq k \leq i$, a été découverte. Dans ce cas, inverse renvoie cette factorisation en levant une exception.

```
fonction inverse(a, {p_1, ..., p_i})
début
  si a ∈ K alors
    retourner a^{-1}
  sinon
```

soit i tel que $\mathrm{ld}\, a = \mathrm{ld}\, p_i$
$(u_1, u_2, u_3) :=$ Bézout $(p_i,\ a,\ \{p_1, \ldots, p_{i-1}\})$
si $u_3 = 1$ alors
retourner u_2
sinon
le calcul d'inverse échoue ; on lève une exception en renvoyant
la factorisation $p_i = u_3 \times \mathsf{pquo}(p_i, u_3, x_i)$ modulo $(p_1, \ldots, p_{i-1})$
fin si
fin si
fin

La fonction Bézout prend en entrée :

- deux polynômes a et b de même indéterminée principale x_i algébriquement réduits par rapport à $\{p_1, \ldots, p_{i-1}\}$. On suppose de plus $\imath_a = 1$;
- l'ensemble $\{p_1, \ldots, p_{i-1}\}$.

Elle tente de calculer une identité de Bézout

$$u_1\, a + u_2\, b = u_3 \mod (p_1, \ldots, p_{i-1})$$

vérifiant :

- les u_i sont dans $K[x_1, \ldots, x_i]$ et sont algébriquement réduits par rapport à l'ensemble $\{p_1, \ldots, p_{i-1}\}$;
- u_3 divise a et b modulo $(p_1, \ldots, p_{i-1})$;
- coeff_principal$(u_3, x_i) = 1$ (i.e. soit u_3 vaut 1, soit u_3 est un polynôme d'indéterminée principale x_i et d'initial 1).

Si le calcul échoue, cela signifie qu'un appel à inverse a échoué, et qu'une exception a été levée par inverse.

fonction Bézout $(a, b, \{p_1, \ldots, p_{i-1}\})$
début
$(u_1, u_2, u_3) := (1, 0, a)$
$(v_1, v_2, v_3) := (0, 1, b)$
tant que $v_3 \neq 0$ faire
$\overline{c} :=$ inverse (coeff_principal(v_3, x_i), $\{p_1, \ldots, p_{i-1}\}$)
$(v_1, v_2, v_3) := \overline{c} \cdot (v_1, v_2, v_3)$ (prendre les formes normales des coefficients)
$q :=$ le quotient de la division euclidienne de u_3 par v_3
(u_3 et v_3 vus comme des polynômes en x_i)
$(t_1, t_2, t_3) := (v_1, v_2, v_3)$
$(v_1, v_2, v_3) := (u_1, u_2, u_3) - q \cdot (v_1, v_2, v_3)$ (prendre les formes normales des coefficients)
$(u_1, u_2, u_3) := (t_1, t_2, t_3)$
fait
retourner(u_1, u_2, u_3)
fin

1.5 Détection des diviseurs de zéro

L'algorithme inverse permet de déterminer si un polynôme a est un diviseur de zéro. En effet, si un polynôme a est inversible, il est obligatoirement non diviseur de zéro. Pour tenir ce raisonnement, nous avons néanmoins supposé que nous travaillions en dimension zéro.

Ce raisonnement se généralise à la dimension positive. Considérons une chaîne régulière $T = \{p_1, \ldots, p_m\}$ fortement normalisée et notons L l'ensemble de ses indéterminées principales et N les autres indéterminées. Nous avons vu, grâce au lemme 1, que l'on peut calculer dans l'anneau $K(N)[L]$ (au lieu de $K[L,N]$) ce qui ramène des calculs en dimension zéro. Ainsi, T peut être considérée (en rendant unitaires ses initiaux) comme une chaîne fortement normalisée à autant d'équations que d'inconnues dans $K(N)[L]$. Si l'on calcule l'inverse b d'un polynôme a modulo $\mathfrak{a} = (T) : {I_T}^\infty$, on obtient un polynôme b dans $K(N)[L]$ qui peut comporter des polynômes de $K[N]$ au dénominateur. Si l'on chasse ces dénominateurs de b (en prenant le "numérateur" de b vu comme une fraction rationnelle), on obtient un polynôme b' vérifiant :

$$a\,b' = r \mod \mathfrak{a} \text{ avec } r \in K[N]$$

Si un tel polynôme b' est calculé, le polynôme a est non diviseur de zéro modulo $\mathfrak{a}$. En effet, si a était diviseur de zéro modulo $\mathfrak{a}$, $a\,b'$ serait aussi diviseur de zéro, ce qui est impossible car r n'est pas diviseur de zéro d'après le lemme 1.

Si l'algorithme inverse lève une exception, cela signifie qu'une factorisation d'un des polynômes $p_i = g\,h \mod (p_1, \ldots, p_{i-1})$ a été détectée. Dans ce cas, on pratique ce que Moreno Maza appelle un scindage de deuxième espèce dans [39, page 66]. Cela revient à "couper" la chaîne T en deux ensembles $T_g = T \setminus \{p_i\} \cup \{g\}$ et $T_h = T \setminus \{p_i\} \cup \{h\}$.

On montre (par le théorème des zéros) que les deux ensembles ainsi obtenus sont des chaînes régulières et que :

$$\sqrt{(T) : {I_T}^\infty} = \sqrt{(T_g) : {I_{T_g}}^\infty} \cap \sqrt{(T_h) : {I_{T_h}}^\infty}$$

On peut alors reprendre le raisonnement dans chacune des deux chaînes régulières.

1.6 Implantation

Les versions naïves de Bézout et inverse ont été codées en `Maple Vr5`. Elles nécessitent environ 300 lignes, si l'on inclut les procédures annexes de manipulation de polynômes en plusieurs variables (variable principale, coefficient principal, ...).

En pratique, on ne travaille pas dans l'anneau $K(N)[L]$ mais dans l'anneau de polynômes $K[N,L]$. Cela permet d'utiliser un algorithme des sous–résultants (par exemple, celui de Lionel Ducos de [20], ou celui de [35]) dans la fonction Bézout afin de limiter la taille des données intermédiaires. Toutefois, la fonction Bézout nécessite quelques aménagements pour être modifiée de la sorte : il faut supprimer les normalisations effectuées à chaque boucle, et remplacer le calcul d'inverse de coeff_principal(v_3,x_i) par un test

vérifiant si coeff_principal(v_3,x_i) est non diviseur de zéro (on a vu un tel test dans la sous–section précédente).

La réduction de la taille des données en utilisant un algorithme des sous–résultants a deux atouts majeurs. D'une part, le temps de calcul est amélioré car les calculs sur des données de petite taille sont plus rapides que sur des données de taille plus importante. D'autre part, lors de calculs complexes et coûteux en place mémoire, on évite une saturation de la mémoire qui pourrait faire échouer le calcul.

On peut éviter certains calculs dans Bézout. Le premier polynôme u_1 de l'identité de Bézout n'est jamais utilisé, et son calcul est donc inutile. Le coefficient u_2 est quant à lui utile pour calculer l'inverse d'un polynôme mais n'est pas utile pour tester si un polynôme est diviseur de zéro.

Les versions améliorées de Bézout, inverse ainsi qu'une fonction estRégulier (testant si un polynôme est régulier modulo un idéal $(C) : {I_C}^{\infty}$ où C est une chaîne régulière) ont été implantées en `Maple Vr5` (800 lignes de code) et utilisent la version des sous–résultants de Lionel Ducos.

Ces fonctions ont d'ailleurs permis d'implanter l'algorithme Decompose de Marc Moreno Maza qui décompose un système polynomial fini quelconque Σ en t chaînes régulières $C_1,\ldots,C_t$ vérifiant :

$$V(\Sigma) = W(C_1) \cup \cdots W(C_t)$$

où $W(C_i)$ désigne l'ensemble des zéros de l'idéal (C_i) qui n'annulent pas les initiaux de C_i.

Le langage Maple ne dispose pas de mécanisme d'exceptions. Pour lever ce problème, dans le code Maple, les fonctions Bézout et inverse renvoient un résultat spécial indiquant la factorisation découverte.

Chapitre 2

Algèbre différentielle

Sommaire

Ce chapitre présente les outils et les opérations nécessaires pour traiter les problèmes différentiels de cette thèse. Les résultats de ce chapitre sont essentiellement tirés de [52], [28], [7], [8]. Les sections 2.5 et 2.6 comportent toutefois trois résultats nouveaux : l'introduction des *chaînes différentielles régulières*, une clarification de la définition de *présentation caractéristique* donnée dans [8] et des outils permettant de calculer la *forme normale* d'un polynôme modulo une chaîne différentielle régulière.

Le cheminement du chapitre est similaire à celui du chapitre précédent. On présente l'algèbre différentielle définie par Ritt et Kolchin, qui étend les théories des idéaux et des polynômes au cas différentiel en introduisant des dérivations. Nous considérons alors des systèmes de polynômes différentiels du type :

$$\Sigma \begin{cases} p_1 = u_x^2 - 4u \\ p_2 = u_{xy} v_y - u + 1 \\ p_3 = v_{xx} - u_x \end{cases}$$

où u et v sont deux indéterminées différentielles (appelées aussi variables dépendantes) sur lesquels agissent deux dérivations δ_x et δ_y. Dans le système Σ, on a noté les dérivations en indice : u_x désigne $\delta_x u$.

Comme dans le chapitre précédent, on cherche un moyen de tester l'appartenance à un idéal différentiel engendré par un système fini de polynômes différentiels. Le contexte différentiel fait surgir de nouveaux problèmes par rapport au cas algébrique. Une fois ces problèmes identifiés et résolus, nous introduisons en section 2.5 la notion de *chaîne différentielle régulière*, qui est la généralisation des chaînes régulières au cas différentiel.

Nous faisons alors le lien entre les chaînes différentielles régulières et les ensembles caractéristiques de Ritt grâce aux théorèmes 8 et 9. Ce résultat est nouveau dans le sens où il constitue l'analogue du théorème 6.1 de [2] pour le cas différentiel. Les arguments sur lesquels ce résultat s'appuie sont toutefois prouvés dans [12] et [23, lemma 6.1].

Nous donnons alors en section 2.6 une nouvelle définition des *présentations caractéristiques*. Une présentation caractéristique est un ensemble caractéristique fortement normalisé dont les éléments de C sont primitifs (condition **D3** de la définition 6). Grâce à ces conditions, on prouve (propriété 9) qu'une présentation caractéristique est un ensemble caractéristique canonique de l'idéal qui lui est associé. Cette notion de présentation caractéristique s'applique également aux chaînes régulières, fournissant ainsi la même propriété de canonicité. Citons au passage qu'Ollivier a introduit, en se restreignant aux idéaux premiers, des ensembles caractéristiques particuliers [44, théorème 2, page 94 et définition 10, page 96] un peu plus faibles que les présentations caractéristiques : leurs éléments ne sont pas primitifs. Ainsi, ces ensembles caractéristiques ne sont pas canoniques[4].

Nous donnons ensuite des outils permettant de calculer la *forme normale* d'un polynôme modulo une chaîne différentielle régulière. Le problème du calcul de forme normale modulo des équations polynomiales différentielles était, à notre connaissance, uniquement cité dans [6] et nécessitait le calcul d'une base de Gröbner. La méthode que nous donnons est uniquement basée sur les ensembles triangulaires et la réduction de Ritt. Cette

4. Toutefois, quand des représentants canoniques sont nécessaires, par exemple en automatique, Ollivier divise les éléments de ses ensembles caractéristiques par leurs initiaux, obtenant ainsi des représentants canoniques.

méthode résout un problème laissé ouvert dans [6]. Cette méthode s'applique également pour des polynômes non différentiels modulo des chaînes régulières.

Le calcul de forme normale canonique de polynômes différentiels modulo une chaîne différentielle régulière C est intéressant car l'ensemble des formes normales modulo C forme un espace vectoriel sur le corps de base K des équations. On peut alors facilement rechercher des dépendances linéaires entre des éléments de l'anneau des polynômes quotienté par l'idéal «associé à C[5]». Cette idée est mise en œuvre dans l'algorithme FGLM [22] dans le contexte des bases de Gröbner et est adaptée aux systèmes différentiels réguliers dans l'algorithme dFGLM de [6].

Nous nous intéressons également aux solutions d'idéaux différentiels et donnons une reformulation du lemme de Rosenfeld qui donne des conditions suffisantes assurant l'existence et l'unicité de solutions.

Nous terminons le chapitre par une brève description des algorithmes connus de décomposition de systèmes d'équations différentielles. Nous présentons plus en détail l'algorithme Rosenfeld–Gröbner (implanté dans le paquetage `diffalg`) qui décompose un système d'équations en un nombre fini de présentations caractéristiques.

2.1 Idéaux différentiels

Les ouvrages de référence sont [52] et [28]. Une dérivation sur un anneau R est une application δ de R dans R qui vérifie pour tous $a, b \in R$

$$\begin{aligned} \delta(a+b) &= \delta a + \delta b \\ \delta(a\,b) &= (\delta a)\,b + a\,\delta b \quad \text{(règle de Leibniz)} \end{aligned}$$

Un *anneau différentiel* est un anneau muni d'un nombre fini de dérivations $\delta_1, \ldots, \delta_m$ qui commutent entre elles. Un anneau différentiel *ordinaire* est un anneau muni d'une seule dérivation.

Exemple ▷ Tout anneau peut être muni d'une structure différentielle : il suffit de le munir de la dérivation triviale, qui envoie tous ses éléments sur 0. Le corps $\mathbb{Q}(x)$ muni de la dérivation $\partial/\partial x$ est un exemple de corps différentiel (ordinaire). ◁

Le monoïde commutatif engendré par les dérivations est noté Θ. Ses éléments sont les *opérateurs de dérivations* $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$ où les a_i sont des entiers positifs ou nuls. La somme des exposants a_i, appelée l'*ordre* de l'opérateur θ, est notée $\mathrm{ord}\,\theta$. L'opérateur identité est l'unique opérateur d'ordre 0. Les autres opérateurs sont dits *propres*. Si $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$ et $\phi = \delta_1^{b_1} \cdots \delta_m^{b_m}$ alors $\theta\phi = \delta_1^{a_1+b_1} \cdots \delta_m^{a_m+b_m}$. Un *idéal différentiel* $\mathfrak{a}$ de R est un idéal de R stable par dérivation, c'est–à–dire un idéal vérifiant :

$$a \in \mathfrak{a} \Rightarrow \delta_i a \in \mathfrak{a} \text{ pour } 1 \leq i \leq m$$

Si Σ un sous–ensemble non vide de R, on note $[\Sigma]$ l'idéal différentiel engendré par Σ : c'est l'intersection de tous les idéaux différentiels contenant Σ. Les notions d'idéal radical, de radical d'un idéal et de saturation d'un idéal par une famille finie restent valables dans le cas différentiel.

5. Il s'agit de l'idéal $[C] : {H_C}^{\infty}$

2.2 Polynômes différentiels et réduction de Ritt

Soit $U = \{u_1, \ldots, u_n\}$ un ensemble de n *indéterminées différentielles*. Les opérateurs de dérivation agissent sur les indéterminées différentielles, donnant des *dérivées* θu. Si θu et ϕu sont deux dérivées d'une même indéterminée différentielle, on note $\mathrm{ppdc}(\theta u,\phi u) = \mathrm{ppcm}(\theta,\phi)\, u$ leur plus petite[6] dérivée commune.

On note ΘU l'ensemble des dérivées. Soit K un corps différentiel. L'anneau différentiel des polynômes différentiels construits sur l'alphabet ΘU et à coefficients dans K est noté $K\{u_1, \ldots, u_n\}$. Dans la suite, nous le noterons R.

Exemple ▷ Reprenons l'exemple donné en introduction. Il comporte trois polynômes différentiels.

$$\Sigma \begin{cases} p_1 = u_x^2 - 4u \\ p_2 = u_{xy} v_y - u + 1 \\ p_3 = v_{xx} - u_x \end{cases}$$

Il y a deux dérivations qui sont ∂/∂_x et ∂/∂_y et deux indéterminées différentielles u et v représentant moralement deux fonctions $u(x,y)$ et $v(x,y)$ de deux variables. On peut prendre pour corps des coefficients K le corps $\mathbb{Q}$ des rationnels ou le corps des fractions rationnelles $\mathbb{Q}(x,y)$. L'anneau de polynômes différentiels est $K\{u,v\}$. Les dérivées figurant dans le système sont u_x, u, u_{xy}, v_y et v_{xx}. Les opérateurs de dérivation sont notés en indice. Par exemple, $u_x = \partial u/\partial x$ et $u_{xy} = \partial^2 u/\partial x \partial y$. ◁

Comme dans le cas algébrique, on peut ordonner les dérivées de ΘU entre elles. Toutefois on ne considère pas des ordres totaux quelconques sur les dérivées mais des ordres particuliers appelés classements. Ces ordres sont présentés dans [28].

Classements (rankings) Un *classement* (en anglais un *ranking*) est un ordre total sur l'ensemble des dérivées, compatible avec l'action des dérivations sur ΘU. Il s'agit donc d'un ordre total sur ΘU vérifiant :

1. $\delta v > v$ (pour toute dérivation δ et toute dérivée v) ;
2. $v > w \Rightarrow \delta v > \delta w$ (pour toute dérivation δ et toutes dérivées v et w).

Parmi la grande famille des classements, qui sont d'ailleurs classifiés dans [48], on peut citer les deux types de classements suivants :

1 : les classements compatibles avec l'ordre total, ou plus simplement classements de l'ordre total (en Anglais *orderly*), c'est–à–dire vérifiant :

$$\mathrm{ord}\,\theta > \mathrm{ord}\,\phi \quad \Rightarrow \quad \theta u > \phi v \quad \text{pour tous } u,v \in U$$

2 : les classements d'élimination qui satisfont

$$u > v \quad \Rightarrow \quad \theta u > \phi v \quad \text{pour tous } \theta,\phi \in \Theta \text{ et } u,v \in U.$$

Une fois fixé un classement, on peut définir la *dérivée dominante* d'un polynôme différentiel p : c'est l'indéterminée principale (le leader) de p, vu comme un polynôme sur l'alphabet infini des dérivées. L'initial et le séparant d'un polynôme différentiel sont alors

6. la qualification "plus petite" prendra son sens lorsqu'on aura défini les classements

définis comme dans le cas algébrique. Les axiomes des classements font que le séparant d'un polynôme différentiel f est égal à l'initial de toutes les dérivées propres de f.

Exemple ▷ Soit $\mathcal{R}$ un classement de l'ordre total, commençant par :

$$u < v < u_y < u_x < v_y < v_x < u_{yy} < u_{xy} < u_{xx} < v_{yy} < v_{xy} < v_{xx} < \cdots$$

Les dérivées dominantes des éléments de Σ sont respectivement u_x,u_{xy},v_{xx} ; les rangs u_x^2,u_{xy},v_{xx} ; les séparants $2u_x$, v_y et 1. Dérivons le polynôme p_1 par rapport à y :

$$\delta_y p_1 = 2u_x u_{xy} - 4u_y.$$

On vérifie que l'initial de ce polynôme est bien le séparant de p_1. ◁

Les algorithmes de réduction de Ritt sont des extensions de l'algorithme de pseudo–réduction aux polynômes différentiels : on s'autorise à dériver les polynômes par lesquels on pseudo–divise.

Polynômes (partiellement) réduits Soit $p \in R \setminus K$ et $q \in R$ deux polynômes différentiels. Notons $\operatorname{rang} p = v^d$. Le polynôme différentiel q est dit *partiellement réduit* par rapport à p si aucune dérivée propre de la dérivée dominante de p ne figure dans q ; il est dit *réduit* par rapport à p s'il est partiellement réduit par rapport à p et si $\deg(q, v) < d$.

Si $A \subset R \setminus K$ et si $v \in \Theta U$, on pose :

$$A_v = \{\theta p \mid p \in A,\ \theta \in \Theta \text{ et } \operatorname{ld} \theta p \leq v\}.$$

Par conséquent, R_v désigne le sous–anneau de R constitué par les polynômes différentiels de dérivée dominante inférieure ou égale à v et

$$A \cap R_v = \{p \in A \mid \operatorname{ld} p \leq v\}.$$

On distingue l'algorithme de *réduction partielle* de l'algorithme de *réduction complète*. Soient $f \in R$ un polynôme différentiel et A un sous–ensemble fini de $R \setminus K$. Notons v la dérivée dominante de f et $\overline{A} = \{g \in A \mid \operatorname{ld} g \leq v\}$. L'algorithme de réduction partielle de f par A calcule un polynôme différentiel r (noté $r = \mathsf{reste\_partiel}(f, A)$) et un produit h de puissances de séparants d'éléments de $\overline{A}$ vérifiant :

1. r est partiellement réduit par rapport à $\overline{A}$ (et aussi par rapport à A) ;
2. $h\, f = r \mod (\overline{A}_v)$.

fonction reste_partiel(f, A)
début
  $h := 1$
  $r := f$
  tant que r n'est pas partiellement réduit
                par rapport à tous les éléments de A faire
    soit w la plus grande dérivée figurant dans r qui soit aussi
        la dérivée propre de la dérivée dominante d'un élément $p \in A$
    soit $\theta \in \Theta$ tel que $\theta \operatorname{ld} p = w$

$h := h\, s_p^{\deg(r,w)}$
$r :=$ prem$(r, \theta p, w)$
fait
retourner $[h,r]$
fin

L'algorithme de réduction complète de f par A calcule un polynôme différentiel r (noté $r =$ reste_complet(f, A)) et un produit h de puissances d'initiaux et de séparants d'éléments de $\overline{A}$ vérifiant :

1. r est réduit par rapport à $\overline{A}$ (et aussi par rapport à A) ;
2. $h\, f = r \mod (\overline{A}_v)$.

fonction reste_complet(f, A)
début
$h := 1$
$r := f$
tant que r n'est pas réduit par rapport à tous les éléments de A faire
soit w la plus grande dérivée figurant dans r qui vérifie
aussi l'une des conditions suivantes
(a) w est la dérivée propre de la dérivée dominante d'un élément $p \in A$
(b) w est égale à la dérivée dominante d'un $p \in A$ et $\deg(r, w) \geq \deg(p, w)$
si la condition (a) est remplie alors
soit $\theta \in \Theta$ tel que $\theta \operatorname{ld} p = w$
$h := h\, s_p^{\deg(r,w)}$
$r :=$ prem$(r, \theta p, w)$
sinon
$h := h\, i_p^{\deg(r,w)-\deg(p,w)+1}$
$r :=$ prem(r, p, w)
fin si
fait
retourner $[h,r]$
fin

Remarque : comme dans le cas algébrique, le résultat obtenu dépend de l'ordre dans lequel on opère les pseudo–divisions. Cette indétermination est levée dans les implantations.

Exemple ▷ Considérons le polynôme différentiel $f = 2u_{xy} + u_x$ et calculons le polynôme reste_partiel(f, Σ). La dérivée dominante u_{xy} de f est une dérivée propre de la dérivée dominante u_x de p_1. On dérive donc p_1 par rapport à y, obtenant un polynôme différentiel

$$\delta_y p_1 = 2u_x u_{xy} - 4u_y.$$

Le calcul de $r =$ prem$(f, \delta_y p_1, u_{xy})$ consiste à interpréter $\delta_y p_1$ comme la règle de réécriture

$$u_{xy} \to \frac{4u_y}{2u_x}$$

et à multiplier le résultat par une puissance appropriée du séparant de p_1 (le polynôme h) pour chasser les dénominateurs. Le reste

$$r = u_x^2 + 4u_y$$

est partiellement réduit par rapport à Σ. Notons $w = u_{xy}$ la dérivée dominante de f. Alors $\overline{\Sigma} = \{p_1,p_2\}$ et $\overline{\Sigma}_w = \{p_1,\delta_y p_1,p_2\}$. On peut vérifier que $hf = r \mod (\overline{\Sigma}_w)$. Le calcul de $\mathsf{reste\_complet}(f, A)$ commence comme ci–dessus. Le reste r n'est pas réduit par rapport à p_1. Il suffit de lui appliquer la substitution

$$u_x^2 \to 4u$$

pour obtenir le nouveau reste $4u_y + 4u$ avec $h = 2u_x$. ◁

Dérivée sous l'escalier Soit L est un ensemble (fini) de dérivées. On appelle *dérivée sous l'escalier de L* tout dérivée v vérifiant : v n'est la dérivée d'aucun des éléments de L.

Dans le cas où il y a une, deux ou trois dérivations, on peut représenter graphiquement un escalier, comme le montre la figure 2.1.

Exemple ▷

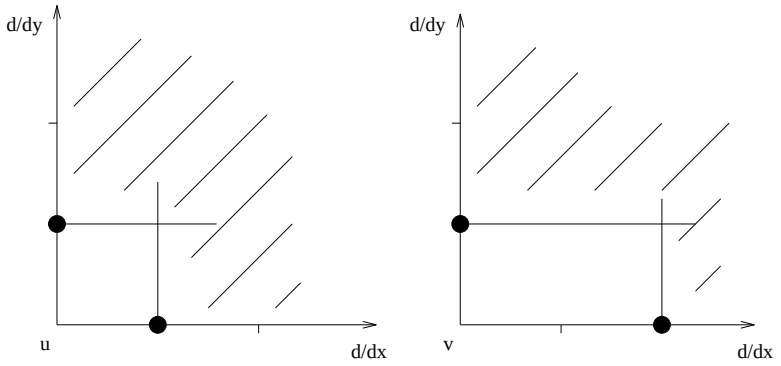


FIG. 2.1 – *Escalier de $L = \{u_x,u_y,v_{xx},v_y\}$*

Les dérivées sous l'escalier sont : u, v et v_x. ◁

Soit p un polynôme réduit par rapport à un système de polynômes A ; on pose $L = \mathrm{ld}\, A$. Alors, les dérivées figurant dans p appartiennent soit à L, soit à l'escalier de L. Nous verrons que la notion de dérivée sous l'escalier est utile lorsque l'on s'intéresse aux solutions d'un système de polynômes différentiels.

Propriété 6 (Réduction complète par un ensemble) *Soient p un polynôme et un ensemble fini $A \subset R \setminus K$. On a :*

$$\mathsf{reste\_complet}(p,A) = 0 \implies p \in [A] : {H_A}^\infty$$

Dans le cas algébrique, les chaînes régulières ont été introduites pour obtenir l'implication $p \in (A) : {I_A}^\infty \implies \mathsf{prem}(p,A) = 0$. Dans le cas différentiel, nous recherchons l'implication $p \in [A] : {H_A}^\infty \implies \mathsf{reste\_complet}(p,A) = 0$; la notion de chaîne régulière n'est pas suffisante pour plusieurs raisons. La première est que les réductions différentielles par un ensemble C font intervenir les initiaux mais aussi les séparants (qui sont les initiaux des dérivées de polynômes de C) ce qui oblige à saturer par H_A au lieu de I_A. L'exemple suivant illustre ce problème :

Exemple ▷ Soit $A = \{u_x^2\}$. L'idéal $I = [A] : {H_A}^\infty$ est égal à l'anneau R car I contient 1 (à cause de la saturation par le séparant valant $2\,u_x$).

On a $u_x \in I$ alors que $\mathsf{reste\_complet}(u_x,A) = u_x \neq 0$. ◁

La définition des chaînes régulières impose aux initiaux des polynômes d'être non diviseurs de zéro. Dans le cas différentiel, il faudra imposer de surcroît que les séparants soient non diviseurs de zéro, pour tenir compte de la saturation par H_A. Nous verrons que cela revient à considérer des chaînes régulières sans carré.

Un autre problème plus complexe est celui de la présence possible de relation "cachée" illustrée dans l'exemple suivant.

Exemple ▷ Reprenons le système Σ vu précédemment. Les polynômes p_1 et p_2 ont même indéterminée différentielle u. Les polynômes $p_3 = \delta_y p_1 = 2\,u_x\,u_{xy} - 4\,u_y$ et p_2 ont même dérivée dominante u_{xy}.

Ainsi le polynôme $q = i_{p_3}\,p_2 - i_{p_2}\,p_3$ ne contient plus la dérivée u_{xy}.

Le polynôme q vaut $2\,u_x p_2 - v_y\,p_3 = (2\,u_x\,v_y\,u_{xy} - 2\,u_x\,u + 2\,u_x) - (2\,u_x\,v_y\,u_{xy} - 4\,v_y\,u_y) = 4\,v_y\,u_y - 2\,u_x\,u + 2\,u_x$.

On a $q \in [p_1,p_2]$ alors que $\mathsf{reste\_complet}(q,\{p_1,p_2\}) = q \neq 0$. ◁

Ce type de relation "cachée" (à rapprocher des S–polynômes de la théorie des bases de Gröbner) porte le nom de Δ–polynômes et nécessite une étude particulière détaillée dans la section suivante.

2.3 Paires critiques et Δ–polynômes

Définition 1 (paires critiques) *Un ensemble $\{p_1, p_2\}$ de polynômes différentiels forme une* paire critique *si les dérivées dominantes de p_1 et de p_2 ont même indéterminée différentielle. Si A est un ensemble de polynômes différentiels alors* paires_critiques(A) *désigne l'ensemble de toutes les paires critiques qu'il est possible de former avec ses éléments.*

Dans une paire critique, l'ordre des éléments est sans importance. On ne considérera jamais de paires critiques $\{p_1, p_2\}$ telles que $\operatorname{rang} p_1 = \operatorname{rang} p_2$ (par contre, il se peut que les dérivées dominantes soient égales). Si la dérivée dominante de (mettons) p_2 est une dérivée de celle de p_1 alors la paire est appelée *paire de réduction.*

Définition 2 (Δ–polynômes) *Soit $\{p_1, p_2\}$ une paire critique avec $\operatorname{rang} p_1 < \operatorname{rang} p_2$. Notons respectivement $\theta_1 u$, $\theta_2 u$ les dérivées dominantes de p_1 et de p_2 et $\theta_{12} u$ leur plus petite dérivée commune. Le Δ–polynôme $\Delta(p_1, p_2)$ entre p_1 et p_2 est défini comme suit :*

si $\{p_1, p_2\}$ *est une paire de réduction alors*

$$\Delta(p_1, p_2) = \mathsf{prem}(p_2, \frac{\theta_2}{\theta_1} p_1, \theta_2 u)$$

sinon

$$\Delta(p_1, p_2) = s_1 \frac{\theta_{12}}{\theta_2} p_2 - s_2 \frac{\theta_{12}}{\theta_1} p_1.$$

Si A *est un ensemble de polynômes différentiels,* $\Delta(A)$ *désigne l'ensemble de tous les* Δ*–polynômes qu'il est possible de former à partir de ses éléments.*

Exemple ▷ On a paires_critiques(Σ) = $\{\{p_1,p_2\}\}$. La paire $\{p_1,p_2\}$ est une paire de réduction et

$$\Delta(p_1,p_2) = \mathsf{reste\_complet}(p_2, \delta_y p_1) = 4u_y v_y - 2uu_x + 2u_x.$$

Ce polynôme (appelons–le p_4) admet v_y pour dérivée dominante. Son séparant est $s_4 = 4u_y$. Il forme une paire qui n'est pas une paire de réduction avec p_3 et on a

$$\begin{aligned} \Delta(p_3,p_4) &= \delta_{xx} p_4 - s_4 \delta_y p_3 \\ &= 2u_{xxx} - 2u_{xxx}u - 6u_{xx}u_x + 4u_{xxy}v_y + 8u_{xy}v_{xy} + 4u_y u_{xy}. \end{aligned}$$

◁

Le polynôme $\Delta(p_1,p_2)$ est précisément le polynôme q (qu'on avait appelé relation "cachée") calculé dans l'exemple de la sous–section précédente. Nous avions vu que l'implication $p \in [A] : {H_A}^\infty \implies \mathsf{reste\_complet}(p,A)$ était fausse pour $p = \Delta(p_1,p_2)$.

Pour régler ce problème, on pourrait imposer aux paires critiques $\{p_1,p_2\}$ d'un ensemble A de vérifier $\mathsf{reste\_complet}(\Delta(p_1,p_2),A) = 0$. Cette notion *intuitive* est toutefois peu commode pour écrire les preuves d'algorithmes. On lui préfère la notion plus algébrique de *paire critique résolue* :

Définition 3 (paires critiques résolues) *Une paire critique* $\{p_1, p_2\}$ *est dite* résolue *par un système d'équations et d'inéquations polynomiales différentielles* $A = 0$, $S \neq 0$ *s'il existe une dérivée* v *strictement inférieure à la plus petite dérivée commune des dérivées dominantes de* p_1 *et de* p_2 *telle que*

$$\Delta(p_1, p_2) \in (A_v) : (S \cap R_v)^\infty.$$

Le lecteur peut vérifier que toute paire critique résolue selon le sens intuitif est résolue au sens de la définition 3, sous réserve que les initiaux des éléments de A fassent partie de S. Dans les algorithmes, nous testerons qu'une paire critique est résolue selon le sens intuitif car il est plus facile de tester $\mathsf{reste\_complet}(\Delta(p_1,p_2),A) = 0$ que $\Delta(p_1, p_2) \in (A_v) : (S \cap R_v)^\infty$.

2.4 Idéaux différentiels réguliers

On considère des systèmes $A = 0$, $S \neq 0$ tels que toutes les paires critiques de A soient résolues par $A = 0$, $S \neq 0$, et vérifiant aussi deux hypothèses techniques. Ce sont les systèmes différentiels réguliers. Grâce à ces systèmes, on pourra introduire l'équivalent des chaînes régulières dans le cas différentiel.

Ensembles différentiellement triangulaires et autoréduits Soit $R = K\{U\}$ un anneau de polynômes différentiels. Un ensemble $A \subset R \setminus K$ est dit *différentiellement triangulaire* s'il est triangulaire et si ses éléments sont deux–à–deux partiellement réduits. Un ensemble $A \subset R \setminus K$ est dit *autoréduit* si ses éléments sont réduits deux–à–deux. Tout ensemble autoréduit est différentiellement triangulaire.

Définition 4 (Systèmes différentiels réguliers) *Un système différentiel d'équations et d'inéquations $A = 0$, $S \neq 0$ est appelé* système différentiel régulier *s'il vérifie les trois conditions suivantes :*

C1 *A est différentiellement triangulaire ;*

C2 *S contient les séparants des éléments de A et ne comporte que des polynômes différentiels partiellement réduits par rapport à A ;*

C3 *toutes les paires critiques $\{p, p'\} \in$ paires_critiques(A) sont résolues par le système $A = 0$, $S \neq 0$ (propriété de cohérence).*

Si $A = 0$, $S \neq 0$ est un système différentiel régulier, on appelle *idéal algébrique régulier* défini par le système l'idéal $(A) : S^\infty$ et *idéal différentiel régulier* l'idéal différentiel $[A] : S^\infty$.

Lien avec les ensembles autoréduits et cohérents Les ensembles autoréduits et cohérents définis dans [54, 28] sont des cas particuliers de systèmes différentiels réguliers. Plus précisément, si C est un ensemble autoréduit et cohérent alors le système $C = 0$, $H_C \neq 0$ est un système différentiel régulier.

Les deux lemmes qui suivent synthétisent les principales propriétés des systèmes différentiels réguliers. Afin de les énoncer, nous rappelons le théorème de décomposition d'un idéal radical en idéaux premiers (le théorème de décomposition d'un idéal en idéaux primaires ne s'applique pas car les anneaux différentiels ne sont pas nœtheriens).

Théorème 7 (Décomposition d'un idéal radical en idéaux premiers) *Tout idéal différentiel radiciel $\mathfrak{r}$ de R ($\mathfrak{r} \neq R$) est une intersection finie d'idéaux différentiels premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Cette décomposition est unique lorsqu'elle est minimale (i.e. $i \neq j \implies \mathfrak{p}_i \subsetneq \mathfrak{p}_j$). Les idéaux $\mathfrak{p}_i$ sont appelés les* composantes premières minimales *de $\mathfrak{r}$.*

Lemme 3 (Lemme de Rosenfeld) *Soient $A = 0$, $S \neq 0$ un système différentiel régulier d'un anneau de polynômes différentiels R et R_0 l'anneau des polynômes différentiels partiellement réduits par rapport à A. On a :*

$$[A] : S^\infty \cap R_0 = (A) : S^\infty$$

Lemme 4 (Remontée du lemme de Lazard) *Soient $A = 0$, $S \neq 0$ un système différentiel régulier d'un anneau de polynômes différentiels R et R_0 l'anneau des polynômes différentiels partiellement réduits par rapport à A. Alors*

1. *l'idéal différentiel $[A] : S^\infty$ est radiciel ;*
2. *il y a bijection entre les idéaux différentiels premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ minimaux sur $[A] : S^\infty$ et les idéaux premiers $\mathfrak{b}_1, \ldots, \mathfrak{b}_t$ minimaux sur $(A) : S^\infty$ donnée par $\mathfrak{p}_i \cap R_0 = \mathfrak{b}_i$.*

La remontée du lemme de Lazard pour les idéaux différentiels est énoncée pour la première fois dans [8]. Une autre preuve apparaît dans [23].

Grâce au lemme de Rosenfeld, on peut ramener des problèmes différentiels à des problèmes algébriques. Voyons par exemple, le problème de l'appartenance d'un polynôme p à $[A] : S^\infty$, où $A = 0$, $S \neq 0$ est un système différentiel régulier. Si p appartient à R_0, le point 3 nous donne l'équivalence : $p \in [A] : S^\infty \iff p \in (A) : S^\infty$. On est donc ramené à un problème algébrique.

2.5 Chaînes différentielles régulières et ensembles caractéristiques de Ritt

Nous avons vu précédemment que l'on pouvait, grâce aux systèmes différentiels réguliers, ramener un problème différentiel à un problème algébrique. Si l'on raffine ces systèmes en leur imposant des propriétés algébriques (à savoir d'être des chaînes régulières sans carré), on obtient alors l'équivalent des chaînes régulières dans le cas différentiel. Ces ensembles sont naturellement appelées *chaînes différentielles régulières.* Nous verrons, dans le chapitre 4, l'algorithme regCaractéristique qui convertit un système différentiel régulier $A = 0$, $S \neq 0$ [7] en une ou plusieurs chaînes différentielles régulières.

Définition 5 (Chaîne différentielle régulière) *On appelle* chaîne différentielle régulière[8] *tout ensemble C vérifiant :*

- *$C = 0$, $H_C \neq 0$ est un système différentiel régulier ;*
- *C est une chaîne régulière sans carré.*

Comme les chaînes régulières, les chaînes différentielles fournissent un test d'appartenance.

Propriété 7 *Soit C une chaîne différentielle régulière. On a :*

$$p \in [C] : {H_C}^\infty \iff \mathsf{reste\_complet}(p,C) = 0$$

Preuve :

L'implication de droite à gauche étant évidente, il suffit de prouver que $p \in [C] : {H_C}^\infty$ implique $\mathsf{reste\_complet}(p,C) = 0$.

Soit $p \in [C] : {H_C}^\infty$ et soit $r = \mathsf{reste\_complet}(p,C)$. En notant R_0 l'anneau des polynômes partiellement réduits par rapport à C, on a $r \in R_0$. Ainsi $r \in R_0 \cap [C] : {H_C}^\infty$ car $p \in [C] : {H_C}^\infty$.

D'après le lemme de Rosenfeld (lemme 3), on a $r \in (C) : {H_C}^\infty$. Comme C est une chaîne régulière sans carré, $(C) : {I_C}^\infty = (C) : {H_C}^\infty$ d'après la propriété 5. Ainsi $r = \mathsf{prem}(r,C)$ et $r \in (C) : {I_C}^\infty$, ce qui implique que $r = 0$. □

Comme dans le cas algébrique, on peut faire le lien entre les chaînes régulières et les ensembles caractéristiques de Ritt. On obtient alors l'analogue du théorème 6.1 de [2].

7. vérifiant $H_A \subset S$

8. Les impatients pourront dire *chaîne d-régulière* mais éviteront la *d-chaîne régulière !*

Ensembles caractéristiques Soit $A \subset K\{U\}$ un ensemble de polynômes. Supposons que A ne contienne aucun élément non nul de K. Alors un sous–ensemble C de A est un *ensemble caractéristique* de A s'il est autoréduit et si A ne contient aucun élément non nul réduit par rapport à C.

Propriété 8 (Réduction par un ensemble caractéristique) *Soit C un ensemble caractéristique d'un idéal I. Tout élément de I est réduit à 0 par C.*

Preuve :
La preuve est identique au cas algébrique en remplaçant prem par reste_complet. □

Par conséquent, si C est un ensemble caractéristique de $[C] : {H_C}^\infty$, on a l'équivalence $p \in [C] : {H_C}^\infty \iff \mathsf{reste\_complet}(p,C) = 0$, propriété que possèdent les chaînes différentielles régulières. Les théorèmes 8 et 9 donnent l'équivalent[9] du théorème 6.1 de [2] pour les chaînes différentielles régulières :

Théorème 8 *Soit C un ensemble différentiellement triangulaire. Les deux conditions suivantes sont équivalentes :*

1. *C est une chaîne différentielle régulière ;*
2. *pour tout p de R, $\mathsf{reste\_complet}(p,C) = 0 \iff p \in [C] : {H_C}^\infty$.*

Preuve :
L'implication 1 $\implies$ 2 n'est rien d'autre que la propriété 7.

Prouvons l'autre implication. Le système $C = 0$, $H_C \neq 0$ vérifie les conditions **C1** et **C2**. Soit $\{p,p'\}$ une paire critique de C. Comme $\Delta(p,p') \in [C] : {H_C}^\infty$, on a $\mathsf{reste\_complet}(\Delta(p,p'),C) = 0$ ce qui assure la condition **C3**. Ainsi $C = 0$, $H_C \neq 0$ est un système différentiel régulier.

Il reste à prouver que C est une chaîne régulière sans carré. Soit R_0 l'anneau des polynômes partiellement réduits par rapport à C. Soit p un polynôme de $(C) : {I_C}^\infty$ (qui est un idéal de l'anneau R_0). Comme $(C) : {I_C}^\infty \subset \mathfrak{a}$, $\mathsf{reste\_complet}(p,C) = 0$. Comme $p \in R_0$, seules des réductions algébriques se produisent lors du calcul de $\mathsf{reste\_complet}(p,C)$. Ainsi, on a $\mathsf{prem}(p,C) = 0$. D'après le théorème 1, C est une chaîne régulière.

De l'inclusion $(C) : {H_C}^\infty \subset \mathfrak{a}$, et par un raisonnement similaire, on a l'implication : $p \in (C) : {H_C}^\infty \implies \mathsf{prem}(p,C) = 0$. On a donc $(C) : {I_C}^\infty = (C) : {H_C}^\infty$. D'après la propriété 5, C est une chaîne régulière sans carré.

□

Théorème 9 *Si C est une chaîne différentielle régulière (a priori non autoréduite), C a même rang que tout ensemble caractéristique de $[C] : {H_C}^\infty$. Si C est un ensemble différentiellement triangulaire, les deux conditions suivantes sont équivalentes :*

1. *C est une chaîne différentielle régulière autoréduite ;*
2. *C est un ensemble caractéristique de $[C] : {H_C}^\infty$.*

9. Comme dans le cas algébrique, on formule ce théorème en deux théorèmes à cause de la condition d'autoréduction.

Preuve :
$1 \implies 2$.

Soit p un polynôme réduit par rapport à C. On doit montrer que p est nul. Le polynôme p étant réduit, p est dans R_0, où R_0 désigne l'anneau des polynômes partiellement réduits par rapport à C. Comme $C = 0$, $H_C \neq 0$ est un système différentiel régulier, le lemme de Rosenfeld (lemme 3), s'applique et on a $p \in (C) : {H_C}^\infty$. Comme C est sans carré, on a $(C) : {I_C}^\infty = (C) : {H_C}^\infty$ d'après la propriété 5. Ainsi, p est réduit par rapport à C et $p \in (C) : {I_C}^\infty$ ce qui implique $p = 0$ d'après le théorème 2.

$2 \implies 1$.

On a l'équivalence $p \in [C] : {H_C}^\infty \iff \mathsf{reste\_complet}(p,C) = 0$ car C est un ensemble caractéristique de $[C] : {H_C}^\infty$. On en déduit grâce au théorème 8 que C est une chaîne différentielle régulière. L'ensemble C est autoréduit car un ensemble caractéristique l'est par définition. □

2.6 Présentations caractéristiques et formes normales

Cette section présente deux résultats nouveaux. Le premier est une clarification de la notion de *présentation caractéristique* introduite dans [8]. Une *présentation caractéristique* est une chaîne différentielle régulière particulière parmi toutes les chaînes différentielles régulières qui engendrent le même idéal. Nous donnons une nouvelle définition des présentations caractéristiques, conceptuellement plus simple que celle fournie dans [8], qui n'utilise pas de base de Gröbner. Une conséquence directe de cette clarification est que l'on obtient le même résultat de canonicité pour les chaînes régulières.

Le deuxième résultat concerne la définition et le calcul de la forme normale d'un polynôme modulo une chaîne différentielle régulière. On obtient alors l'équivalent des formes normales modulo un idéal $\mathfrak{a}$ dont une base de Gröbner est $\mathcal{B}$:

$$p = p' \mod \mathfrak{a} \iff \text{forme\_normale}(p,\mathcal{B}) = \text{forme\_normale}(p',\mathcal{B})$$

Les formes normales dans la théorie des bases de Gröbner sont des polynômes. Toutefois, les formes normales que nous introduisons sont des fractions en raison des multiplications par les initiaux et les séparants qui se produisent lors des réductions. Si C est une chaîne différentielle régulière, et en notant $\mathrm{NF}(p,C)$ la forme normale de p modulo C, nous avons :

$$p = p' \mod [C] : {H_C}^\infty \iff \mathrm{NF}(p,C) = \mathrm{NF}(p',C)$$

De plus, cette notion de forme normale est également valable dans le cas algébrique, c'est–à–dire pour les chaînes régulières.

2.6.1 Présentations caractéristiques

Une chaîne différentielle régulière C n'est en général pas un représentant canonique de l'idéal $\mathfrak{a} = [C] : {H_C}^\infty$ i.e. il peut exister une autre chaîne différentielle régulière C' telle que $\mathfrak{a} = [C'] : {H_{C'}}^\infty$.

Exemple ▷ C et C' sont deux chaînes différentielles régulières (avec $u > v$) et $[C] : {I_C}^\infty = \overline{[C'] : {I_{C'}}^\infty}$.

$$C \left\{ \begin{array}{c} u - v \\ v^2 - 2 \end{array} \right. \qquad C' \left\{ \begin{array}{c} v\,u - 2 \\ v^2 - 2 \end{array} \right.$$

Il suffit de remarquer que $v\,(u - v) = v\,u - v^2 = v\,u - 2 \mod (v^2 - 2)$ ◁

Pour obtenir une chaîne différentielle régulière C canonique, il suffit d'imposer trois conditions supplémentaires :

Définition 6 *Une chaîne différentielle régulière C pour un classement $\mathcal{R}$ est une* présentation caractéristique *si (L est l'ensemble des dérivées dominantes et N les autres dérivées figurant dans C) :*

D1 *C est autoréduit ;*

D2 *C est fortement normalisé ;*

D3 *les polynômes de C, vus comme des polynômes à coefficients dans $K[N]$ et à indéterminées dans L, sont primitifs i.e. pour tout $p \in C$, le pgcd des coefficients de p (vu comme polynôme de $K[N][L]$) vaut 1.*

On dira aussi que C est la présentation caractéristique d'un idéal $\mathfrak{a}$ si C est une présentation caractéristique et si $[C] : {H_C}^\infty = \mathfrak{a}$.

Cette notion a été introduite dans [8] (par une définition différente[10] basée sur les bases de Gröbner) puis clarifiée dans [23] et [10].

Exemple ▷ Le système différentiel ci–dessous est la présentation caractéristique de l'idéal $\sqrt{[\Sigma]}$ pour un classement commençant par :

$$u < v < u_y < u_x < v_y < v_x < u_{yy} < u_{xy} < u_{xx} < v_{yy} < v_{xy} < v_{xx} < \cdots$$

$$C \left\{ \begin{array}{l} v_{xx} - u_x \\ 4v_y u + u_x u_y - u_x u_y u \\ u_x^2 - 4u \\ u_y^2 - 2u \end{array} \right.$$

◁

Propriété 9 (Canonicité des présentations caractéristiques) *Une présentation caractéristique est un représentant canonique de l'idéal qu'elle définit : elle ne dépend que de l'idéal et du classement choisi.*

Preuve :

Soient C et C' deux présentations caractéristiques d'un même idéal $\mathfrak{a} = [C] : {H_C}^\infty = [C'] : {H_{C'}}^\infty$. Les deux ensembles ont même rang car ce sont deux ensembles caractéristiques du même idéal. Ainsi, C et C' ont même ensemble de dérivées dominantes noté L. On note N l'ensemble des dérivées sous l'escalier donné par L.

10. nous ne prouvons pas l'équivalence de ces deux définitions

Soient $f \in C$ et $f' \in C'$ deux polynômes de même rang v^d. Soient i et i' leurs initiaux respectifs. Le polynôme $p = i'\,f - i\,f'$ appartient à $\mathfrak{a}$.

Le degré de p en v est strictement inférieur à d ; comme f et f' sont réduits par rapport à C et C', p est réduit par rapport à C et C'. Ainsi, p est le polynôme nul.

Par conséquent, $i'\,f = i\,f'$. Comme f et f' (vus comme polynômes de $K[N][L]$) sont primitifs, on a $f = f'$. On a donc $C = C'$. □

Application au cas algébrique Tout se qui précède se transpose au cas algébrique : si une chaîne régulière C vérifie les trois conditions **D1**, **D2** et **D3** de la définition 6, alors C est un représentant canonique de $(C) : {I_C}^\infty$.

Ce problème de la canonicité est essentiellement déjà résolu dans [31, propriété 2]. Toutefois, dans [31, propriété 2], la normalisation simple n'est pas suffisante pour assurer la canonicité. La condition D2 (normalisation forte), déjà introduite par Ollivier dans [44, déf. 10, p.96], est un peu plus restrictive que la normalisation simple, et garantit la canonicité.

2.6.2 Formes normales modulo une chaîne différentielle régulière

Soit C une chaîne différentielle régulière pour un classement $\mathcal{R}$. Ce qui suit est extrait de [10]. L est l'ensemble des dérivées dominantes de C et N est l'ensemble des autres dérivées figurant dans C. On note $(K[N]^*)^{-1}R$ l'anneau R localisé par $K[N]^* = K[N]\backslash\{0\}$ i.e. les fractions à numérateur dans R et à dénominateur dans $K[N] \setminus \{0\}$.

Théorème-définition 1 (Forme normale) *pour tout $a \in R$, il existe une unique fraction rationnelle p/q de $(K[N]^*)^{-1}R$, appelée* forme normale *de a modulo C, et notée* NF(a,C)*, satisfaisant :*

1. $q\,a = p \mod [C] : {H_C}^\infty$;
2. *p est réduit par rapport à C.*

Preuve :

L'existence de la forme normale est une conséquence de la méthode de calcul fournie plus loin. On montre l'unicité. Soient p/q et p'/q' deux formes normales de a. On a $p'\,q - p\,q' \in [C] : {H_C}^\infty$. Comme p et p' sont réduits par rapport à C et que q et q' sont dans $K[N]$, $p'\,q - p\,q'$ est réduit par rapport à C. Comme C est un ensemble caractéristique de $[C] : {H_C}^\infty$, $p'\,q - p\,q'$ vaut zéro. □

L'ensemble des formes normales de R modulo une chaîne différentielle régulière C forme un espace vectoriel sur K (i.e. toute combinaison linéaire de formes normales est une forme normale). Cette propriété, qui permet de détecter facilement les dépendances linéaires sur K entre éléments de $R/\mathfrak{a}$ (où $\mathfrak{a} = [C] : {H_C}^\infty$), a fourni un analogue de [22] mis en œuvre dans [6]. Le produit de deux formes normales n'est en général pas une forme normale car la condition 2 n'est pas assurée (le produit de deux polynômes réduits par rapport à C n'est a priori pas réduit par rapport à C).

Lemme 5 *Soit q et q' deux polynômes de R et C une chaîne différentielle régulière. On pose $\mathfrak{a} = [C] : {H_C}^\infty$.*

Si $q = q' \mod \mathfrak{a}$, *alors* $\mathrm{NF}(q,C) = \mathrm{NF}(q',C)$.

Preuve :
Soit a/b et a'/b' les formes normales respectives de q et q'. Le polynôme $a\,b' - a'\,b$ est dans $K[N]$ car $b, b' \in K[N]$ et a, a' sont réduits par rapport à C. Comme C est un ensemble caractéristique de $\mathfrak{a}$, le polynôme $a\,b' - a'\,b$ est nul et $\mathrm{NF}(q,C) = \mathrm{NF}(q',C)$. □

Calcul de la forme normale (cas où C est une présentation caractéristique)
Soient $a \in R$ un polynôme différentiel et $r = \mathsf{reste\_complet}(a,C)$. On a la relation

$$i_1^{\alpha_1} \cdots i_t^{\alpha_t}\, s_1^{\beta_1} \cdots s_t^{\beta_t}\, a \;=\; r \mod \mathfrak{a} \tag{2.1}$$

où les i_ℓ et les s_ℓ désignent respectivement les initiaux et les séparants des éléments de C et où les α_ℓ,β_ℓ sont des entiers naturels.

L'algorithme inverse de calcul d'inverse permet, pour chaque s_ℓ, de calculer un couple $(\overline{s}_\ell, \overline{r}_\ell)$ tel que $\overline{r}_\ell \in K[N]$ et

$$\overline{s}_\ell\, s_\ell = \overline{r}_\ell \mod \mathfrak{a}.$$

En pratique, les inverses des séparants peuvent être précalculés pour éviter des calculs inutiles. En multipliant l'égalité (2.1) par les puissances appropriées des $\overline{s}_\ell$ on obtient

$$i_1^{\alpha_1} \cdots i_t^{\alpha_t}\, \overline{r}_1^{\beta_1} \cdots \overline{r}_t^{\beta_t}\, a \;=\; \overline{s}_1^{\beta_1} \cdots \overline{s}_t^{\beta_t}\, r \mod \mathfrak{a}. \tag{2.2}$$

Le terme $i_1^{\alpha_1} \cdots i_t^{\alpha_t}\, \overline{r}_1^{\beta_1} \cdots \overline{r}_t^{\beta_t}$ appartient à $K[N]$ car les initiaux de C sont dans $K[N]$ (C est fortement normalisé) et les $\overline{r}_i$ sont, par construction, dans $K[N]$.

Cependant, le membre droit n'est pas nécessairement réduit par rapport à C. En effectuant une réduction purement algébrique du membre droit, on obtient

$$i_1^{\gamma_1} \cdots i_t^{\gamma_t}\, \overline{s}_1^{\beta_1} \cdots \overline{s}_t^{\beta_t}\, r \;=\; r' \mod \mathfrak{a}. \tag{2.3}$$

La forme normale $\mathrm{NF}(a,C)$ s'obtient en rendant irréductible la fraction rationnelle

$$\frac{r'}{i_1^{\alpha_1+\gamma_1} \cdots i_t^{\alpha_t+\gamma_t}\, \overline{r}_1^{\beta_1} \cdots \overline{r}_t^{\beta_t}}.$$

qui est obtenue en combinant les relations 2.2 et 2.3.

Exemple ▷ Considérons le polynôme différentiel $u_x^2 - 4u$, qui forme une présentation caractéristique C de l'idéal différentiel premier $\mathfrak{a} = [u_x^2 - 4u] : \{u_x\}^\infty$.

Calculons la forme normale de u_{xy}. En réduisant partiellement u_{xy} par $u_x^2 - 4u$, on trouve la relation

$$2u_x\, u_{xy} = 4u_y \mod \mathfrak{a}$$

Un calcul d'inverse algébrique fournit $1/u_x = u_x/4u \mod \mathfrak{a}$, ce qui nous donne

$$\mathrm{NF}(u_{xy},C) = \frac{u_x\, u_y}{2u}.$$

◁

Calcul de la forme normale (cas où C n'est pas une présentation caractéristique) Dans ce cas, les initiaux de C ne sont pas, a priori, des éléments de $K[N]$. La méthode exposée précédemment ne peut donc pas s'appliquer directement. Une méthode simple est de se ramener au cas précédent en transformant C en présentation caractéristique (en appliquant, par exemple, l'algorithme regCaractéristique exposé dans le chapitre 4).

2.7 Solutions d'idéaux différentiels

On s'intéresse maintenant aux solutions des idéaux différentiels. Nous verrons que l'on peut en donner plusieurs définitions équivalentes et plus ou moins intuitives. Nous étudierons ensuite le problème de l'existence et de l'unicité de solutions.

Nous formulons les définitions de solutions dans l'anneau $\mathbb{Q}\{U\}$ (U désigne l'ensemble des indéterminées différentielles). Cela est suffisant d'un point de vue pratique. Toutefois, les définitions de solutions se généralisent pour un anneau $k\{U\}$ (où k est un corps différentiel quelconque), mais cela est moins intéressant en pratique.

La première notion de solution présentée est celle de zéro d'un idéal. Ces zéros seront appelés solutions abstraites. La définition est différente du cas algébrique car l'ensemble des dérivées est infinie (ce qui justifie l'utilisation de la fonction ϕ).

Définition 7 (Zéro ou solution abstraite d'un idéal différentiel) *Soit un idéal $\mathfrak{a}$ de $\mathbb{Q}\{U\}$. Soit une fonction $\phi : \Theta U \to \mathbb{C}$. Cette fonction se prolonge de manière unique en un morphisme (qu'on ne suppose pas différentiel) d'anneau de $\mathbb{Q}\{U\}$ dans $\mathbb{C}$, qu'on appelle également ϕ.*

On dit que ϕ est un zéro (ou solution abstraite) de $\mathfrak{a}$ si pour tout p de $\mathfrak{a}$, $\phi(p) = 0$

Informellement, cela revient à attribuer des valeurs aux dérivées de ΘU qui annulent les polynômes de $\mathfrak{a}$. On peut énoncer le théorème des zéros adapté au cas différentiel :

Théorème 10 (Théorème des zéros) *Soit Σ un système de polynômes différentiels de $\mathbb{Q}\{U\}$. Pour tout polynôme différentiel p, on a $p \in \sqrt{[\Sigma]}$* ssi *toute solution de Σ est solution de p. En particulier, Σ est sans solutions si et seulement si $1 \in \sqrt{[\Sigma]}$.*

La deuxième notion de solution consiste à voir les indéterminées de U comme des fonctions. Nous pourrions considérer des fonctions quelconques qui annulent tous les polynômes de $\mathfrak{a}$; toutefois, les ensembles triangulaires différentiels permettent seulement de déterminer la valeur des dérivées des fonctions solutions en un point. Ainsi, nous considérons uniquement des solutions données par des séries formelles (dont l'étude est détaillée dans le chapitre 3).

Définition 8 (Série formelle) *On appelle série formelle en $x_1, \ldots, x_m$ centrée au point $x^0 = (x_1^0, \ldots, x_m^0)$ et à coefficients dans $\mathbb{C}$ la somme*

$$S = \sum_{\alpha \in \mathbb{N}^m} c_\alpha (x - x^0)^\alpha$$

où :

- *$c_\alpha \in \mathbb{C}$ et $x^0 \in \mathbb{C}^m$;*

- $\alpha = (\alpha_1, \ldots, \alpha_m)$;
- $(x - x^0)^\alpha = (x_1 - x_1^0)^{\alpha_1} \cdots (x_m - x_m^0)^{\alpha_m}$.

L'ensemble de ces séries formelles est noté $\mathbb{C}[[x - x^0]]$.

Les séries formelles peuvent être vues comme des développements de Taylor infinis, de la convergence desquels on ne se soucie pas. On munit facilement $\mathbb{C}[[x - x^0]]$ d'une structure d'anneau. On fait ensuite agir les dérivations δ_1, ..., δ_m sur $\mathbb{C}[[x - x^0]]$ en posant, pour $1 \leq i \leq m$ et $1 \leq j \leq m$, $\delta_i x_j = 1$ si $i = j$ et 0 sinon.

On peut alors définir la solution en série formelle d'un système.

Définition 9 (Solution en série formelle d'un idéal) *Soit un idéal* $\mathfrak{a}$ *de* $\mathbb{Q}\{U\}$. *Soient un point* x^0 *de* $\mathbb{C}^m$ *et un n-uplet* $\overline{u} = (\overline{u}_1, \ldots, \overline{u}_n)$ *de séries formelles centrées en* x^0.

Soit ψ *l'application :* $U \to \mathbb{C}[[x - x^0]]$ *qui à* u_i *associe* $\overline{u}_i$. *Cette application se prolonge, de manière unique, en un morphisme d'anneau différentiel de* $\mathbb{Q}\{U\}$ *dans* $\mathbb{C}[[x - x^0]]$.

On dit que $\overline{u}$ *est solution du système si pour tout polynôme* p *de* $\mathfrak{a}$, *on a* $\psi(p) = 0$ *(i.e.* $\psi(p)$ *est la série formelle nulle).*

Informellement, cela signifie que chaque polynôme de $\mathfrak{a}$ donne la série formelle nulle quand on l'évalue sur les $\overline{u}_i$.

Ces deux notions de solutions sont en fait équivalentes dans le sens où une solution abstraite peut se convertir en solution en série formelle et inversement. La première partie du lemme suivant apparaît à la page 160 de [61]. La deuxième partie est quant à elle immédiate.

Lemme 6 *Soit* $\mathfrak{a}$ *un idéal différentiel. Soit* ϕ *une solution abstraite de ce système. On peut construire à partir de* ϕ *une solution en série formelle au point* x^0 *de la façon suivante :*

$$\overline{u}_i = \sum_{\alpha \in \mathbb{N}^m} \phi(\theta u_i) \frac{(x - x^0)^\alpha}{\alpha!}$$

où $\alpha = (\alpha_1, \ldots, \alpha_m)$, $\theta = \delta_1^{\alpha_1} \cdots \delta_m^{\alpha_m}$ *et* $\alpha! = \alpha_1! \cdots \alpha_m!$.

Inversement, toute solution en série formelle $\overline{u} = \{\overline{u}_1, \ldots, \overline{u}_n\}$ *au point d'expansion* x^0 *se convertit en une solution abstraite* ϕ *de la manière suivante :*

- *pour tout* θu_i *de* ΘU, $\phi(\theta u_i) = (\theta \overline{u}_i)(x^0)$.

Voici une illustration de la première partie de ce lemme, à savoir la conversion d'une solution abstraite en solution en série formelle.

Exemple ▷ Soit l'idéal $\mathfrak{a} = [u_x^2 - 4\,u]$ et soit ϕ une solution abstraite de $\mathfrak{a}$ (l'idéal $\mathfrak{a}$ admet des solutions, par exemple $\phi(v) = 2$ si $v = u_{xx}$ et 0 sinon).

On construit la série formelle à l'origine :

$$\overline{u} = \phi(u) + \phi(u_x)\, x + \phi(u_{xx})\, \frac{x^2}{2!} + \cdots$$

Pour alléger l'écriture, on note $\widetilde{u_{x^i}}$ au lieu de $\phi(u_{x^i})$. Il faut prouver que tout polynôme de $\mathfrak{a}$ s'annule si on l'évalue sur $\overline{u}$. Voyons ce qui produit sur le polynôme $p = u_x^2 - 4\,u$.

$$\begin{aligned}
p(\overline{u}) &= \overline{u}_x^2 - 4\overline{u} \\
&= (\widetilde{u_x} + \widetilde{u_{xx}}\, x + \widetilde{u_{xxx}}\frac{x^2}{2} + \cdots)^2 - 4(\widetilde{u} + \widetilde{u_x}\, x + \widetilde{u_{xx}}\,\frac{x^2}{2!} + \cdots) \\
&= \widetilde{u_x}^2 + 2\widetilde{u_x}\,\widetilde{u_{xx}}\, x + (\widetilde{u_{xx}}^2 + \widetilde{u_x}\,\widetilde{u_{xxx}})x^2 + \cdots - 4(\widetilde{u} + \widetilde{u_x}\, x + \widetilde{u_{xx}}\,\frac{x^2}{2!} + \cdots) \\
&= \underbrace{(\widetilde{u_x}^2 - 4\,\widetilde{u})}_{\phi(p)} + \underbrace{(2\widetilde{u_x}\,\widetilde{u_{xx}} - 4\widetilde{u_x})}_{\phi(\delta_x p)}\, x + \underbrace{(\widetilde{u_{xx}}^2 + \widetilde{u_x}\,\widetilde{u_{xxx}} - 2\widetilde{u_{xx}})}_{\phi(\delta_x^2 p)}\,\frac{x^2}{2!} + \cdots
\end{aligned}$$

On montre, par un calcul un peu technique, que le coefficient de $\frac{x^n}{n!}$ vaut $\phi(\delta_x^n p)$. Comme ϕ est une solution, tous les coefficients de la série formelle $p(\overline{u})$ sont nuls. Ainsi, $\overline{u}$ est bien une solution en série formelle à l'origine. $\triangleleft$

Déterminer les solutions d'un idéal quelconque est un problème ardu. Si l'on se restreint aux idéaux différentiels réguliers, on dispose de mécanismes intéressants permettant de décrire les solutions.

2.7.1 Solutions d'idéaux différentiels réguliers

On s'intéresse dans cette section aux solutions de l'idéal $[A] : S^\infty$ où $A = 0$, $S \neq 0$ est un système différentiel régulier. Sous cette hypothèse, on dispose du lemme de Rosenfeld qui permet de ramener la recherche d'une solution différentielle à un simple problème algébrique. Toutefois, ce lemme ne s'applique pas à toutes les solutions de $[A] : S^\infty$ mais seulement à celles n'annulant pas les polynômes de S. De telles solutions seront dites solutions du système $A = 0$, $S \neq 0$.

Bien évidemment, tous les résultats qui suivent s'appliquent également aux chaînes différentielles régulières car celles-ci sont, en particulier, des systèmes différentiels réguliers.

Lemme 7 (Reformulation du lemme de Rosenfeld) *Soit un système différentiel régulier $A = 0$, $S \neq 0$ de $\mathbb{Q}\{U\}$. Soit L l'ensemble des dérivées dominantes de A et N l'ensemble des dérivées sous l'escalier.*

- *le système $A = 0$, $S \neq 0$, vu comme un système de $\mathbb{Q}[N \cup L]$, admet une solution algébrique si et seulement si le système $A = 0$, $S \neq 0$ admet une solution différentielle ;*
- *toute solution algébrique de $A = 0$, $S \neq 0$, vu comme système de $\mathbb{Q}[N \cup L]$, se prolonge de manière unique en une solution différentielle de $A = 0$, $S \neq 0$.*

Informellement, ce lemme signifie la chose suivante. Si l'on fixe des valeurs des dérivées de $N \cup L$ qui vérifient $A = 0$, $S \neq 0$, alors on détermine de manière unique une solution différentielle de $A = 0$, $S \neq 0$.

Voici une application pratique de ce lemme :

Exemple ▷ Dans l'exemple qui suit, on a $U = \{u,v\}$ et $\Theta = \{\delta_x,\delta_y\}$. On considère le système différentiel régulier suivant :

$$A \begin{cases} v_{xx} - u_x \\ 4v_y u + u_x u_y - u_x u_y u \\ u_x^2 - 4u \\ u_y^2 - 2u \end{cases} \qquad S = \{4u, 2u_x, 2u_y\}$$

On recherche une solution en série formelle à l'origine. L'ensemble des dérivées dominantes est $L = \{u_x,u_y,v_y,v_{xx}\}$ et les dérivées sont l'escalier de L sont $N = \{u,v,v_x\}$.

On voit le système $A = 0$, $S \neq 0$ comme un système algébrique de $K[N \cup L]$.

$$A = 0,\ S \neq 0 \begin{cases} v_{xx}(0,0) - u_x(0,0) = 0 \\ 4v_y(0,0)u(0,0) + u_x(0,0)u_y(0,0) - u_x(0,0)u_y(0,0)u(0,0) = 0 \\ u_x(0,0)^2 - 4u(0,0) = 0 \\ u_y(0,0)^2 - 2u(0,0) = 0 \\ 4u(0,0) \neq 0 \\ 2u_x(0,0) \neq 0 \\ 2u_y(0,0) \neq 0 \end{cases}$$

Ce système se résout simplement car le lemme de Lazard s'applique. On sait en effet qu'on peut prendre les conditions initiales associées aux dérivées sous l'escalier comme constantes arbitraires :

$$u(0,0) = c_0, \quad v(0,0) = c_1, \quad v_x(0,0) = c_2.$$

En notant $u_x(0,0) = c_3$ et $u_y(0,0) = c_4$ on obtient les conditions :

$$c_3^2 = 4\,c_0, \quad c_4^2 = 2\,c_0.$$

Les inéquations se résument en $c_0 \neq 0$.

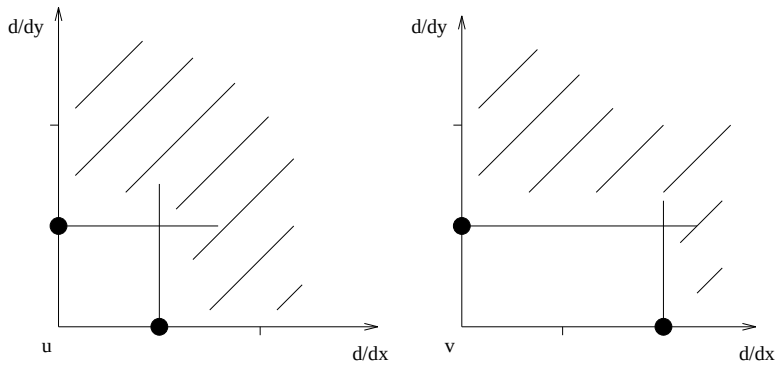


FIG. 2.2 – *Escalier des dérivées dominantes*

On peut alors calculer les valeurs des dérivées manquantes, c'est–à–dire les dérivées des zones hachurées de la figure 2.2. Raisonnons sur l'indéterminée u. Soit θu une dérivée

de la zone hachurée du diagramme de u. Pour déterminer θu, il suffit de réduire cette dérivée grâce à l'algorithme de réduction partielle en une fraction

$$\theta u \to \frac{r}{h}$$

puis d'évaluer la fraction sur les conditions initiales déjà calculées.

$$\theta u(0,0) = \frac{r(0,0)}{h(0,0)}$$

Le dénominateur est non nul puisqu'il est égal à un produit de puissances de séparants d'éléments de A.

Remarquer que la fraction r/h n'est pas définie de façon unique mais que sa valeur en les conditions initiales l'est : si θu se réécrit en une autre fraction r'/h' alors on a, en posant $q = r\,h' - r'h$, $q \in (A_w)$ où w est une dérivée strictement inférieure à θu. Si on a déterminé la valeur en zéro des dérivées inférieures à w par le mécanisme précédent, les polynômes de A_w s'annulent sur les conditions initiales. Ainsi, on obtient alors 0 si on évalue q sur les conditions initiales ce qui implique $r(0,0)/h(0,0) = r'(0,0)/h'(0,0)$.

On peut également calculer la valeur de $\theta u(0,0)$ en calculant la forme normale p/q de θu par rapport à C. On pose alors $\theta u(0,0) = p(0,0)/q(0,0)$. ◁

2.7.2 Cas des systèmes différentiels réguliers de $\mathbb{Q}[x]\{U\}$

On s'intéresse aux solutions d'un système différentiel régulier $A = 0$, $S \neq 0$ de $\mathbb{Q}[x]\{U\}$, où $x = \{x_1, \ldots, x_m\}$ et $\Theta = \{\theta_1, \ldots, \theta_m\}$. On suppose de plus que, pour $1 \leq i \leq m$ et $1 \leq j \leq m$, on a $\theta_i x_j = 1$ si $i = j$ et 0 sinon.

On se ramène à un nouveau système différentiel régulier $A' = 0$, $S' \neq 0$ de $\mathbb{Q}\{U \cup X\}$ où $X = \{X_1, \ldots, X_m\}$ est un ensemble de m nouvelles indéterminées différentielles. On obtient ce nouveau système de la manière suivante :

- $A' = \{A$ où chaque x_i est remplacé par $X_i\} \cup \{\theta_i X_j = 1$ si $i = j$ et 0 sinon$\}$;
- $S' = \{S$ où chaque x_i est remplacé par $X_i\}$.

Nous illustrons cette méthode sur un exemple.

Exemple ▷ Soit $U = \{u\}$ et $\Theta = \{\delta_x\}$. On munit l'anneau de polynômes $\mathbb{Q}[x]$ de la dérivation δ_x de telle manière que $\delta_x x = 1$ et $\delta_x r = 0$ pour tout r de $\mathbb{Q}$. On travaille dans l'anneau $R = \mathbb{Q}[x]\{u\}$. Pour simplifier la notation, on note la dérivation en indice, i.e. $\delta_x u$ est noté u_x. On considère le système différentiel régulier $A = 0$, $S \neq 0$ où $A = \{u_x - x\}$, $S = \emptyset$.

On introduit une nouvelle indéterminée X. On construit alors le système différentiel régulier $A' = 0$, $S' \neq 0$ avec $S' = \emptyset$ et

$$A' \left\{ \begin{array}{rcl} u_x - X & = & 0 \\ X_x & = & 1 \end{array} \right.$$

On obtient donc un système différentiel régulier de $\mathbb{Q}\{u,X\}$ dont on peut étudier la solution en série formelle en $x = 0$. On applique le lemme 7 : si l'on fixe les valeurs de $u(0)$ et $X(0)$, on détermine une unique solution en série formelle donnée par :

$$\begin{aligned} \overline{X} &= X(0) + X_x(0)\, x + \cdots \\ &= X(0) + x \end{aligned}$$

$$\begin{aligned} \overline{u} &= u(0) + u_x(0)\, x + u_{xx}(0)\frac{x^2}{2} + \cdots \\ &= u(0) + X(0)x + X_x(0)\frac{x^2}{2} \\ &= u(0) + X(0)x + \frac{x^2}{2} \end{aligned}$$

On réinterprète $\overline{u}$ comme une série formelle en X au point d'expansion $X(0)$ en remplaçant x par $X - X(0)$ et en renommant $u(0)$ en $u(X_0)$.

$$\overline{u} = u(X_0) + X_0(X - X_0) + \frac{(X - X_0)^2}{2}$$

Pour terminer, on renomme X_0 en x_0 et X en x et on obtient :

$$\overline{u} = u(x_0) + x_0(x - x_0) + \frac{(x - x_0)^2}{2}$$

qui est la solution en série formelle au point x_0 de $u_x - x = 0$. ◁

2.7.3 Solutions de $[A] : S^\infty$ et de $A = 0,\ S \neq 0$

Le lemme de Rosenfeld ne traite pas toutes les solutions de $[A] : S^\infty$ mais seulement celles n'annulant pas S. Ainsi, certaines solutions ne sont pas obtenues par le lemme de Rosenfeld.

Exemple ▷ Soit $A = \{u_x^2 - 4\,u\}$, $S = \{u_x\}$. C'est un système différentiel régulier. Plaçons nous à l'origine. Le polynôme $u(x) = x^2$ n'est pas solution de $A = 0$, $S \neq 0$ car à l'origine, le séparant $u_x(x) = 2\,x$ s'annule.

Toutefois, on montre que $u(x) = x^2$ est solution de l'idéal $[A] : S^\infty$. ◁

De plus, l'hypothèse de non annulation des inéquations est une condition suffisante qui dans certains cas n'est pas nécessaire. Si l'on poursuit l'exemple précédent :

Exemple ▷ Il existe une et une seule solution de $[A] : S^\infty$ vérifiant $u(0) = u_x(0) = 0$. En effet, l'idéal $[A] : S^\infty$ contient le polynôme $u_{xx} - 2$ qui implique $u_{xx}(0) = 2$ et $u_{x^k}(0) = 0$ pour $k > 2$. On retrouve la solution $u(x) = x^2$. ◁

À notre connaissance, il n'existe pas de théorème qui généralise le lemme de Rosenfeld à des conditions initiales annulant S.

2.8 Algorithmes de décomposition en algèbre différentielle

L'algorithme Rosenfeld–Gröbner est un simplificateur de systèmes d'équations différentielles (détaillé dans [5, 7, 8]). L'algorithme Rosenfeld–Gröbner calcule un nombre fini d'ensembles $C_1, \ldots, C_t$ tels que :

$$\sqrt{[\Sigma]} = [C_1] : {H_{C_1}}^{\infty} \cap \cdots \cap [C_t] : {H_{C_t}}^{\infty}.$$

De plus, chaque C_i est une présentation caractéristique de $[C_i] : {H_{C_i}}^{\infty}$ (pour la définition de [8]).

D'autres algorithmes existent. Initialement, Ritt a proposé, dans [52], un algorithme de décomposition reposant sur des factorisations au dessus de tours d'extensions algébriques. Wu Wen Tsün a décrit dans [65] une variante de l'algorithme de Ritt, sans factorisations, mais fournissant un résultat plus faible. Par exemple, l'algorithme de Wu ne décide pas du vide (i.e. ne détecte pas les systèmes sans solutions). Ziming Li et Dongming Wang développent dans [34] un algorithme proche de Rosenfeld–Gröbner basé sur les algorithmes de Ritt-Wu [65] et de Seidenberg [60].

Des travaux ont étendu les bases de Gröbner au cas différentiel. Ollivier [44] et Carra-Ferro [14] ont généralisé l'algorithme de Buchberger pour calculer des bases de Gröbner différentielles. Leurs bases de Gröbner différentielles ont toutefois l'inconvénient d'être infinies dans certains cas.

Mansfield [38] donne une définition différente des bases de Gröbner différentielles. Elle propose un algorithme (basé sur des calculs de pseudo–réductions) qui se termine dans tous les cas mais qui ne garantit pas que le résultat calculé soit une base de Gröbner différentielle. Toutefois, cet algorithme traite des problèmes concrets et permet même d'exprimer, sur certains systèmes, la forme générale des solutions [37].

Bouziane, Kandri Rody et Maârouf [12, 36] ont mis au point un algorithme dont la spécification est très proche de celle de Rosenfeld–Gröbner. Cet algorithme utilise des techniques algébriques basées sur des calculs d'inverses algébriques utilisant l'algorithme de Kalkbrener.

Hubert [23] a proposé une variante d'un algorithme de Ritt (dont certaines parties n'étaient pas effectives) en s'appuyant sur le lemme de Lazard et la remontée de ce même lemme.

Sadik [58] a rédigé une description très synthétique des algorithmes [7, 12, 8, 23] entièrement fondée sur [28]. Sadik [57] fournit également une borne sur l'ordre des polynômes (l'ordre d'un polynôme p est le maximum des ordres des dérivées figurant dans p) d'un ensemble caractéristique d'un idéal premier (pour un classement d'élimination).

Pour finir, on peut citer les travaux de Boulton, Lin, Reid, Rust et Wittkopf [50, 49, 56]. Leur approche est plus orientée géométrie différentielle. L'avantage de cette méthode et qu'on l'on s'intéresse aux propriétés des systèmes indépendamment du système de coordonnées dans lequel est exprimé le système. De plus, les équations traitées peuvent être des fonctions analytiques et non des simples polynômes.

L'algorithme Rif[11] (Reduced Involutive Form) met en pratique ces idées. Toutefois,

11. maintenu par Allan Wittkopf

cet algorithme utilise tout de même des techniques d'algèbre différentielle (classement, élimination). Selon Reid, Wittkopf et Boulton [49, page 4], les deux approches (géométrie différentielle et algèbre différentielle) sont intéressantes et les obstacles pour rendre les algorithmes effectifs pour chacune de ces approches sont liés. Parmi les fonctionnalités de l'algorithme Rif, on peut citer : la mise sous forme involutive d'un système différentiel non linéaire polynomial, la détermination des conditions initiales dont dépendent les solutions et le calcul effectif des coefficients de Taylor d'un solution pour des conditions initiales fixées.

2.9 L'algorithme Rosenfeld–Gröbner

L'algorithme Rosenfeld–Gröbner traite un système Σ en procédant en deux phases :

- on calcule t' systèmes différentiels réguliers $A_1 = 0,\ S_1 \neq 0,\ \ldots,\ A_{t'} = 0,\ S_{t'} \neq 0$ tels que :
$$\sqrt{[\Sigma]} = [A_1] : {S_1}^\infty \cap \cdots \cap [A_{t'}] : {S_{t'}}^\infty$$
Il est à noter que t' peut être nul. Dans ce cas, l'idéal $\sqrt{[\Sigma]}$ est égal à l'anneau différentiel R tout entier.
- on transforme chaque système régulier $A = 0,\ S \neq 0$ obtenu précédemment, en t'' présentations caractéristiques $C_1, \ldots, C_{t''}$ telles que :
$$[A] : S^\infty = [C_1] : {H_{C_1}}^\infty \cap \cdots \cap [C_{t''}] : {H_{C_{t''}}}^\infty$$
Si t'' vaut 0, cela signifie que $[A] : S^\infty$ est égal à R tout entier.

La deuxième phase peut se réaliser uniquement par des opérations algébriques. Ce résultat a été avancé (sans preuves) dans [8, page 35]. Les premières preuves complètes de ce résultat sont données dans [23].

2.9.1 Première phase

Cette phase différentielle est décrite dans [5, 7, 8]. Nous ne la rappelons pas car la seconde phase nous intéresse davantage. La section 5.1 explique le fonctionnement de cette première phase dans un cas où les scindages peuvent être évités. Cette version est un peu plus facile à comprendre car on ne construit qu'un seul système différentiel régulier.

2.9.2 Seconde phase

La phase algébrique est décrite dans [5, 7, 8]. Le plus élémentaire des traitements algébriques consiste à calculer une base de Gröbner B de l'idéal $(A) : S^\infty$. C'est ce qui est fait dans [5, 7]. Ce calcul ne fournit pas une présentation caractéristique de l'idéal. En pratique, on calcule une base de Gröbner $\overline{B}$ de l'idéal $S^{-1}(A)$ de l'anneau $S^{-1}R$ en appliquant l'algorithme de Buchberger à la famille

$$A \cup \{s\overline{s} - 1 \mid s \in S\}.$$

Chaque $\overline{s}$ désigne une nouvelle indéterminée codant l'inverse de s dans $S^{-1}R$. Si le classement choisi est un ordre qui élimine les $\overline{s}$ alors la base B de $(A) : S^\infty$ s'obtient en retirant de $\overline{B}$ tous les polynômes dans l'écriture desquels au moins un $\overline{s}$ apparaît.

fonction traitement_algébrique ($A = 0$, $S \neq 0$)
début
  Calculer une base de Gröbner $\overline{B}$ de l'idéal $S^{-1}(A)$
  si $1 \notin \overline{B}$ alors
    retourner $\{\overline{B}$ privé des polynômes contenant un $\overline{s}\}$
  sinon
    retourner l'ensemble vide
  fin si
fin

En posant X l'ensemble des dérivées figurant dans $A \cup S$, L l'ensemble des dérivées dominantes de A et $N = X \setminus L$, le calcul de base de Gröbner peut se faire dans l'anneau $K(N)[L]$. Cette méthode accélère considérablement les calculs et rend la base plus petite. Cette méthode se justifie par le lemme de Lazard qui assure que les éléments de $K[N]$ sont non diviseurs de zéro modulo $(A) : S^\infty$.

Le paquetage `diffalg` utilise cette technique. Nous verrons un algorithme regCaractéristique dans le chapitre 4 qui remplace les calculs de bases de Gröbner par des méthodes triangulaires.

Chapitre 3

Analycité des solutions

Sommaire

Nous nous intéressons dans ce chapitre à l'analycité des solutions en série formelle (pour des conditions initiales fixées) des systèmes différentiels réguliers. Ce problème peut avoir un intérêt pratique : si l'on sait qu'une solution est analytique en un point x^0, on peut, par des techniques numériques, en obtenir une bonne approximation au voisinage de x^0.

Ce problème a été traité par Kovalevskaya [30] (théorème de Cauchy-Kovalevskaya) dans le cas de systèmes particuliers à autant d'équations que d'inconnues, privilégiant une dérivation. Riquier a ensuite généralisé [51] le théorème de Cauchy-Kovalevskaya aux systèmes orthonomes passifs. Ces deux théorèmes concluent chacun (sous certaines hypothèses) que la solution d'un système différentiel est analytique. En outre, il faut que les équations du système soient analytiques et que les conditions initiales soient données par des fonctions analytiques.

Ce chapitre contient deux résultats nouveaux. Le premier est une nouvelle preuve du théorème d'analycité d'Ariane Péladan–Germa [45, page 34] qui prouve que la solution d'un système différentiel régulier[12] pour un classement de Riquier[13] de l'ordre total est analytique si les conditions initiales sont données par des fonctions analytiques. Ce théorème est différent du théorème d'analycité de Riquier car ce dernier ne s'applique pas aux systèmes différentiels réguliers mais aux systèmes orthonomes passifs. Le théorème 17 s'appuie sur le théorème 16 (page 69), qui fournit une nouvelle preuve du théorème d'analycité de Riquier. Un atout de cette preuve est qu'elle utilise un formalisme récent, ce qui en facilite la compréhension.

Le deuxième résultat est un contre-exemple à la conjecture suivante :

> si C est un système différentiel régulier (ou un système orthonome passif) pour un classement de l'ordre total et si les conditions initiales sont données par des fonctions analytiques, alors la solution en série formelle est analytique.

Le système suivant prouve que cette conjecture est fausse.

$$C \left\{ \begin{array}{rcl} u_{xx} & = & u_{xy} + u_{yy} + v \\ v_{yy} & = & v_{xy} + v_{xx} + u \end{array} \right.$$

$$\text{avec } u(0,y) = u_x(0,y) = e^y \text{ et } v(x,0) = v_y(x,0) = e^x$$

Ce système est un système différentiel régulier (et aussi un système orthonome passif) pour un classement de l'ordre total et ses conditions initiales sont analytiques. Toutefois, la solution de ce système *n'*est *pas* analytique.

On savait que l'hypothèse de classement de l'ordre total était importante grâce à l'exemple suivant (fourni par Sophie Kovalevskaya) dont la solution n'est pas analytique :

$$u_t(x,t) = u_{xx}(x,t)$$

$$u(x,0) = 1/(1-x)$$

12. ou la solution d'une chaîne différentielle régulière
13. les classements de Riquier sont définis dans ce chapitre

Les conditions initiales de ce système sont données pour un classement qui n'est pas de l'ordre total : en effet, d'après la condition initiale, u_t est nécessairement la dérivée dominante de l'équation. Les coefficients $u_{x^n}(0,0)$ de la solution valent $n!$. Ainsi, les coefficients $u_{t^n}(0,0)$ valent $(2n)!$. On montre (par le lemme d'Hadamard par exemple) que ces coefficients $u_{t^n}(0,0)$ croissent trop vite pour que la solution soit analytique.

Ce chapitre commence par énoncer le théorème d'analycité (pour les systèmes différentiels réguliers et les chaînes différentielles régulières). Sa preuve sera seulement donnée page 75 car de nombreux rappels sont nécessaires à son écriture.

Suivent la section de rappels 3.2 et la section 3.3 présentant des résultats sur l'évaluation d'une suite croissante de monômes ordonnés selon un ordre admissible (résultats utilisés dans la preuve d'analycité). La section 3.4 présente brièvement les travaux de Cauchy–Kovalevskaya, de Riquier et contient la preuve d'analycité pour les systèmes différentiels réguliers. La section 3.5 présente le contre-exemple à la conjecture citée précédemment. La section 3.6 détaille quelques différences entre la preuve du théorème 16 et la preuve, reformulée par Janet, du théorème d'analycité de Riquier. Le chapitre se termine par une mise en pratique de la preuve d'analycité sur des exemples simples.

Dans ce chapitre, X est l'ensemble $\{x_1,\ldots,x_m\}$ et $U=\{u_1,\ldots,u_n\}$ désigne l'ensemble des indéterminées différentielles. Le corps $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou le corps $\mathbb{C}$. Cette convention allège agréablement les notions valables aussi bien dans les réels que dans les complexes.

3.1 Théorème d'analycité

Voici l'énoncé du théorème d'analycité pour les systèmes différentiels réguliers, dont la preuve est donnée page 75. Nous définissons d'abord les classements de Riquier (dont l'étude est détaillée dans la section 3.2).

Classement de Riquier *On appelle classement de Riquier tout classement vérifiant :* $\theta_1 u_i < \theta_2 u_i \iff \theta_1 u_j < \theta_2 u_j$ *pour tous* $\theta_1,\theta_2 \in \Theta$, $1 \leq i,j \leq n$.

Théorème d'analycité *Soit* $A=0$, $S\neq 0$ *un système différentiel régulier de* $\mathbb{K}[X]\{U\}$ *pour un classement* $\mathcal{R}$ *de Riquier et de l'ordre total. Soit* $x^0=(x_1^0,\ldots,x_m^0)$ *un point d'expansion. On note* R_0 *l'anneau des polynômes réduits par rapport à* A.

On suppose que le système $A=0, S\neq 0$, *vu comme un système algébrique de* R_0, *admet une solution ; cette solution fixe donc des conditions initiales. Pour terminer, on suppose que ces conditions initiales sont données par des fonctions analytiques en* x^0, *ce qui signifie que les* n *séries formelles* $u_i^0 = \sum_{\theta u_i \in E_i} \frac{(\theta u_i)(x^0)}{\alpha_1!\cdots\alpha_m!}(x-x^0)^\alpha$ *(où* $\theta=\delta x_1^{\alpha_1}\cdots\delta x_m^{\alpha_m}$ *et* E_i *est l'ensemble des dérivées de* u_i *pour lesquelles on a fixé une valeur) ont un domaine de convergence non vide.*

Le problème admet alors une unique solution en série formelle analytique en x^0.

3.2 Rappels

Matrices

Définition 10 (Norme vectorielle) *Soit V un espace vectoriel sur $\mathbb{K}$. On appelle norme sur V toute application de V dans $\mathbb{R}$ vérifiant :*

- $||v|| \geq 0$ *pour tout* v *dans* V *et* $||v|| = 0 \iff v = 0$;
- $||\alpha\, v|| \leq |\alpha| \cdot ||v||$ *pour tout* v *de* V *et tout* α *de* $\mathbb{K}$;
- $||u + v|| \leq ||u|| + ||v||$ *pour tous* u *et* v *de* V.

Définition 11 (Norme matricielle) *On appelle norme matricielle toute application à valeurs dans $\mathbb{R}$ telle que (A et B désignent deux matrices carrées à coefficients dans $\mathbb{K}$):*

- $||A|| \geq 0$ *pour tout* A *et* $||A|| = 0 \iff A = 0$;
- $||\alpha A|| \leq |\alpha| \cdot ||A||$ *pour tout* A *et tout* α *de* $\mathbb{K}$;
- $||A + B|| \leq ||A|| + ||B||$ *pour tous* A *et* B ;
- $||A\, B|| \leq ||A|| \cdot ||B||$ *pour tous* A *et* B.

Définition 12 (Norme matricielle subordonnée) *Soit $||\cdot||$ une norme vectorielle sur l'espace vectoriel $\mathbb{C}^n$. Cette norme étant donnée, on peut construire une norme sur les matrices $n \times n$ à coefficients dans $\mathbb{C}$ de la manière suivante :*

$$||A|| = \sup_{v \in \mathbb{C}^n, v \neq 0} \frac{||Av||}{||v||}$$

Cette norme est appelée norme subordonnée (à la norme vectorielle $||\cdot||$).
Remarques :

- *on vérifie que l'on définit bien une norme matricielle (on pourra se reporter à [16, page 16]) ;*
- *on utilise la même notation $||\cdot||$ pour les vecteurs et les matrices.*

Les normes matricielles utilisées dans ce chapitre seront toutes subordonnées.

Exemple ▷ Voici deux normes couramment utilisées, les normes 1 et ∞ :

$$||A||_1 = \max_j \sum_i |a_{ij}|$$

$$||A||_\infty = \max_i \sum_j |a_{ij}|$$

◁

Définition 13 (Rayon spectral) *Soit A une matrice carrée à coefficients dans $\mathbb{K}$. On appelle rayon spectral de A, que l'on note $\rho(A)$, le maximum des modules des valeurs propres de A.*

Lemme 8 *Soit D une matrice carrée à coefficients dans $\mathbb{K}$ et $\rho(D)$ son rayon spectral. Les assertions suivantes sont équivalentes :*

P1 $\rho(D) < 1$;

P2 $||D|| < 1$ *pour au moins une norme matricielle subordonnée* $||\cdot||$.

Preuve :
Voir [16, théorème 1.5-1 page 21] □

Lemme 9 *Soient D une matrice carrée à coefficients dans $\mathbb{K}$ et $||\cdot||$ une norme matricielle subordonnée. Si $||D|| < 1$, alors la matrice $I - D$ est inversible et son inverse est $\sum_{k=0}^{\infty} D^k$*

Preuve :
Voir [16, Théorème 1.4-5 page 20] □

Séries formelles et fonctions analytiques

La définition de série formelle a déjà été introduite dans le chapitre 2. Nous la rappelons néanmoins.

Définition 14 (Série formelle) *Soient un m-uplet $x^0 = (x_1^0, \ldots, x_m^0)$ de $\mathbb{K}^m$ et m indéterminées $x_1, \ldots, x_m$.*

On appelle série formelle en $x_1, \ldots, x_m$ à valeurs dans $\mathbb{K}$ et centrée en x^0 la somme infinie $S = \sum_{\alpha \in \mathbb{N}^m} c_\alpha (x - x^0)^\alpha$ où

- $c_\alpha \in \mathbb{K}^m$;
- $(x - x^0)^\alpha = (x_1 - x_1^0)^{\alpha_1} \cdots (x_m - x_m^0)^{\alpha_m}$ *où* $\alpha = (\alpha_1, \ldots, \alpha_m)$.

L'ensemble de ces séries formelles est noté $\mathbb{K}[[x - x^0]]$.

Définition 15 (Série formelle majorante) *Soient deux séries formelles S et s données par $S = \sum_{\alpha \in \mathbb{N}^m} C_\alpha (x - x^0)^\alpha$ et $s = \sum_{\alpha \in \mathbb{N}^m} c_\alpha (x - x^0)^\alpha$. On dit que S majore s si :*

- *S est une série formelle à coefficients réels positifs ;*
- *pour tout α de $\mathbb{N}^m$, on a $|c_\alpha| \leq C_\alpha$.*

Exemple ▷ La série formelle (qui ici est un polynôme) $1 - x - 2\,x^2 + 4\,x^3$ est majorée par la série $\frac{4}{1-x} = 4 + 4\,x + 4\,x^2 + \cdots$ ◁

La définition qui suit généralise la dérivée des polynômes aux séries formelles.

Définition 16 (Dérivation d'une série formelle) *Soit S une série formelle égale à $\sum_{\alpha \in \mathbb{N}^m} c_\alpha (x - x^0)^\alpha$. La dérivée de S par rapport à x_i, notée $\delta_{x_i} S$ est définie par :*

$$\delta_{x_i} S = \sum_{(\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m} (\alpha_i + 1) c_{\alpha_1, \ldots, \alpha_i + 1, \ldots, \alpha_m} (x - x^0)^\alpha$$

Propriété 10 *Si la série S majore s, alors pour tout i, $\delta_{x_i} S$ majore aussi $\delta_{x_i} s$.*

Preuve :
Immédiat. □

Définition 17 (Domaine de convergence d'une série formelle) *Soit S la série formelle en $x_1,\ldots,x_m$ donnée par $S = \sum_{\alpha\in\mathbb{N}^m} c_\alpha (x-x^0)^\alpha$.*

On appelle domaine de convergence de S, que l'on note $\Delta(S)$, l'ensemble des m-uplets de $\mathbb{C}$ pour lesquels la série S est absolument convergente, c'est–à–dire :

$\Delta(S) = \{z = (z_1,\ldots,z_m) \in \mathbb{C}^m \mid \sum_{\alpha\in\mathbb{N}^m} |c_\alpha z^\alpha| \text{ est convergente}\}$

Exemple ▷ La série d'une variable complexe z, $S(z) = \frac{1}{1-z} = 1 + z + z^2 + \cdots$ admet pour domaine de convergence le disque ouvert de rayon 1 i.e. $\Delta(S) = \{z \in \mathbb{C}/|z| < 1\}$ ◁

Propriété 11 (Domaine de convergence d'une série majorée) *Si la série formelle $S = \sum_{\alpha\in\mathbb{N}^m} C_\alpha (x-x^0)^\alpha$ majore la série formelle $s = \sum_{\alpha\in\mathbb{N}^m} c_\alpha (x-x^0)^\alpha$, alors on a $\Delta(s) \supset \Delta(S)$.*

Preuve :
Si $z \in \Delta(S)$, la somme $\sum_{\alpha\in\mathbb{N}^m} |C_\alpha z^\alpha|$ est convergente ce qui implique que $\sum_{\alpha\in\mathbb{N}^m} |c_\alpha z^\alpha|$ est aussi convergente. On a donc $\Delta(s) \supset \Delta(S)$. □

Définition 18 (Fonction analytique en un point) *Soit f une fonction des variables $x_1,\ldots,x_m$, de $\mathbb{K}^m$ dans $\mathbb{K}$, définie dans un voisinage W d'un point x^0 de $\mathbb{K}^m$.*

On dit que f est analytique en x^0 (ou aussi développable en série entière au point x^0) s'il existe une série formelle S centrée en x^0 et un voisinage non vide $V \subset W$ de x^0 tels que :

- *le domaine de convergence de S contient V ;*
- *$f(x) = S(x)$ pour tout x de V.*

Définition 19 (Série de Taylor) *Soit f une fonction des variables $x_1,\ldots,x_m$, de $\mathbb{K}^m$ dans $\mathbb{K}$, définie dans un voisinage d'un point $x^0 = (x_1^0,\ldots,x_m^0)$.*

Si f est indéfiniment dérivable au point x^0, on associe à f la série formelle, appelée série de Taylor de f en x^0, $S = \sum_{\alpha\in\mathbb{N}^m} c_\alpha (x-x^0)^\alpha$ où :

$$c_{\alpha_1,\ldots,\alpha_m} = \frac{1}{\alpha_1!\cdots\alpha_m!} \frac{\partial f^{(\alpha_1+\cdots+\alpha_m)}}{\partial x_1^{\alpha_1}\cdots\partial x_m^{\alpha_m}}(x^0)$$

Exemple ▷ La fonction de deux variables complexes $f(z_1,z_2) = e^{z_1+z_2}$ est analytique à l'origine (i.e. en $z_1 = z_2 = 0$) et sa série de Taylor est :

$$S(z_1,z_2) = \sum_{(p,q)\in\mathbb{N}^2} \frac{z_1^p z_2^q}{p!\,q!}$$

◁

Propriété 12 *Si f est analytique en x^0, alors au voisinage de x_0 on a $f(x) = S(x)$, où S est la série de Taylor de f en x^0.*

Propriété 13 (Inverse d'une fonction analytique) *Soit f une fonction $\mathbb{K}^m$ dans $\mathbb{K}$ et un point $x^0 \in \mathbb{K}^m$. Si f est analytique en x^0 et si $f(x^0) \neq 0$, alors la fonction $1/f$ est analytique en x^0.*

Preuve :
On trouvera une preuve (limitée au cas d'une seule variable) dans [15, proposition 6.1, page 23]. □

Propriété 14 *Soit f une fonction analytique à l'origine. Soit S sa série de Taylor à l'origine. Soit s une série formelle majorée par S.*

Alors, s est convergente dans $\Delta(S)$ ce qui implique que la fonction $s(x)$ existe dans un voisinage de l'origine et qu'elle est analytique à l'origine. De plus, $\Delta(s) \supset \Delta(S)$.

Preuve :
Simple conséquence de la définition 18 et de la propriété 11. □

Le lemme qui suit est classique. Sa preuve est tirée de [46].

Lemme 10 *Toute série formelle $S = \sum_{\alpha \in \mathbb{N}^m} c_\alpha x^\alpha$ de domaine de convergence non vide peut être majorée par une série formelle de la forme*

$$F = \frac{M}{1 - \frac{x_1 + \cdots + x_m}{s}}$$

où M et s sont deux réels strictement positifs.
De plus, F est analytique à l'origine.

Preuve :
Soit $r = (r_1, \ldots, r_m)$ un m-uplet de réels strictement positifs tel que $\sum |c_\alpha| r^\alpha$ soit convergente (possible car S a un domaine de convergence non vide). Cette somme étant convergente, il existe un réel positif M tel que pour tout $\alpha \in \mathbb{N}^m$, $|c_\alpha| r^\alpha \leq M$.

Soit T la série formelle définie par $T = \dfrac{M}{(1 - \frac{x_1}{r_1}) \cdots (1 - \frac{x_m}{r_m})}$

En développant T avec la formule $M(1 + \frac{x_1}{r_1} + \left(\frac{x_1}{r_1}\right)^2 + \cdots) \cdots (1 + \frac{x_m}{r_m} + \left(\frac{x_m}{r_m}\right)^2 + \cdots)$, on voit que T s'écrit $\sum_{\alpha \in \mathbb{N}^m} t_\alpha x^\alpha$ avec $t_\alpha = M \frac{1}{r_1^{\alpha_1}} \cdots \frac{1}{r_m^{\alpha_m}}$.

De $|c_\alpha| r^\alpha \leq M$, on déduit $|c_\alpha| \leq \frac{M}{r^\alpha} = t_\alpha$. Ainsi S est majorée par T.

On pose alors $s = \min(r_1, \ldots, r_n)$ et $F = \dfrac{M}{1 - \frac{x_1 + \cdots + x_m}{s}}$. En développant F avec la formule $M(1 + \frac{x_1 + \cdots + x_m}{s} + \left(\frac{x_1 + \cdots + x_m}{s}\right)^2 + \cdots)$ et en développant les puissances entières avec la formule du binôme généralisée (calcul fastidieux sans difficulté), on constate que F majore T.

Par transitivité, F majore la série formelle S.

Comme la fonction $1 - \frac{x_1 + \cdots + x_m}{s}$ est analytique en 0 et qu'elle est non nulle en 0, en appliquant la propriété 13, F est analytique en 0. □

Remarque 1 *On peut également majorer p séries formelles S_i (chacune de domaine de convergence non vide) par une même série formelle de la forme* $F = \frac{M}{1-\frac{x_1+\cdots+x_m}{s}}$.

En effet, chaque série S_i peut se majorer par $\frac{M_i}{1-\frac{x_1+\cdots+x_m}{s_i}}$. *Il suffit ensuite de poser* $M = \max_{1\leq i\leq p}(M_i)$ *et* $s = \min_{1\leq i\leq p}(s_i)$

La propriété qui suit considère une série formelle à coefficients dans les matrices. La théorie des séries formelles à coefficients dans un anneau est un peu plus délicate en raison des diviseurs de zéro. Toutefois, la notion d'analyticité se généralise sans difficulté.

Propriété 15 *Soient $A(z)$ une fonction analytique à l'origine d'une variable complexe et à coefficients dans les matrices $n \times n$ de $\mathbb{C}$. On suppose $\rho(A(0)) < 1$.*

Alors la matrice $I - A(z)$ est inversible dans un voisinage de l'origine. De plus, la fonction $E(z) = \frac{1}{1-A(z)}$ est une fonction analytique à l'origine.

Preuve :

On $\rho(A(0)) < 1$. D'après le lemme 8, il existe une norme $||\cdot||$ matricielle telle que $||A(0)|| < 1$. Par continuité de la norme et par continuité de la fonction $A(z)$ (car une fonction analytique est continue), il existe un voisinage V de l'origine tel que $||A(z)|| < 1$ pour $z \in V$.

D'après le lemme 9, pour tout z de V, la matrice $I - A(z)$ est inversible et son inverse $E(z)$ est donnée par $E(z) = \sum_{k=0}^{\infty} A(z)^k$.

En notant $\widetilde{A}(z)$ la comatrice de $I - A(z)$ (i.e. la matrice de ses cofacteurs), on a la relation $(I-A(z))\widetilde{A}(z) = I\det(I-A(z))$. La comatrice $\widetilde{A}(z)$ est analytique à l'origine, car elle est composée de mineurs qui sont des sommes et produits de fonctions analytiques à l'origine. De même, la fonction déterminant $\det(I - A(z))$ est analytique à l'origine. Comme $\det(I - A(0)) \neq 0$ (car $I - A(0)$ est inversible), on sait, d'après la propriété 13, que $1/\det(I - A(z))$ est analytique à l'origine.

Par conséquent, il existe un voisinage ouvert $W \subset V$ de l'origine, tel que l'on ait $E(z) = \widetilde{A}(z)/\det(I - A(z))$, ce qui prouve que $E(z)$ est analytique à l'origine. □

Majoration des racines d'un polynôme

Lemme 11 *Soient un réel positif ϵ tel que $\epsilon < 1$ et un polynôme P à coefficients dans $\mathbb{C}$ de la forme $P(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ vérifiant $|a_i| \leq \epsilon/n$ pour $1 \leq i \leq n$.*

Si x_0 est racine de P, alors $|x_0|^n \leq \epsilon$:

Preuve :

Soit x_0 une racine de P. Le cas $x_0 = 0$ étant évident, on peut supposer $|x_0| > 0$.

$$P(x_0) = 0 \implies x_0^n = -a_1x_0^{n-1} - \cdots - a_{n-1}x_0 - a_n$$
$$\implies |x_0|^n \leq \epsilon/n(|x_0|^{n-1} + \cdots + |x_0| + 1) \quad \textbf{(I1)}$$

Si $|x_0| \geq 1$, l'inégalité **(I1)** fournit $|x_0|^n \leq \epsilon/n \times n|x_0|^{n-1}$ qui donne $|x_0| \leq \epsilon < 1$, ce qui est contradictoire. Par conséquent, on peut supposer $|x_0| < 1$.

L'inégalité **(I1)** fournit $|x_0|^n \leq \epsilon/n \times n \leq \epsilon$ □

Ordres admissibles

On considère, dans cette sous–section, l'alphabet $X = \{x_1, \ldots, x_m\}$ et l'ensemble Ω des monômes construits sur X. On rappelle qu'un monôme ω est un produit de puissances des x_i, qu'on écrit $\omega = x_1^{a_1} \cdots x_m^{a_m}$ où les a_i sont des entiers naturels. On appelle degré de ω, noté $\deg(\omega)$, la somme des exposants a_i.

Définition 20 (Ordre admissible) *On appelle ordre admissible sur les monômes de Ω toute relation d'ordre total sur Ω vérifiant pour tous monômes ω, ω' et ω'' :*

- $\omega \leq \omega\,\omega'$;
- $\omega \leq \omega' \implies \omega\,\omega'' \leq \omega'\,\omega''$.

Définition 21 *Un ordre admissible $\mathcal{O}$ est dit du degré total si* $\deg(\omega) < \deg(\omega')$ *implique $\omega < \omega'$ pour tous monômes ω et ω'.*

Le paragraphe et l'énoncé du théorème qui suivent sont essentiellement repris de l'article de Rust et Reid [48, page 2, the case n=1].

Les ordres admissibles ont été complètement classifiés par Robbiano dans [53] (voir également l'article de Weispfenning [64]). D'après Reid et Rust, le même problème avait, à peu de choses près, été résolu par Trevisan [62] et Zaĭceva [67]. À l'aide de la notation et de la définition suivantes, nous pouvons énoncer le théorème de classification des ordres admissibles.

Notation 1 *Pour tout monôme $\omega = x_1^{a_1} \cdots x_m^{a_m}$, on note $\Delta(\omega)$ le vecteur colonne à m composantes entières $(a_1, a_2, \ldots, a_m)^t$.*

Définition 22 *Soient deux vecteurs colonnes $a = (a_1, \ldots, a_m)^t$ et $b = (b_1, \ldots, b_m)^t$, on définit l'ordre lexicographique $<_{lex}$ de la manière suivante : $a <_{lex} b$ si la première valeur non nulle de la séquence $b_1 - a_1, \ldots, b_m - a_m$ est positive.*

L'ordre lexicographique est un ordre admissible.

Théorème 11 (Classification des ordres admissibles) *Soit M une matrice réelle de q lignes et m colonnes telle que l'application associée $a \to M\,a$ de $\mathbb{N}^m$ dans $\mathbb{R}^q$ soit injective et telle que les vecteurs colonnes soient supérieurs lexicographiquement au vecteur nul.*

On définit la relation $\leq_M$ sur les monômes de Ω par :

$$\omega \leq_M \omega' \iff M\Delta(\omega) \leq_{lex} M\Delta(\omega')$$

Alors $\leq_M$ définit un ordre admissible $\mathcal{O}$ sur Ω. On dit que l'ordre $\mathcal{O}$ est caractérisé par la matrice M.

De plus, pour tout ordre admissible $\mathcal{O}$, il existe un entier q et une matrice M à q lignes et m colonnes (telle que l'application associée $a \to M\,a$ de $\mathbb{N}^m$ dans $\mathbb{R}^q$ soit injective et telle que les vecteurs colonnes soient supérieurs lexicographiquement au vecteur nul) qui caractérise l'ordre $\mathcal{O}$. Cette matrice M n'est pas unique.

Cela signifie que tout ordre admissible se ramène, par la multiplication par une matrice, à un ordre lexicographique. Cela signifie aussi qu'un ordre admissible quelconque peut être décrit par un système de poids (donné par M) sur les indéterminées de X.

Exemple ▷ L'ordre admissible du degré total raffiné par l'ordre lexicographique pour $x_1 > x_2 > x_3$

$$1 < x_3 < x_2 < x_1 < x_3^2 < x_2\,x_3 < x_2^2 < x_1\,x_3 < x_1\,x_2 < x_1^2 < x_3^3 < \cdots$$

est caractérisé par la matrice :

$$M = \begin{array}{c} \begin{matrix} x_1 & x_2 & x_3 \end{matrix} \\ \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

En effet, la première ligne classe les monômes entre eux suivant leur degré. Si deux monômes ont même degré, les deuxième et troisième lignes les classent suivant l'ordre lexicographique pour $x_1 > x_2 > x_3$. ◁

Propriété 16 *Soit $\mathcal{O}$ un ordre admissible du degré total. Alors $\mathcal{O}$ peut être caractérisé par une matrice dont la première ligne est uniquement composée de 1.*

Preuve :

D'après le théorème 11, il existe une matrice M telle que :

$$\omega \leq \omega' \iff M\Delta(\omega) \leq_{lex} M\Delta(\omega')$$

Appelons $l_1 = (b_1, \ldots, b_m)$ la première ligne de M, que l'on peut supposer non nulle. On va montrer que les b_i pour $1 \leq i \leq m$ sont égaux.

Considérons le monôme x_i pour $1 \leq i \leq m$. Comme $\mathrm{ord}(x_i) = 1$ et $\mathrm{ord}(1) = 0$, on a $M\Delta(x_i) \geq_{lex} M\Delta(1)$ ce qui implique $l_1\Delta(x_i) \geq l_1\Delta(1)$ qui fournit $b_i \geq 0$.

Ainsi, les b_i sont tous positifs. La ligne l_1 étant supposée non nulle, au moins un des b_i est non nul. On peut supposer (en renommant les x_i) que b_1 est le maximum des b_i.

Nous allons maintenant prouver que si $2 \leq i \leq m$, le cas $b_i < b_1$ est impossible. Cela prouvera que tous les b_i sont égaux.

Soit $2 \leq i \leq m$ avec $b_i < b_1$. Il existe un entier n tel que $b_i(1 + \frac{1}{n}) < b_1$. De cette relation, on tire $(n+1)\,b_i < n\,b_1$ qui implique $x_i^{(n+1)} < x_1^n$. Ceci est impossible car $\mathcal{O}$ est un ordre du degré total.

Ainsi, tous les b_i sont strictement positifs et tous égaux. En remplaçant dans M les b_i par 1, on obtient encore une matrice caractérisant l'ordre $\mathcal{O}$. □

Classement de Riquier

Le classement de Riquier est un cas particulier du classement général défini par Kolchin. Dans ses ouvrages, Riquier définit un tel classement en attribuant un système de

poids aux dérivations et aux indéterminées différentielles. Initialement, Riquier imposait aux poids d'être entiers ; de nos jours, les poids sont supposés réels.

On peut également définir les classements de Riquier par la définition équivalente suivante[14] due à Caboara et Silvestri [13].

Définition 23 (Classement de Riquier) *On appelle classement de Riquier tout classement vérifiant :* $\theta_1 u_i < \theta_2 u_i \iff \theta_1 u_j < \theta_2 u_j$ *pour tous* $\theta_1,\theta_2 \in \Theta$, $1 \leq i,j \leq n$.

Ainsi, la façon dont les dérivées d'une même indéterminée différentielle sont ordonnées entre elles, ne dépend pas de l'indéterminée elle même.

Exemple ▷ Voici le début d'un classement de Riquier :

$$u < u_x < u_y < u_{xx} < u_{xy} < v_{yy} < \cdots < v < v_x < v_y < v_{xx} < v_{xy} < v_{yy} \cdots$$

◁

Un classement de Riquier peut être caractérisé par une matrice (contrairement aux classements généraux qui nécessitent un mécanisme complexe mettant en œuvre plusieurs matrices, voir [48]). Le procédé est très proche de celui des ordres admissibles.

Notation 2 *Pour toute dérivée* θu_i *où* $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$, *on note* $\Delta(\theta u_i)$ *le vecteur à* $m+n$ *composantes entières* $(a_1,a_2,\ldots,a_m,0,\ldots,0,\overset{(m+i)}{1},0,\ldots,0)$.

Théorème 12 (Classification des classements de Riquier) *Soit une matrice réelle* M *de* q *lignes et* $m+n$ *colonnes. On suppose les vecteurs colonnes supérieurs lexicographiquement au vecteur nul.*

On définit l'ordre $\leq_M$ *sur les dérivées par* $v \leq_M w \iff M\Delta(v) \leq_{lex} M\Delta(w)$ *pour toutes dérivées* v *et* w.

Si l'ordre $\leq_M$ *est total, alors* $\leq_M$ *définit un classement de Riquier* $\mathcal{R}$ *sur* ΘU. *On dit alors que le classement* $\mathcal{R}$ *est caractérisé par la matrice* M.

De plus, pour tout classement de Riquier $\mathcal{R}$, *il existe un entier* q *et une matrice* M *à* q *lignes et* $m+n$ *colonnes qui caractérise le classement* $\mathcal{R}$, *les vecteurs colonnes étant supérieurs lexicographiquement au vecteur nul. Cette matrice* M *n'est pas unique.*

Remarque : contrairement au théorème de classification des ordres admissibles, l'application associée $a \to M\,a$ de $\mathbb{N}^{m+n}$ dans $\mathbb{R}^q$ n'est pas nécessairement injective. Cela vient de la forme particulière des vecteurs $\Delta(\theta u_i)$. Ainsi, dans chacun des deux exemples suivants, l'application $a \to M\,a$ de $\mathbb{N}^4$ dans $\mathbb{R}^3$ n'est pas injective car la dernière colonne est nulle. Toutefois, dans chacun des exemples, M définit bien un classement de Riquier.

Exemple ▷ Soit $X = \{x,y\}$ et $U = \{u,v\}$.

$$M = \begin{array}{c} \begin{array}{cccc} x & y & u & v \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

14. On trouvera une ébauche de preuve de cette équivalence dans [13] et une preuve complète dans [48].

La première ligne de la matrice implique que toute dérivée de u est supérieure à toute dérivée de v. Les deux autres lignes définissent un classement de l'ordre total raffiné par l'ordre lexicographique $x > y$.

$$\cdots > u_{xx} > u_{xy} > u_{yy} > u_x > u_y > u > \cdots > v_{xx} > v_{xy} > v_{yy} > v_x > v_y > v$$

◁

Exemple ▷ Soit $X = \{x,y\}$ et $U = \{u,v\}$.

$$M = \begin{array}{c} \begin{array}{cccc} x & y & u & v \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

La première ligne définit un classement de l'ordre total. La deuxième ligne classe les dérivées selon l'ordre lexicographique $x > y$. Pour finir, la troisième ligne entraîne que les dérivées de u sont plus grandes que celles v.

$$\cdots > u_{xx} > v_{xx} > u_{xy} > v_{xy} > u_{yy} > v_{yy} > u_x > v_x > u_y > v_y > u > v$$

◁

En identifiant les opérateurs de dérivation $\delta_{x_1}^{a_1} \cdots \delta_{x_m}^{a_m}$ aux monômes $x_1^{a_1} \cdots x_m^{a_m}$, on a la propriété suivante :

Propriété 17 *Soit $\mathcal{R}$ un classement de Riquier. Le classement $\mathcal{R}$ induit un ordre admissible sur les opérateurs de dérivation de Θ de la manière suivante :*

$$\theta_1 < \theta_2 \iff \theta_1 u_1 < \theta_2 u_1$$

Preuve :
La preuve découle immédiatement des axiomes des classements. □

Propriété 18 *Si on connaît une matrice M à q lignes et $m+n$ colonnes caractérisant le classement $\mathcal{R}$, alors la matrice $\overline{M}$ constituée des m premières colonnes de M caractérise l'ordre admissible induit par $\mathcal{R}$ sur les opérateurs de dérivation.*

Preuve :
Il suffit de remarquer que lorsque l'on compare $\theta_1 u_1$ et $\theta_2 u_1$ en utilisant la matrice M, les n dernières colonnes sont inutiles car les n dernières composantes de $\Delta(\theta_1 u_1)$ et $\Delta(\theta_2 u_1)$ sont identiques. □

Exemple ▷ Reprenons le premier des exemples précédents, à savoir :
$X = \{x,y\}$ et $U = \{u,v\}$ avec

$$M = \begin{array}{c} \begin{array}{cccc} x & y & u & v \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

La matrice $\overline{M}$ extraite de M :

$$\overline{M} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}$$

définit l'ordre lexicographique pour $x > y$. $\triangleleft$

Système orthonome, système majorant

Définition 24 (Système orthonome) *Soit $\mathcal{R}$ un classement. Un système de p équations est dit orthonome pour $\mathcal{R}$ s'il peut s'écrire sous la forme $v_i = f_i(X,E_i)$ où :*

- *E_i est un ensemble fini de dérivées strictement inférieures à la dérivée v_i (pour le classement $\mathcal{R}$) ;*
- *f_i est une fonction de X et E_i ;*
- *les v_i sont deux à deux distincts.*

Pour chacune des équations, la dérivée v_i en partie gauche est naturellement appelée dérivée dominante.

Exemple $\triangleright$ Soit $\mathcal{R}$ un classement commençant par : $u < v < u_x < u_y < v_x < v_y < u_{xx} < u_{xy} < u_{yy} < v_{xx} < \cdots$.

Σ_1 est un système orthonome pour $\mathcal{R}$: $\Sigma_1 \left\{ \begin{array}{rcl} u_{xx} & = & (v_y + v_y^3)u_x - 3\,v \\ v_y & = & 5\,u_x^2 + 2 \end{array} \right.$

Σ_2 n'est pas un système orthonome pour $\mathcal{R}$: $\Sigma_2 \left\{ \begin{array}{rcl} u_{xx}^2 & = & (v_y + v_y^3)u_{xx} - 3\,v \\ v_y & = & 5\,u_x^2 + 2 \end{array} \right.$ $\triangleleft$

Remarque : la définition ci-dessus est différente de celle donnée par Riquier car les fonctions f_i n'ont a priori aucune propriété de dérivabilité ou d'analycité.

Dans tout ce chapitre, les systèmes que nous considérons seront (ou se ramèneront à) des systèmes orthonomes. Sous certaines conditions, ces systèmes admettent des solutions en série formelle. La définition de ces solutions en série formelle est plus délicate que celle donnée pour les idéaux différentiels. Intuitivement, on souhaite dire qu'une série formelle $\overline{u}$ est solution d'un système de p équations $f_1(u) = 0, \ldots, f_p(u) = 0$ si pour tout $1 \leq i \leq p$, $f_i(\overline{u})$ est la série formelle nulle. Toutefois, on ne peut, sans précaution, évaluer une fonction quelconque sur une série formelle. Les deux définitions qui suivent, servent à présenter rigoureusement les solutions en série formelle. La notation $f[\overline{u}](x)$ est tirée de [55].

Définition 25 ($f[\overline{u}](x)$) *Soit f une fonction des variables $X \cup E$ de $\mathbb{K}^{\mathrm{card}\{X \cup E\}}$ dans $\mathbb{K}$ où E est un sous-ensemble fini de ΘU. Soient un point x^0 de $\mathbb{K}^m$ et un n-uplet de séries formelles de $\mathbb{K}[[x - x^0]]$ $\overline{u}(x) = (\overline{u}_1(x), \ldots, \overline{u}_n(x))$.*

Soit E^0 l'ensemble $\{\theta\overline{u}_i(x^0)\}_{\theta u_i \in E}$.

En supposant que f est analytique en (x^0,E^0), on pose $f[\overline{u}](x) = f(x,(\theta\overline{u}_i)_{\theta u_i \in E})$.

Informellement, cela revient à remplacer dans l'équation f les indéterminées différentielles de U par les séries formelles $\overline{u}_i$. Ceci est possible car la fonction f est supposée analytique en E^0 (on peut alors appliquer l'opération de composition de séries formelles).

Grâce à cette définition, on peut introduire la notion de solution en série formelle d'un système.

Définition 26 (Solution en série formelle d'un système) *Soit un système de p équations f_i où chaque f_i est une fonction des variables $X \cup E$ de $\mathbb{K}^{\mathrm{card}\{X \cup E\}}$ dans $\mathbb{K}$ et où E est un sous–ensemble fini de ΘU.*

Soient un point x^0 de $\mathbb{C}^m$ et un n-uplet $\overline{u}(x) = (\overline{u}_1(x), \ldots, \overline{u}_n(x))$ de séries formelles $\mathbb{C}[[x - x^0]]$.

Soit E^0 l'ensemble $\{\theta\overline{u}_i(x^0)\}_{\theta u_i \in E}$. On suppose que chaque f_i est analytique en (x^0, E^0).

On dit alors que $\overline{u}(x)$ est solution du système si pour tout $1 \leq i \leq p$, la série formelle $f_i[\overline{u}](x)$ est la série formelle nulle.

Un système orthonome Σ peut être vu comme "une machine à calculer" la valeur d'une dérivée quelconque en un point x^0, sous réserve que l'on ait fixé les valeurs des dérivées sous l'escalier des dérivées dominantes de Σ en un point d'expansion x^0. Le processus est très similaire au calcul de solutions en série formelle des systèmes réguliers : on dérive les équations f_i (qu'il faut supposer indéfiniment dérivables en x^0 et les conditions initiales) pour déterminer la valeur des dérivées manquantes en x^0.

Exemple ▷ Considérons le système $u_x = \sin(u)$. Si on impose $u(0) = 1$, on peut calculer les valeurs des dérivées de u en 0 :

$u_x(0) = \sin(u(0)) = \sin(1)$, $u_{xx}(0) = u_x(0)\cos(u(0)) = \sin(1)\cos(1)$, $\ldots$ ◁

Propriété 19 *Soit $\mathcal{R}$ un classement. Soit Σ un système orthonome (pour $\mathcal{R}$) de p équations de la forme $v_i = F_i(X, E_i)$ vérifiant :*

- *E_i est un ensemble fini de dérivées strictement inférieures à la dérivée v_i (pour le classement $\mathcal{R}$) ;*
- *F_i est une fonction de X et de E_i analytique à l'origine.*

On suppose de plus que:

- *les séries de Taylor des F_i à l'origine majorent la série formelle nulle ;*
- *l'on attribue des valeurs positives réelles aux dérivées sous l'escalier (des dérivées dominantes) à l'origine ;*
- *le système Σ admet une série formelle solution $u = (u_1, \ldots, u_n)$.*

Alors, les séries formelles u_i majorent toutes la série formelle nulle.

Preuve :

Il faut prouver que la valeur d'une quelconque dérivée en zéro est positive.

On montre cela par récurrence (sur les dérivées) en utilisant les arguments suivants :

- par hypothèse, les dérivées sous l'escalier ont une valeur réelle positive ;
- chaque fonction F_i évaluée pour des arguments positifs fournit une valeur positive (car la série de Taylor (à l'origine) de F_i majore la série formelle nulle) ;

– toute dérivée d'une des fonctions F_i a une série de Taylor qui majore la série formelle nulle.

□

Exemple ▷ Soit le système $u_x = F(u)$ avec F analytique à l'origine. On suppose que la série de Taylor de F majore la série formelle nulle. On impose $u(0) = 0$.

Le théorème de Cauchy-Kovalevskaya (exposé dans la sous–section 3.4.1) s'applique et assure l'existence d'une série formelle solution qui converge à l'origine.

On peut calculer les dérivées à l'origine de la solution :
$u_x(0) = F(0) \geq 0$, $u_{xx}(0) = u_x(0)\, F'(u(0)) \geq 0$, $\ldots$ ◁

Définition 27 (Système majorant) *Soit $\mathcal{R}$ un classement. Soit Σ (resp. $\overline{\Sigma}$) un système orthonome (pour $\mathcal{R}$) de p équations de la forme $v_i = f_i(X,E_i)$ (resp. $v_i = F_i(X,E_i)$) vérifiant :*

– *E_i est un ensemble fini de dérivées strictement inférieures à la dérivée v_i (pour le classement $\mathcal{R}$) ;*
– *f_i (resp. F_i) est une fonction de X et E_i, indéfiniment dérivable à l'origine.*

On dit que le système $\overline{\Sigma}$ majore le système Σ (pour $\mathcal{R}$) si pour tout $1 \leq i \leq p$, la série de Taylor à l'origine de la fonction F_i majore celle de f_i.

Exemple ▷ On considère le classement $\mathcal{R}$ donné par : $u < v < u_x < u_y < v_x < v_y < u_{xx} < u_{xy} < u_{yy} < v_{xx} < \cdots$.

Le système $\overline{\Sigma}$ majore Σ.

$$\Sigma \begin{cases} u_{xx} &= (v_y + v_y^3)u_x - 3\,v \\ v_y &= 5\,u_x^2 + 2 \end{cases} \qquad \overline{\Sigma} \begin{cases} u_{xx} &= \frac{u_x}{1-v_y} + 3\,v \\ v_y &= \frac{5}{1-u_x} + 2 \end{cases}$$

◁

L'utilité d'une telle définition est de pouvoir appliquer la propriété suivante.

Propriété 20 *Soit $\mathcal{R}$ un classement. Considérons deux systèmes Σ et $\overline{\Sigma}$ tels que le système $\overline{\Sigma}$ majore Σ pour $\mathcal{R}$.*

On suppose qu'on a fixé pour chacun des deux systèmes les valeurs des dérivées sous l'escalier des dérivées dominantes. On impose de plus que les valeurs fixées pour les dérivées de $\overline{\Sigma}$ sont réelles positives et qu'elles majorent, en module, les valeurs fixées pour Σ.

Pour finir, on suppose que chaque système admet une solution sous forme de série formelle.

Sous ces conditions, la solution de $\overline{\Sigma}$ majore celle de Σ.

Preuve :

Il faut prouver que les coefficients de la solution de $\overline{\Sigma}$ majorent ceux de la solution Σ.

La preuve est une simple généralisation de la preuve de la propriété 19. □

3.3 Évaluation de monômes

On considère l'alphabet $X = \{x_1, \ldots, x_m\}$ et l'ensemble Ω des monômes construits sur X. Cette section contient des résultats traitant de l'évaluation (en des valeurs réelles) de monômes de Ω. Étant donné une séquence décroissante $\omega_1 > \cdots > \omega_s$ de monômes pour un ordre admissible $\mathcal{O}$ et un réel positif α, on cherche un m-uplet de réels $\beta = (\beta_1, \ldots, \beta_m)$ tel que tous les rapports $\omega_i(\beta)/\omega_{i+1}(\beta)$, pour $1 \leq i \leq s-1$, soient supérieurs à α ($\omega_i(\beta)$ est le monôme ω_i évalué en β).

Une preuve non constructive de ce résultat serait quasiment immédiate. Toutefois, nous présentons une preuve constructive[15] qui fournit une méthode effective permettant de calculer la valeur des β_i en fonction des ω_i, de l'ordre admissible $\mathcal{O}$ et de α. Cette preuve est découpée en plusieurs propositions.

Lemme 12 *Soit $\mathcal{O}$ un ordre admissible sur Ω. On suppose donnés s monômes $\{\omega_1, \ldots, \omega_s\}$ classés par ordre décroissant pour $\mathcal{O}$ ($\omega_1 > \omega_2 > \cdots > \omega_s$).*

Alors, il existe (au moins un) un vecteur ligne de m réels $b = (b_1, \ldots, b_m)$ tel que : $1 \leq i \leq s-1 \implies b\Delta(\omega_i) > b\Delta(\omega_{i+1})$. De plus, une formule explicite (donnée dans cette preuve) fournit un tel vecteur.

Preuve :

Comme $\mathcal{O}$ est un ordre admissible, d'après la propriété 11, il existe un entier q et une matrice M à q lignes et m colonnes à coefficients dans $\mathbb{R}$ tels que pour tous monômes ω et ω' :

$$\omega < \omega' \iff M\Delta\omega <_{lex} M\Delta\omega'$$

On pose $E = \{\Delta(\omega_i) - \Delta(\omega_{i+1}), 1 \leq i \leq s-1\}$. On a alors la propriété suivante (car les ω_i sont classés par ordre décroissant) :

$$\forall \Delta \in E,\ M\Delta >_{lex} (0, \ldots, 0)^t$$

On note $l_1, \ldots, l_q$ les q vecteurs lignes de la matrice M. Si on considère un élément Δ de E, on a $M\Delta >_{lex} (0, \ldots, 0)^t$, ce qui implique que (par définition de l'ordre lexicographique) un (et un seul) des q cas suivants se produit :

- $l_1\Delta > 0$ ou
- $l_1\Delta = 0$ et $l_2\Delta > 0$ ou
- $\ldots$
- $l_1\Delta = 0$ et $l_2\Delta = 0$ et $\ldots$ $l_{q-1}\Delta = 0$ et $l_q\Delta > 0$

On pose $E_i = \{\Delta \in E$ tel que $l_1\Delta = 0$ et $l_2\Delta = 0$ et $\ldots$ $l_{i-1}\Delta = 0$ et $l_i\Delta > 0\}$. Les E_i forment une partition de E.

Certains E_i pouvant être vides, on introduit l'ensemble $\{j_1, \ldots, j_p\}$ des indices i tel que E_i est non vide. Ainsi les $(E_{j_i})_{1 \leq i \leq p}$ forment encore une partition de E.

15. dans l'espoir de pouvoir estimer le domaine de convergences des solutions des systèmes différentiels réguliers

On pose alors pour $1 \leq i \leq p$: $y_i = \min(l_{j_i}\Delta,\ \Delta \in E_{j_i})$ et $Y_i = \max(|l_{j_i}\Delta|,\ \Delta \in E)$.
Par construction, on a $0 < y_i \leq Y_i$.

Soit le vecteur ligne : $b = \sum_{k=1}^{p} c_k l_{j_k}$ avec $c_1 = 1$ et $c_i = \frac{y_{i-1}}{2Y_i} c_{i-1}$ pour $2 \leq i \leq p$.

On a :

$$b = l_{j_1} + \frac{y_1}{2Y_2} l_{j_2} + \frac{y_1 y_2}{4Y_2 Y_3} l_{j_3} + \frac{y_1 y_2 y_3}{8Y_2 Y_3 Y_4} l_{j_4} + \cdots + \frac{y_1 y_2 y_3 \cdots y_{p-1}}{2^{p-1} Y_2 Y_3 Y_4 \cdots Y_p} l_{j_p}$$

De plus, il est évident que les c_i sont tous strictement positifs.

Nous allons prouver que $\forall \Delta \in E,\ b\Delta > 0$ (voir l'interprétation géométrique à la fin de la preuve). Pour ce faire, montrons que pour tout $1 \leq i \leq p$, on a $\forall \Delta \in E_{j_i}, b\Delta > 0$. Ceci est suffisant car les $(E_{j_i})_{1 \leq i \leq p}$ forment une partition de E.

Si $i = p$ et $\Delta \in E_{j_p}$, on a $b\Delta = c_p l_{j_p}\Delta > 0$ car $c_p > 0$ et $l_{j_p}\Delta > 0$

Soient $1 \leq i \leq p-1$ et $\Delta \in E_{j_i}$.

$$b\Delta = \sum_{k=1}^{p} c_k l_{j_k}\Delta = c_i l_{j_i}\Delta + \sum_{k=i+1}^{p} c_k l_{j_k}\Delta$$

Soit k tel que $i+1 \leq k \leq p$.

$$\begin{aligned} \left|c_k l_{j_k}\Delta\right| &= c_{k-1}\frac{y_{k-1}}{2}\left|\frac{l_{j_k}\Delta}{Y_k}\right| \leq c_{k-1}\frac{y_{k-1}}{2} = c_i\left(\prod_{l=i}^{k-2}\frac{y_l}{2Y_{l+1}}\right)\frac{y_{k-1}}{2} \\ &= c_i\frac{y_i}{2}\prod_{l=i+1}^{k-1}\frac{y_l}{2Y_l} \leq c_i y_i \frac{1}{2^{k-i}} \end{aligned}$$

Grâce à cette inégalité et d'après l'inégalité $a + b \geq a - |b|$ vraie pour tous réels a et b, on a :

$$\begin{aligned} b\Delta &\geq c_i l_{j_i}\Delta - \sum_{k=i+1}^{p}\left|c_k l_{j_k}\Delta\right| \geq c_i y_i - \sum_{k=i+1}^{p} c_i y_i \frac{1}{2^{k-i}} \\ &= c_i y_i\left(1 - \sum_{k=i+1}^{p}\frac{1}{2^{k-i}}\right) = c_i y_i\left(1 - \frac{1/2 - (1/2)^{p-i}}{1 - 1/2}\right) \\ &= c_i y_i(1 - (1/2)^{p-i}) > 0 \text{ car } p - i > 0 \end{aligned}$$

Ainsi $\forall \Delta \in E,\ b\Delta > 0$. On a donc $1 \leq i \leq s-1 \implies b\Delta(\omega_i) > b\Delta(\omega_{i+1})$ □

Propriété 21 *Avec les mêmes notations que dans le lemme précédent, si l'ordre $\mathcal{O}$ est du degré total, on peut construire un vecteur ligne b à coefficients positifs.*

Preuve :

Pour prouver cette propriété, on adapte la démonstration précédente aux nouvelles hypothèses. L'ordre $\mathcal{O}$ étant du degré total, d'après la propriété 16, la première ligne l_1 de la matrice M peut être supposée remplie de 1.

Si l'on ajoute la ligne l_1 à une ligne l_j (pour $j > 1$), on obtient une matrice $\overline{M}$ qui caractérise également l'ordre $\mathcal{O}$. Ainsi, on peut supposer (en additionnant autant de fois que nécessaire l_1 aux autres lignes) que tous les coefficients de la matrice M sont positifs.

La construction du vecteur b fournit alors un vecteur de nombres positifs. □

Remarque : Si l'on impose aux coefficients de M d'être strictement positifs, on obtient un vecteur b à coefficients strictement positifs.

Interprétation graphique

L'ensemble E est très particulier. La figure 3.1 décrit le cas $q = 2$ et $m = 2$. Les points de E sont soit dans E_1 soit dans E_2. Un point Δ de E_1 vérifie $l_1\Delta > 0$, et se situe donc dans un demi-plan ouvert dont la frontière est la droite D1 d'équation $l_1 x = 0$. Un point de E_2 vérifie $l_1\Delta = 0$ et $l_2\Delta > 0$, c'est–à–dire se situe sur la droite D1 et dans un demi-plan ouvert délimité par la droite D2 d'équation $l_2 x > 0$.

Les petits cercles représentent les points de E et la droite D en trait plein a pour équation $(l_1 + \epsilon l_2)x = 0$ où ϵ est positif et suffisamment petit pour que la droite D reste en dessous des points de E (un tel choix de ϵ est possible car E contient un nombre fini de valeurs).

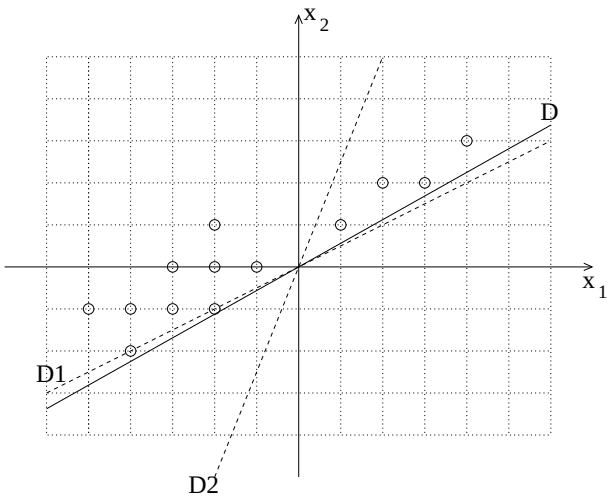


FIG. 3.1 – *Interprétation graphique*

Le lemme 12 a une conséquence directe :

Lemme 13 *Soit $\mathcal{O}$ un ordre admissible sur Ω. On suppose donnés s monômes $\{\omega_1, \ldots, \omega_s\}$ classés par ordre décroissant pour $\mathcal{O}$ ($\omega_1 > \omega_2 > \cdots > \omega_s$).*

Pour tout α réel tel que $\alpha > 1$, il existe un m-uplet $\beta = (\beta_1, \ldots, \beta_m)$ de réels strictement positifs tel que : $1 \leq i \leq s-1 \implies \frac{\omega_i(\beta)}{\omega_{i+1}(\beta)} \geq \alpha$

Preuve :

En utilisant le lemme 12, on sait qu'il existe un vecteur ligne de réels $b = (b_1, \ldots, b_m)$ tel que pour $1 \leq i \leq s-1$ on a $b\Delta(\omega_i) > b\Delta(\omega_{i+1})$

On pose $E = \{\Delta(\omega_i) - \Delta(\omega_{i+1}), 1 \leq i \leq s-1\}$. Soient $\delta = \min_{\Delta \in E}(b\Delta)$ et $\gamma = e^{\ln(\alpha)/\delta}$ (possible car $\alpha > 0$) On pose pour $\leq i \leq m$, $\beta_i = \gamma^{b_i}$.

Par construction même de b, on a $\delta > 0$. Par conséquent, comme $\alpha > 1$, on a $\gamma > 1$.

Ainsi pour $1 \leq i \leq s-1$, en posant $\Delta = \Delta(\omega_i) - \Delta(\omega_{i+1})$ on a :

$$\frac{\omega_i(\beta)}{\omega_{i+1}(\beta)} = \gamma^{b\Delta} \geq \gamma^{\delta} = \alpha \text{ car } b\Delta \geq \delta \text{ et } \gamma > 1$$

De plus par construction, les β_i sont des réels strictement positifs. □

Remarque : le cas $\alpha \leq 1$ est dégénéré car il suffit de prendre $\beta = (1, \ldots, 1)$.

Propriété 22 *En adoptant les mêmes hypothèses que dans le lemme précédent 13 et en supposant que l'ordre $\mathcal{O}$ est du degré total, le vecteur ligne construit dans le lemme 12 est à coefficients supérieurs à 1.*

Preuve :

En utilisant la propriété 21 et par la construction même des $\beta_i = \gamma^{b_i}$, comme $\gamma > 1$ et $b_i \geq 0$, on a $\beta_i \geq 1$. □

Exemple ▷

Voici une mise en pratique du lemme 13 et de la propriété 22. Soit $\mathcal{O}$ l'ordre admissible, sur les monômes de $X = \{a,b,c\}$, caractérisé par la matrice :

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

On considère les quatre monômes $abc > b^3 > ac^2 > bc^2$ et on pose $\alpha = 5$.

L'ensemble E vaut :

$$E = \{(1,-2,1)^t, (-1,3,-2)^t, (1,-1,0)^t\}$$

Les ensembles E_1, E_2 et E_3 sont :

$$E_1 = \emptyset,\ E_2 = \{(-1,3,-2)^t, (1,-1,0)^t\},\ E_3 = \{(1,-2,1)\}$$

Ainsi, on a $p = 2$, $j_1 = 2$ et $j_2 = 3$

$y_1 = \min(1,1) = 1$ et $y_2 = 1$

$Y_1 = \max(1,1,0) = 1$ et $Y_2 = \max(|-1|,1,1) = 1$

$b = l_2 + 1/2 l_3 = (5/2,1,0)$

$\delta = \min(1/2,1/2,3/2) = 1/2$ et $\gamma = e^{\ln 5/\delta} = e^{2\ln 5} = 25$

$\beta_a = 25^{5/2} = 5^5 = 3125$, $\beta_b = 25^1 = 25$ et $\beta_c = 25^0 = 1$

On peut alors calculer les trois rapports en évaluant respectivement a, b et c en β_a, β_b et β_c :

$$\frac{abc}{b^3} = 5, \quad \frac{b^3}{ac^2} = 5, \quad \frac{ac^2}{bc^2} = 125$$

Les trois rapports sont bien supérieurs à 5, et les valeurs attribuées à a, b et c sont bien supérieures à 1. ◁

Par simple curiosité, les lemmes 12 et 13 admettent une réciproque que voici :

Lemme 14 *On suppose donnés s monômes* $\{\omega_1,\ldots,\omega_s\}$ *de* Ω.

On suppose qu'il existe $\alpha > 1$ *et un m-uplet* $\beta = (\beta_1,\ldots,\beta_m)$ *de réels strictement positifs tel que :* $1 \leq i \leq s-1 \implies \frac{\omega_i(\beta)}{\omega_{i+1}(\beta)} \geq \alpha$.

Alors, il existe une infinité d'ordres admissibles tels que la suite des monômes soit classée par ordre décroissant $(\omega_1 > \omega_2 > \cdots > \omega_s)$.

Preuve :

On considère la matrice M donnée par : $M = \begin{pmatrix} \ln(\beta_1) & \cdots & \ln(\beta_m) \\ a_1 & \cdots & a_m \end{pmatrix}$.

La première ligne de M est forcément non nulle. En effet, si tous les β_i valaient 1, tous les rapports $\frac{\omega_i(\beta)}{\omega_{i+1}(\beta)}$ vaudraient 1 et l'inégalité $\frac{\omega_i(\beta)}{\omega_{i+1}(\beta)} \geq \alpha$ serait fausse car on suppose $\alpha > 1$.

On suppose les a_i algébriquement indépendants et que les vecteurs $(\ln(\beta_1),\ldots,\ln(\beta_m))$ et $(a_1,\ldots,a_m)$ sont linéairement indépendants. L'application $a \to M\,a$ de $\mathbb{N}^m$ dans $\mathbb{R}^2$ est donc injective et définit bien un ordre admissible d'après le théorème 11.

Si $1 \leq i \leq s-1$. En posant $\Delta = \Delta(\omega_i) - \Delta(\omega_{i+1})$, on a :

$\frac{\omega_i(\beta)}{\omega_{i+1}(\beta)} \geq \alpha \implies (\ln(\beta_1),\ldots,\ln(\beta_m))\Delta \geq \ln\alpha > 0$ ce qui signifie que $\omega_i > \omega_{i+1}$. □

3.4 Analycité des solutions

Après quelques rappels sur le théorème de Cauchy-Kovalevskaya et le théorème d'analycité de Riquier, nous montrons que les solutions des systèmes différentiels réguliers[16] (pour un classement de Riquier de l'ordre total et pour des conditions initiales "décrites" par des fonctions analytiques) sont analytiques. Rappelons que ce résultat était déjà démontré dans [45, page 34].

3.4.1 Théorème de Cauchy-Kovalevskaya

On doit le théorème de Cauchy-Kovalevskaya à Sophie Kovalevskaya dans [30]. En voici une formulation[17] :

Théorème 13 *Soit* Σ *un système de n d'équations :*

$$\Sigma \begin{cases} \frac{\partial^{N_1} u_1}{\partial x_1^{N_1}} &= f_1(x_1,\ldots,x_m,\overline{U}) \\ &\vdots \\ \frac{\partial^{N_n} u_n}{\partial x_1^{N_n}} &= f_n(x_1,\ldots,x_m,\overline{U}) \end{cases}$$

où $\overline{U}$ *désigne l'ensemble des dérivées du type* $\frac{\partial^{k_1+\cdots+k_m} u_j}{\partial x_1^{k_1}\ldots\partial x_m^{k_m}}$ *où* $1 \leq j \leq n$, $k_1 < N_j$ *et* $k_1 + \cdots + k_m \leq N_j$.

16. et en particulier les solutions des chaînes différentielles régulières

17. largement inspirée de [46]

On suppose que les conditions initiales sont données de la manière suivante : pour $1 \leq i \leq n$ *et* $1 \leq k \leq N_i - 1$, *on impose* $\frac{\partial^k u_i}{\partial x_1^k}(x_1^0,x_2,\ldots,x_m) = \Phi_{i,k}(x_2,\ldots,x_n)$ *où les fonctions* $\Phi_{i,k}$ *sont des fonctions analytiques en* $(x_2^0,\ldots,x_m^0)$.

Pour terminer, on suppose que les f_i *sont analytiques au point* $(x_1^0,\ldots,x_m^0,\overline{U}^0)$, *où* $\overline{U}^0$ *désigne l'ensemble des valeurs (fixées par les conditions initiales) des éléments de* $\overline{U}$ *en* $(x_1^0,\ldots,x_m^0)$.

Alors, le système Σ *admet une unique solution en série formelle analytique au point* $(x_1^0,\ldots,x_m^0)$.

Preuve :

Une preuve, limitée au cas où les fonctions f_i sont linéaires, se trouve dans les [46, Pages 14-26]. □

Le théorème de Cauchy-Kovalevskaya impose une équation par indéterminée différentielle. Cela implique en outre qu'il n'y pas de contraintes d'intégrabilité (notion expliquée dans la prochaine sous–section) et que l'existence d'une solution prolongeant les conditions initiales est assurée.

Ce théorème assez restrictif a été généralisé par Riquier.

3.4.2 Théorèmes d'existence et d'analycité de Riquier

Riquier a traité le problème de l'existence et de l'analycité des solutions pour des systèmes orthonomes plus généraux que ceux du théorème de Cauchy-Kovalevskaya. Le lecteur trouvera une exposition détaillée de la théorie de Riquier dans les ouvrages [51], [24] et [52, Chapitre VIII]. Une présentation claire et succinte de cette théorie se trouve dans [45, page 30].

Il faut bien distinguer deux problèmes séparés : celui de l'existence d'une solution et celui de son analycité. Commençons par le problème de l'existence. Les systèmes traités par la théorie de Riquier sont des systèmes orthonomes pour un ranking $\mathcal{R}$ supposé de Riquier.

$$\Sigma \left\{ \begin{array}{rcl} \theta_{1,1}u_1 & = & f_{1,1}(X,\overline{U}_{1,1}) \\ & \vdots & \\ \theta_{1,l_1}u_1 & = & f_{1,l_1}(X,\overline{U}_{1,l_1}) \\ & \vdots & \\ \theta_{n,1}u_n & = & f_{n,1}(X,\overline{U}_{n,1}) \\ & \vdots & \\ \theta_{n,l_n}u_n & = & f_{n,l_n}(X,\overline{U}_{n,l_n}) \end{array} \right.$$

où :

- les $f_{i,j}$ sont des fonctions de X et de $\overline{U}_{i,j}$;
- $\mathcal{R}$ est un classement de Riquier et $\overline{U}_{i,j}$ est un ensemble fini de dérivées inférieures à $\theta_{i,j}u_i$.

De tels systèmes peuvent contenir un nombre arbitraire d'équations (et non plus exactement n) et les dérivées de gauche des équations sont quelconques.

Contrairement au théorème Cauchy-Kovalevskaya, on n'est pas assuré de l'existence de solutions. Ceci est lié aux possibles contraintes d'intégrabilité non résolues ; de manière informelle dire qu'une contrainte d'intégrabilité entre deux équations e_1 et e_2 n'est pas résolue par Σ signifie qu'on peut obtenir de e_1 et e_2 une équation non "réduite" à 0 par le système Σ. Cette notion est à rapprocher de celle de paire critique résolue par un système d'équations et d'inéquations.

Pour résoudre ce problème, Riquier a introduit la notion de système passif. Cette définition est technique mais elle peut se résumer en substance par : un système orthonome est passif si toutes ses contraintes d'intégrabilités sont résolues.

On peut alors formuler le théorème d'existence de solution :

Théorème 14 *Si Σ est un système orthonome passif et si l'on fixe des conditions initiales en fixant les valeurs de toutes les dérivées sous l'escalier des dérivées dominantes de Σ, alors Σ admet une unique série formelle solution satisfaisant les conditions initiales.*

Vient ensuite le théorème d'analycité de Riquier (qui est une généralisation du théorème de Cauchy-Kovalevskaya) :

Théorème 15 *On suppose que :*

- *$\mathcal{R}$ est un classement de Riquier de l'ordre total ;*
- *le système Σ est orthonome et passif ;*
- *les conditions initiales sont données par des fonctions analytiques en x^0, ce qui signifie que les n fonctions $u_i^0 = \sum_{\theta u_i \in E_i} \frac{(\theta u_i)(x^0)}{\alpha_1! \cdots \alpha_m!}(x - x^0)^\alpha$ (où $\theta = \delta x_1^{\alpha_1} \cdots \delta x_m^{\alpha_m}$ et E_i est l'ensemble des dérivées de u_i sous l'escalier des $\theta_{i,j} u_i$ pour $1 \leq j \leq l_i$) sont analytiques en x^0 ;*
- *les fonctions $f_{i,j}$ sont analytiques en $x^0 = (x_1^0, \ldots, x_m^0, \overline{U}_{i,j}^0)$, où $\overline{U}_{i,j}^0$ désigne l'ensemble des valeurs en x^0 des éléments de $\overline{U}_{i,j}$ (ces valeurs sont fixées par les conditions initiales).*

Alors Σ admet une unique solution analytique en x^0.

3.4.3 Théorème d'analycité pour les systèmes différentiels réguliers

Nous donnons dans cette sous–section le théorème 17 assurant l'analycité des solutions en série formelle d'un système différentiel régulier. Ce théorème s'applique également aux chaînes différentielles régulières.

La preuve du théorème 17 s'appuie sur le théorème 16 ci–dessous. Le théorème 16 fournit une nouvelle preuve du théorème d'analycité de Riquier. La preuve du théorème 16 est relativement longue et complexe mais a l'avantage d'être écrite dans un formalisme récent.

Le lecteur trouvera en section 3.7 quelques mises en pratique de la preuve qui suit sur des exemples simples.

Théorème 16 *Soit $\mathcal{R}$ un classement de Riquier de l'ordre total. On considère un système Σ orthonome pour $\mathcal{R}$:*

$$\Sigma \begin{cases} \theta_{1,1}u_1 &= \displaystyle\sum_{\theta u_k < \theta_{1,1}u_1} a_{1,1}^{\theta u_k}\theta u_k + b_{1,1} \\ &\vdots \\ \theta_{1,l_1}u_1 &= \displaystyle\sum_{\theta u_k < \theta_{1,l_1}u_1} a_{1,l_1}^{\theta u_k}\theta u_k + b_{1,l_1} \\ &\vdots \\ \theta_{n,1}u_n &= \displaystyle\sum_{\theta u_k < \theta_{n,1}u_1} a_{n,1}^{\theta u_k}\theta u_k + b_{n,1} \\ &\vdots \\ \theta_{n,l_n}u_n &= \displaystyle\sum_{\theta u_k < \theta_{n,l_n}u_1} a_{n,l_n}^{\theta u_k}\theta u_k + b_{n,l_n} \end{cases}$$

vérifiant :

H1 *les $\theta_{i,j}$ et les θ figurant dans les sommes sont des opérateurs de dérivation d'ordre p ;*

H2 *les $a_{i,j}^{\theta u_k}$ et les $b_{i,j}$ sont des fonctions en $x_1,\ldots,x_m$ et en les dérivées d'ordre au plus $p-1$, et sont analytiques à l'origine ;*

H3 *pour tous $1 \leq i \leq n$ et $j \geq 2$, on a $\theta_{i,1}u_i > \theta_{i,j}u_i$ i.e. la première dérivée dominante en u_i est plus grande que les autres dérivées dominantes en u_i ;*

H4 *à l'origine, les valeurs des dérivées sous l'escalier sont fixées à 0 ;*

H5 *le système admet une solution en série formelle. Cette solution est un n-uplet de séries formelles de $\mathbb{C}[[X]]$ que l'on note $\widetilde{u} = (\widetilde{u}_1,\ldots,\widetilde{u}_n)$.*

Sous ces hypothèses, chaque $\widetilde{u}_i$ est analytique à l'origine.

Remarque : les sommes apparaissant dans le système Σ sont finies car $\mathcal{R}$ est un classement de l'ordre total (pour tout entier q, il n'y a qu'un nombre fini d'opérateurs d'ordre q).

Preuve :

La démonstration est inspirée de celle du théorème de Cauchy-Kovalevskaya donnée dans [46, Pages 14-26]. La démonstration ci–dessous est plus difficile à comprendre car elle nécessite l'utilisation de classements et davantage d'algèbre linéaire.

Cette preuve (même si les hypothèses de départ diffèrent) est proche de celle de Janet fournie dans [24]. Cependant, elle a été rédigée indépendamment, ce qui explique certaines différences qui seront décrites en section 3.6.

Voici une description des étapes de la preuve :

Étape 1 On construit un système $\overline{\Sigma}_1$;

Étape 2 On prouve que $\overline{\Sigma}_1$ admet une solution de la forme $\overline{u}_i = g_i(\beta_1 x_1 + \cdots + \beta_m x_m)$, où les $\overline{u}_i$ sont des fonctions analytiques majorant la fonction nulle ;

Étape 3 À l'aide des $\overline{u}_i$ ainsi obtenus, on majore le système Σ par un système $\overline{\Sigma}$ qui admet également $\overline{u}_i$ comme solution. On conclut que les séries formelles $\widetilde{u}_i$ sont analytiques car elles sont majorées par les $\overline{u}_i$ (car Σ est majoré par $\overline{\Sigma}$) qui sont analytiques.

Sauf contre-indication, tous les opérateurs de dérivations (y compris ceux présents dans les sommes) sont supposés d'ordre p.

Étape 1

En renommant si nécessaire les indéterminées u_i, on peut supposer $u_1 > u_2 > \cdots > u_n$.

On introduit :

- $V_u = \{\theta u_i, \theta \in \Theta[X], \mathrm{ord}(\theta) \leq p-1 \text{ et } 1 \leq i \leq n\}$, i.e. toutes les dérivées d'ordre au plus $p-1$.

Grâce au lemme 10 et à la remarque 1, on peut majorer toutes les fonctions $a_{i,j}^{\theta u_k}$ de Σ par une même fonction analytique $\overline{A}$ de la forme (avec M_a et r_a réels strictement positifs) :

$$\overline{A}(X,V_u) = \frac{M_a}{1 - \frac{x_1+\cdots+x_m+\sum_{v\in V_u} v}{r_a}}$$

De même, on majore tous les $b_{i,j}$ de Σ par une fonction $\overline{B}$ de la forme (avec M_b et r_b réels strictement positifs) :

$$\overline{B}(X,V_u) = \frac{M_b}{1 - \frac{x_1+\cdots+x_m+\sum_{v\in V_u} v}{r_b}}$$

D'après la propriété 17, le classement $\mathcal{R}$ induit un ordre admissible sur les opérateurs de dérivation. De plus, cet ordre est du degré total (car $\mathcal{R}$ est un classement de l'ordre total). Grâce à cet ordre, on construit la suite S décroissante des opérateurs de dérivations d'ordre au plus $n\,p$.

Si on considère un réel $\alpha > 1$ (dont la valeur sera fixée plus tard), en appliquant le lemme 13 d'évaluation des monômes à la suite S et en utilisant la propriété 22, on sait qu'il existe un m-uplet de réels $\beta = (\beta_1, \ldots, \beta_m)$ tel que :

- $\beta_i \geq 1$ pour $1 \leq i \leq m$;
- si $\theta > \theta'$ sont deux opérateurs de dérivation consécutifs de S, alors $\frac{\theta(\beta)}{\theta'(\beta)} \geq \alpha$ (où $\theta(\beta)$ (resp. $\theta'(\beta)$) est égal au monôme associé à θ (resp. θ') évalué en β).

On construit alors deux nouvelles fonctions analytiques A et B :

$$A(X,V_u) = \frac{M_a}{1 - \frac{\beta_1 x_1+\cdots+\beta_m x_m+\sum_{v\in V_u} v}{r_a}} \text{ et } B(X,V_u) = \frac{M_b}{1 - \frac{\beta_1 x_1+\cdots+\beta_m x_m+\sum_{v\in V_u} v}{r_b}}$$

Comme les β_i sont supérieurs à 1, les fonctions A et B majorent respectivement $\overline{A}$ et $\overline{B}$ et donc majorent respectivement les $a_{i,j}^{\theta u_k}$ et les $b_{i,j}$.

On construit alors le système $\overline{\Sigma}_1$:

$$\overline{\Sigma}_1 \left\{ \begin{array}{rcl} \theta_{1,1}u_1 & = & A\Big(\displaystyle\sum_{\theta u_k < \theta_{1,1}u_k} m_1^{\theta u_k}\theta u_k\Big) + \theta_{1,1}(\beta)B \\ & \vdots & \\ \theta_{n,1}u_n & = & A\Big(\displaystyle\sum_{\theta u_k < \theta_{n,1}u_n} m_n^{\theta u_k}\theta u_k\Big) + \theta_{n,1}(\beta)B \end{array} \right.$$

$$\text{où } m_i^{\theta u_k} = 1 + \frac{\theta_{i,1}(\beta)}{\theta(\beta)} \sum_{\theta u_k < \theta' u_i < \theta_{i,1} u_i} \frac{\theta(\beta)}{\theta'(\beta)}$$

Étape 2

On va montrer que $\overline{\Sigma}_1$ admet une solution de la forme $\overline{u}_i = g_i(\beta_1 x_1 + \cdots + \beta_m x_m)$, où les $\overline{u}_i$ sont des fonctions analytiques majorant la fonction nulle.

Si l'on remplace dans le système $\overline{\Sigma}_1$ les indéterminées u_i par $g_i(\beta_1 x_1 + \cdots + \beta_m x_m)$, on obtient :

$$\begin{cases} \theta_{1,1}(\beta) g_1^{(p)} = A\Big(\displaystyle\sum_{\theta u_1 < \theta_{1,1} u_1} m_1^{\theta u_1} \theta(\beta) g_1^{(p)} + \cdots \\ \qquad\qquad + \displaystyle\sum_{\theta u_n < \theta_{1,1} u_1} m_1^{\theta u_n} \theta(\beta) g_n^{(p)} \Big) + \theta_{1,1}(\beta) B \\ \qquad \vdots \\ \theta_{n,1}(\beta) g_n^{(p)} = A\Big(\displaystyle\sum_{\theta u_1 < \theta_{n,1} u_n} m_n^{\theta u_1} \theta(\beta) g_1^{(p)} + \cdots \\ \qquad\qquad + \displaystyle\sum_{\theta u_n < \theta_{n,1} u_n} m_n^{\theta u_n} \theta(\beta) g_n^{(p)} \Big) + \theta_{n,1}(\beta) B \end{cases}$$

Ce système peut être reformulé de la manière suivante (on appelle ce système Σ_g) :

$$\Sigma_g \begin{cases} g_1^{(p)} = A\Big(d_1^1 g_1^{(p)} + \cdots + d_1^n g_n^{(p)} \Big) + B \\ \qquad \vdots \\ g_n^{(p)} = A\Big(d_n^1 g_1^{(p)} + \cdots + d_n^n g_n^{(p)} \Big) + B \end{cases}$$

avec :

$$\begin{aligned} d_i^k &= \sum_{\theta u_k < \theta_{i,1} u_i} \frac{\theta(\beta)}{\theta_{i,1}(\beta)} m_i^{\theta u_k} = \sum_{\theta u_k < \theta_{i,1} u_i} \frac{\theta(\beta)}{\theta_{i,1}(\beta)} \left(1 + \frac{\theta_{i,1}(\beta)}{\theta(\beta)} \sum_{\theta u_k < \theta' u_i < \theta_{i,1} u_i} \frac{\theta(\beta)}{\theta'(\beta)} \right) \\ &= \sum_{\theta u_k < \theta_{i,1} u_i} \left(\frac{\theta(\beta)}{\theta_{i,1}(\beta)} + \sum_{\theta u_k < \theta' u_i < \theta_{i,1} u_i} \frac{\theta(\beta)}{\theta'(\beta)} \right) \\ &= \sum_{\theta u_k < \theta_{i,1} u_i} \left(\sum_{\theta u_k < \theta' u_i \leq \theta_{i,1} u_i} \frac{\theta(\beta)}{\theta'(\beta)} \right) \end{aligned}$$

En posant $t = \beta_1 x_1 + \cdots + \beta_m x_m$, ce système peut être considéré comme un système différentiel ordinaire où la seule dérivée est t. En appelant V_g l'ensemble des dérivées des g_i d'ordre au plus $p-1$, les fonctions A et B peuvent être vues comme des fonctions en t et V_g analytiques en $t = 0$ et $V_g = 0$.

Ce système peut être alors écrit de façon matricielle :

$$(I - AD)G = (B, \ldots, B)^t$$

où I est la matrice $n \times n$ identité, $G = (g_1^{(p)}, \ldots, g_n^{(p)})^t$, $D = (d_i^k)_{1 \leq i,k \leq n}$.

Supposons que $I - AD$ soit inversible d'inverse E au voisinage de $t = 0$ et $V_g = 0$, pour une certaine valeur de α (déterminée plus loin). Supposons de plus que E soit une matrice de fonctions analytiques à l'origine majorant la fonction nulle.

On peut alors écrire : $G = E(B, \ldots, B)^t$. En posant pour conditions initiales $g_i^{(j)}(0) = 0$ pour $1 \leq i \leq n$ et $1 \leq j \leq p-1$, le théorème de Cauchy-Kovalevskaya nous apprend que Σ_g admet une solution analytique $\overline{u}_1, \ldots, \overline{u}_n$ dans un voisinage W de $t = 0$. De plus, comme $E(B, \ldots, B)^t$ est un vecteur de fonctions analytiques en t et V_g qui majorent la fonction nulle (car E est une matrice de fonctions majorant la fonction nulle et B majore la fonction nulle), les fonctions solutions $\overline{u}_1, \ldots, \overline{u}_n$ majorent aussi la fonction nulle. L'étape 2 est ainsi prouvée.

On termine l'étape 2 en montrant que la matrice E existe. Pour ce faire, on s'intéresse [18] à $\rho(D)$ (rayon spectral de D) et on détermine une valeur de α telle que $\rho(D) \leq 1/(2M_a)$.

Pour une telle valeur de α, on a $\rho(M_a D) \leq 1/2$ qui implique que $\rho(A(0)D) \leq 1/2$ (car $M_a = A(0)$). En appliquant la propriété 15, on a : $I - AD$ est inversible d'inverse $E = \sum_{k=0}^{\infty} (AD)^k$ dans un voisinage de l'origine et cet inverse est analytique à l'origine. De plus, E est une matrice de fonctions analytiques majorant la fonction nulle.

Il ne nous reste plus qu'à déterminer une valeur de α telle que $\rho(D) \leq 1/(2M_a)$.

Pour cela, on étudie les valeurs propres de D qui sont racines du polynôme caractéristique $P(y)$ de D : $P(y) = \det(yI - D) = y^n - f_1 y^{n-1} + f_2 y^{n-2} + (-1)^{n-1} f_{n-1} y + (-1)^n f_n$

Les f_i vérifient la formule :

$$f_i = \sum_{J=\{j_1,\ldots,j_i\} \subset \{1,\ldots,n\}} \sum_{\sigma \in S(J)} \epsilon(\sigma) d_1^{\sigma(1)} \cdots d_{j_i}^{\sigma(j_i)}$$

Un coefficient f_i est, en module, majoré par une somme d'un nombre fini de quantités (éventuellement nulles) du type $d_1^{\sigma(1)} \cdots d_{j_i}^{\sigma(j_i)}$ où σ est une permutation d'un sous–ensemble de $\{1, \ldots, n\}$.

Considérons un produit non nul du type $d_1^{\sigma(1)} \cdots d_{j_i}^{\sigma(j_i)}$ où σ est une permutation d'un sous–ensemble de $\{1, \ldots, n\}$. En décomposant la permutation σ en cycles $\sigma_1, \ldots \sigma_s$, on a :

$$d_1^{\sigma(1)} \cdots d_{j_i}^{\sigma(j_i)} = \prod_{1 \leq i \leq s, \sigma_i = (z_1, \ldots, z_l)} d_{z_1}^{z_2} d_{z_2}^{z_3} \cdots d_{z_l}^{z_1}$$

Un terme $d_{z_1}^{z_2} d_{z_2}^{z_3} \cdots d_{z_l}^{z_1}$ peut être majoré : en le développant (en utilisant la formule de d_i^k), on obtient une somme de termes de la forme $\frac{\theta^1(\beta)}{\theta_1'(\beta)} \cdots \frac{\theta^l(\beta)}{\theta_l'(\beta)}$ avec

$$\theta^1 u_{z_2} < \theta_1' u_{z_1}, \quad \theta^2 u_{z_3} < \theta_2' u_{z_2}, \quad \ldots, \quad \theta^l u_{z_1} < \theta_l' u_{z_l}$$

Grâce à la structure circulaire de ces inégalités sur les dérivées, on peut prouver que $\theta^1 \theta^2 \cdots \theta^l u_1 < \theta_1' \theta_2' \cdots \theta_l' u_1$ ce qui implique $\theta^1 \theta^2 \cdots \theta^l < \theta_1' \theta_2' \cdots \theta_l'$.

18. pour comprendre pourquoi on ne cherche pas à majorer la norme de D, voir la remarque 2 à la fin de la preuve

Grâce à cette inégalité sur ces opérateurs de dérivations (qui sont tous deux d'ordre $n\,p$), on a $\frac{\theta^1(\beta)}{\theta'_1(\beta)} \cdots \frac{\theta^l(\beta)}{\theta'_l(\beta)} \leq \frac{1}{\alpha}$

Un terme d_i^k est une somme finie de termes de la forme $\frac{\theta(\beta)}{\theta'(\beta)}$. On appelle n_i^k le nombre de ces termes. On pose $N = (\max_{1\leq i,k\leq n}(n_i^k))^n$.

On a alors $d_{z_1}^{z_2} d_{z_2}^{z_3} \cdots d_{z_l}^{z_1} \leq \frac{N}{\alpha}$.

Ainsi, le coefficient $d_1^{\sigma(1)} \cdots d_{j_i}^{\sigma(j_i)}$ est inférieur à $\left(\frac{N}{\alpha}\right)^s$.

Choisissons alors α tel que $\alpha > Nn! \max(2n, 2^n M_a^n n)$. On remarque qu'on a bien $\alpha > 1$, condition qui avait été supposée précédemment.

On a $\frac{N}{\alpha} \leq N \frac{1}{Nn! \max(2n, 2^n M_a^n n)} \leq \frac{1}{n!} \min\left(\frac{1}{2n}, \frac{1}{2^n M_a^n n}\right)$

Ainsi $d_1^{\sigma(1)} \cdots d_{j_i}^{\sigma(j_i)} \leq \left(\frac{N}{\alpha}\right)^s \leq \frac{N}{\alpha}$ car $\frac{N}{\alpha} \leq 1$. On peut alors majorer le module de f_i par $\frac{N}{\alpha}$ que multiplie le nombre de toutes les permutations des sous–ensembles de cardinal i de $\{1, \ldots n\}$. On a donc $|f_i| \leq C_n^i i! \frac{N}{\alpha} = \frac{n!}{(n-i)!} \frac{N}{\alpha} \leq n! \frac{N}{\alpha} \leq \min\left(\frac{1}{2n}, \frac{1}{2^n M_a^n n}\right) = \frac{1}{n} \min\left(\frac{1}{2}, \frac{1}{2^n M_a^n}\right)$

On peut donc appliquer le lemme 11 : on pose $\epsilon = \min\left(\frac{1}{2}, \frac{1}{2^n M_a^n}\right)$ et on a bien $\epsilon < 1$. Les coefficients du polynôme P (excepté le coefficient de y^n) sont en module majorés par ϵ/n. On en déduit que les valeurs propres sont en module inférieures à $\sqrt[n]{\epsilon}$ et on a donc $\rho(D) \leq \frac{1}{2M_a}$.

Étape 3

Nous allons maintenant construire le système $\overline{\Sigma}$ majorant Σ. La méthode utilisée consiste à faire apparaître les solutions $\overline{u}_i$ pour que le système $\overline{\Sigma}$ admette aussi les $\overline{u}_i$ pour solution.

$$\overline{\Sigma} \left\{ \begin{array}{rcl} & \vdots & \\ \theta_{i,j} u_i & = & A\left(\displaystyle\sum_{\theta u_k < \theta_{i,j} u_i} \theta u_k + \sum_{k=1}^{n} \theta_{i,j}(\beta)(d_i^k - \widetilde{d}_{i,j}^k)\overline{u}_k^{(p)} \right) \quad + \quad \theta_{i,j}(\beta) B \\ & \vdots & \end{array} \right.$$

$$\text{avec } \widetilde{d}_{i,j}^k = \sum_{\theta u_k < \theta_{i,j} u_i} \frac{\theta(\beta)}{\theta_{i,j}(\beta)} \text{ pour } 1 \leq i \leq n, 1 \leq j \leq l_n$$

Le système $\overline{\Sigma}$ majore le système Σ pour les raisons suivantes :

- A majore les $a_{i,j}^{\theta u_k}$, B majore les $b_{i,j}$;
- les $\theta_{i,j}(\beta)$ sont plus grands que 1 car pour tout i, $\beta_i \geq 1$;
- $d_i^k - \widetilde{d}_{i,j}^k \geq 0$ (voir ci–dessous) et les $\overline{u}_i$ sont des fonctions analytiques majorant la fonction nulle.

On prouve que $d_i^k \geq \widetilde{d}_{i,j}^k$ en montrant que tout terme de la somme $\widetilde{d}_{i,j}^k$ apparaît dans la somme d_i^k. Un terme de la somme $\widetilde{d}_{i,j}^k$ est de la forme $\frac{\theta(\beta)}{\theta_{i,j}(\beta)}$ avec $\theta u_i < \theta_{i,j} u_k$. Ce terme apparaît dans l'expression de d_i^k car les deux opérateurs de dérivation θ et $\theta' = \theta_{i,j}$ vérifient bien les conditions $\theta u_k < \theta_{i,1} u_i$ (grâce à **H3**) et $\theta u_k < \theta' u_i \leq \theta_{i,1} u_i$ (grâce à **H3** également).

Les quantités $\theta_{i,j}(\beta)(d_i^k - \widetilde{d}_{i,j}^k)\overline{u}_k$ ont été ajoutées pour que le système $\overline{\Sigma}$ admette également les $\overline{u}_i$ comme solution. Considérons une des équations de $\overline{\Sigma}$. Pour prouver que cette équation admet les $\overline{u}_i$ pour solution on vérifie que l'expression suivante est nulle :

$$\theta_{i,j}(\beta)\overline{u}_i^{(p)} \quad - \quad A\left(\sum_{\theta u_k < \theta_{i,j}u_i} \theta(\beta)\overline{u}_k^{(p)} + \sum_{k=1}^{n} \theta_{i,j}(\beta)(d_i^k - \widetilde{d}_{i,j}^k)\overline{u}_k^{(p)}\right) \quad - \quad \theta_{i,j}(\beta)B$$

De manière équivalente, on peut considérer l'expression suivante (en divisant par $\theta_{i,j}(\beta)$ et en faisant apparaître les $\widetilde{d}_{i,j}^k$) :

$$\begin{array}{lll} \overline{u}_i^{(p)} & - & A\left(\widetilde{d}_{i,j}^1\overline{u}_1^{(p)} + \cdots + \widetilde{d}_{i,j}^n\overline{u}_n^{(p)} + \right. \\ & & \left. (d_i^1 - \widetilde{d}_{i,j}^1)\overline{u}_1^{(p)} + \cdots + (d_i^n - \widetilde{d}_{i,j}^n)\overline{u}_n^{(p)}\right) - B = \\ \overline{u}_i^{(p)} & - & A\left(d_i^1\overline{u}_1^{(p)} + \cdots + d_i^n\overline{u}_n^{(p)}\right) - B \end{array}$$

Cette expression est nulle car on y reconnaît une équation du système $\overline{\Sigma}_1$ qui admet les $\overline{u}_i$ comme solution.

Ainsi, les séries formelles $\widetilde{u}_i$ sont majorées par $\overline{u}_i$ ce qui prouve (lemme 14) que les $\widetilde{u}_i$ sont analytiques à l'origine. □

Remarque 2 *La matrice D est très particulière. Certains de ses termes vont grossir si α augmente, et d'autres vont diminuer*[19]*. En effet, prenons deux entiers k et i vérifiant $1 \leq k < i \leq n$. Un terme de la somme qu'exprime $d_{i,1}^k$ est de la forme $\frac{\theta(\beta)}{\theta_{i,1}(\beta)}$ avec $\theta u_k < \theta_{i,1}u_i$. Comme $k < i$, on a $u_k > u_i$ et on a forcément $\theta < \theta_{i,1}$ (car $\theta \geq \theta_{i,1}$ impliquerait $\theta u_k \geq \theta_{i,1}u_k > \theta_{i,1}u_i$). Par conséquent, on a $\frac{\theta(\beta)}{\theta_{i,1}(\beta)} \leq \frac{1}{\alpha}$.*

Comme $d_{i,1}^k$ est une somme finie de termes inférieurs à $\frac{1}{\alpha}$, $d_{i,1}^k$ diminue si α augmente.

Au contraire, les $d_{i,1}^k$ quand $k > i$ peuvent grossir si α augmente (cela dépend de l'ordre, pour certains ordres cela ne se produit pas).

Ceci explique qu'on n'a pas essayé de montrer que $||A|| < 1$ en utilisant la norme 1 ou ∞.

Théorème 17 (Théorème d'analycité) *Soit $A = 0$, $S \neq 0$ un système différentiel régulier de $\mathbb{K}[X]\{U\}$ pour un classement $\mathcal{R}$ de Riquier et de l'ordre total. Soit $x^0 = (x_1^0, \ldots, x_m^0)$ un point d'expansion. On note R_0 l'anneau des polynômes réduits par rapport à A.*

On suppose que le système $A = 0, S \neq 0$, vu comme un système algébrique de R_0, admet une solution ; cette solution fixe donc des conditions initiales. Pour terminer, on suppose que ces conditions initiales sont données par des fonctions analytiques en x^0, ce qui signifie que les n séries formelles $u_i^0 = \sum_{\theta u_i \in E_i} \frac{(\theta u_i)(x^0)}{\alpha_1! \cdots \alpha_m!}(x - x^0)^\alpha$ (où $\theta = \delta x_1^{\alpha_1} \cdots \delta x_m^{\alpha_m}$ et E_i est l'ensemble des dérivées de u_i pour lesquelles on a fixé une valeur) ont un domaine de convergence non vide.

Le problème admet alors une unique solution en série formelle analytique en x^0.

19. Ce phénomène se produit dans l'exemple 2 de la sous–section 3.7.2

Preuve :

Le lemme 7 prouve l'existence et l'unicité d'une solution de $A = 0$, $S \neq 0$. Cette solution est un n-uplet de séries formelles $\widetilde{u} = (\widetilde{u}_1, \ldots, \widetilde{u}_n)$

Nous allons nous ramener à un système vérifiant les hypothèses du théorème 16.

On commence par rendre les équations linéaires en les dérivées d'ordre maximal. La méthode qui suit est identique à celle mise en œuvre dans l'algorithme Rif [50].

Soit $q = a_d v^d + \cdots + a_1 v + a_0$ un polynôme de A vu comme polynôme univarié en sa dérivée dominante v. On pose $p = \operatorname{ord} v$. En dérivant q par rapport à l'une des variables indépendantes (par exemple x_1), on obtient :

$\delta_{x_1} q = s_q(\delta_{x_1} v) + v^d \delta_{x_1} a_d + \cdots + v \delta_{x_1} a_1 + \delta_{x_1} a_0$

Le polynôme obtenu est alors linéaire en les dérivées d'ordre $p+1$. L'équation $\delta_{x_1} q = 0$ s'écrit sous la forme :

$$\delta_{x_1} v = -\frac{v^d \delta_{x_1} a_d + \cdots + v \delta_{x_1} a_1 + \delta_{x_1} a_0}{s_q}$$

Cette fraction est analytique en les conditions initiales car le dénominateur est non nul. En posant $\overline{\theta} u_i = \delta_{x_1} v$, cette équation est de la forme

$$\overline{\theta} u_i = \sum_{\theta u_k < \overline{\theta} u_i,\, \operatorname{ord} \theta = p+1} a^{\theta u_k} \theta u_k + b$$

où les $a^{\theta u_k}$ et les b sont :

- des fonctions de X et des dérivées d'ordre au plus p ;
- analytiques en les conditions initiales.

En remplaçant dans A, le polynôme q par ses m dérivées par rapport à x_1, ..., x_m, on obtient un nouveau système A admettant toujours $\widetilde{u}$ comme solution formelle (voir la figure 3.2).

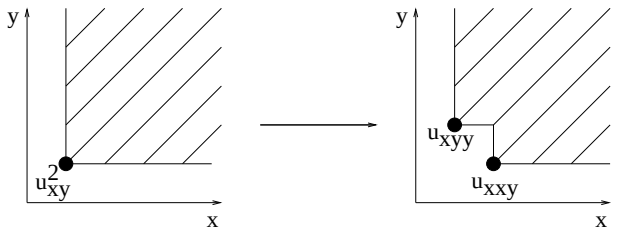


FIG. 3.2 – *Évolution de l'escalier. Un polynôme q (de rang u^2_{xy}) est remplacé par $\delta_x q$ et $\delta_y q$ de rangs respectifs u_{xxy} et u_{xyy}*

En procédant ainsi avec tous les polynômes de A, on se ramène à un système d'équations linéaires en les dérivées d'ordre maximal et où toutes les équations ont même ordre de dérivation (on dérive les polynômes jusqu'à ce qu'ils aient tous le même ordre, à savoir l'ordre maximal de l'ensemble A initial).

Remarque : par cette méthode, on est amené à ajouter à l'ensemble des conditions initiales un nombre fini de valeurs de dérivées sous l'escalier. Ainsi, les nouvelles conditions

initiales sont toujours données par des fonctions analytiques. Sur la figure 3.2, il faudrait ajouter aux conditions initiales les valeurs de $u_{xxy}(x^0)$ et de $u_{xyy}(x^0)$.

Dans le cas où le système obtenu contient plusieurs équations avec la même dérivée dominante, on peut n'en conserver qu'une.

Au cas où une indéterminée u_i n'apparaît pas en partie gauche des équations, les conditions initiales fixent toute la fonction u_i. On peut alors remplacer dans le système u_i par sa valeur, et supposer dans la suite que chaque indéterminée apparaît en partie gauche.

Après un changement d'origine (translation sur les variables indépendantes pour se ramener au cas ${x_1}^0 = \ldots = {x_m}^0 = 0$), et par le changement de variables sur $\overline{u}_i = u_i - u_i^0$ pour $1 \leq i \leq n$, on obtient un système vérifiant les hypothèses du théorème 16.

Remarque : il n'est pas nécessaire (même si cela est facile à réaliser) de rendre le système autoréduit pour appliquer le théorème 16. □

Le théorème 17 qui précède s'applique aux solutions de systèmes $C = 0$, $H_C \neq 0$, où C est une chaîne différentielle régulière. Le théorème 17 s'appuie sur le lemme de Rosenfeld pour assurer l'existence d'une solution en série formelle d'un système différentiel régulier $A = 0$, $S \neq 0$. Par conséquent, le théorème 17 ne donne aucun renseignement d'analycité sur d'éventuelles solutions annulant les inéquations de S (voir sous–section 2.7.3). D'un point de vue pratique, cela n'est pas gênant car, dans ce cas, les développements en série formelle de telles solutions ne peuvent être calculées. D'un point de vue théorique, ce problème mérite certainement d'être creusé.

3.5 Cas où $\mathcal{R}$ est un simple classement de l'ordre total

On conjecturait que le théorème d'analycité de Riquier se généralisait aux classements de l'ordre total. Cela semblait naturel car les classements plus généraux que ceux de Riquier ont (à ma connaissance) été mis en évidence après que Riquier ait prouvé son théorème.

Toutefois, l'hypothèse que le classement $\mathcal{R}$ soit de Riquier est utilisée dans la preuve de Riquier et dans celle qui précède (pour prouver l'inversibilité de la matrice $I - AD$).

Deux issues étaient envisageables : le théorème de Riquier était faux pour des classements de l'ordre total quelconques ou alors il existait une preuve plus générale. L'exemple suivant clôt le débat car il vérifie toutes les hypothèses du théorème (sauf celle du classement de Riquier) et admet une solution non analytique. Ainsi, le théorème d'analycité de Riquier ainsi que le théorème d'analycité pour les systèmes différentiels réguliers ne se généralisent pas aux classements de l'ordre total quelconques.

J'ai également montré dans [33] que, pour tout réel s, cette solution n'était pas Gevrey d'ordre s. Je montre également dans [33] que cette solution est q-Gevrey d'ordre 1.

Exemple ▷ Soit $\mathcal{R}$ le classement[20] commençant par : $v < u < v_x < v_y < u_y < u_x < v_{xx} < v_{xy} < v_{yy} < u_{yy} < u_{xy} < u_{xx} < \cdots$

20. qu'on retrouve à la page 14 de [5] et à la section 6 de [48]

$$C \left\{ \begin{array}{lcl} u_{xx} & = & u_{xy} + u_{yy} + v \\ v_{yy} & = & v_{xy} + v_{xx} + u \end{array} \right.$$

Il est clair que C est la présentation caractéristique de $[C]$: ${H_C}^{\infty} = [C]$. On pose égales à 1 toutes les dérivées sous l'escalier en $x = 0$, $y = 0$ (i.e. pour n entier positif $u_{y^n}(0,0) = u_{xy^n}(0,0) = v_{x^n}(0,0) = v_{x^n y}(0,0) = 1$).

Les conditions initiales définissent bien des fonctions analytiques car

$$u(0,y) = u_x(0,y) = e^y \text{ et } v(x,0) = v_y(x,0) = e^x$$

Toutefois, la solution en série formelle n'est pas analytique. ◁

Idées de la preuve de non-analycité Le calcul de $u_{x^p y^q}(0,0)$ met en œuvre un calcul proche de celui de la suite de Fibonacci :

$$u_{x^p y^q}(0,0) = u_{x^{p-1} y^{q+1}}(0,0) + u_{x^{p-2} y^{q+2}}(0,0) + v_{x^{p-2} y^q}(0,0)$$

Ainsi le terme $u_{x^p y^q}(0,0)$ est la somme des deux dérivées de u voisines en haut à gauche sur la diagonale (plus une dérivée de v), comme le montre la figure 3.3 .

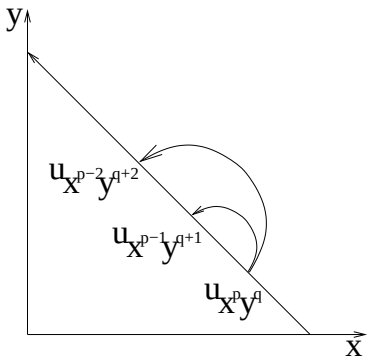


FIG. 3.3 – *Calcul de* $u_{x^p y^q}(0,0)$

En itérant la formule précédente, on obtient $u_{x^p}(0,0) = f_{p-2}\, v_{y^{p-2}}(0,0) +$ un entier positif (cette formule est démontrée plus loin) où f est la suite (décalée d'un cran vers la gauche) de Fibonacci : $f_0 = f_1 = 1$ et $f_{n+2} = f_{n+1} + f_n$ pour $n \geq 0$.

Par symétrie, le calcul de $v_{y^{p-2}}(0,0)$ occasionne le même phénomène dans la direction opposée comme le montre la figure 3.4.

En poursuivant encore, on opère un calcul en *zigzag*. Finalement, la valeur de $u_{x^p}(0,0)$ est supérieure à un produit de termes de la suite (décalée) de Fibonacci. Cette valeur croît trop vite (quand p augmente) pour que u soit analytique.

Preuve de non analycité Pour simplifier la preuve on introduit deux suites à double indice définies par : $a_{i,j} = u_{x^i y^j}(0,0)$ et $b_{i,j} = v_{x^i y^j}(0,0)$.

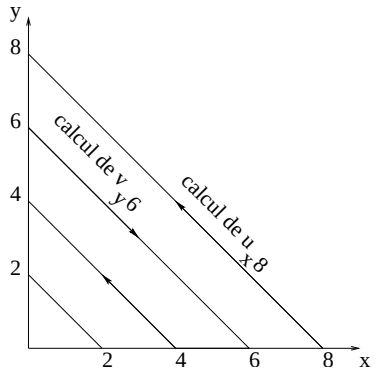


FIG. 3.4 – *Calcul en zigzag*

On obtient alors :

$$\begin{aligned} a_{i,j} &= a_{i-1,j+1} + a_{i-2,j+2} + b_{i-2,j} \text{ si } i \geq 2 \\ a_{i,j} &= 1 \text{ si } i \leq 1 \\ b_{i,j} &= b_{i+1,j-1} + b_{i+2,j-2} + a_{i,j-2} \text{ si } j \geq 2 \\ b_{i,j} &= 1 \text{ si } j \leq 1 \end{aligned} \tag{3.1}$$

Nous allons montrer que le développement en série formelle du système ne converge pas. La preuve est décomposée en trois étapes :

Étape 1 On prouve la formule **F** pour $p \geq 0$, $q \geq 0$:

$$a_{p,q} = f_p + \sum_{i=0}^{p-2} b_{p-2-i,i+q} f_i \qquad \textbf{(F)}$$

où f est la suite définie par : $f_0 = f_1 = 1$ et $f_{n+2} = f_{n+1} + f_n$ pour $n \geq 0$;

Étape 2 On prouve que si u est analytique à l'origine, alors l'ensemble S de réels défini par $S = \left\{ \left(\frac{|a_{2p,0}|}{(2p)!} \right)^{1/(2p)} / p \in \mathbb{N} \right\}$ est borné ;

Étape 3 En utilisant **F**, on prouve que S n'est pas borné. Cela implique que u n'est pas analytique à l'origine.

Preuve :

Étape 1 : on prouve **F** par récurrence sur p et q.

Base de la récurrence:

La formule **F** est vraie pour tout entier naturel q et p valant 0 ou 1.

Cas $p = 0$, q quelconque :

F fournit $a_{0,q} = f_0 = 1$. Cette valeur coïncide avec celle fournie par les conditions initiales.

Cas $p = 1$, q quelconque :

F fournit $a_{1,q} = f_1 = 1$. Cette valeur coïncide également avec celle fournie par les conditions initiales. La base de la récurrence est ainsi prouvée.

Hypothèse de récurrence :

La formule **F** est vraie pour p et tout entier naturel q, et vraie pour $p+1$ et tout entier naturel q. On montre que **F** est vraie pour $p+2$ et tout entier naturel q.

$$\begin{aligned}
a_{p+2,q} &= a_{p+1,q+1} + a_{p,q+2} + b_{p,q} \text{ d'après 3.1} \\
&= f_{p+1} + \sum_{i=0}^{p-1} b_{p-1-i,i+q+1} f_i + f_p + \sum_{i=0}^{p-2} b_{p-2-i,i+q+2} f_i + b_{p,q} \\
&= (f_{p+1} + f_p) + b_{p-1,q+1} + \sum_{i=1}^{p-1} b_{p-1-i,i+q+1} f_i + \sum_{i=1}^{p-1} b_{p-i-1,i+q+1} f_{i-1} + b_{p,q} \\
&= f_{p+2} + b_{p-1,q+1} + \sum_{i=1}^{p-1} b_{p-1-i,i+q+1} f_{i+1} + b_{p,q} \\
&= f_{p+2} + b_{p-1,q+1} f_1 + \sum_{i=2}^{p} b_{p-i,i+q} f_i + b_{p,q} f_0 \\
&= f_{p+2} + \sum_{i=0}^{p} b_{p-i,i+q} f_i
\end{aligned}$$

La formule **F** est donc vraie pour $p+2$ et tout entier naturel q, ce qui achève la preuve par récurrence.

Remarquons qu'on obtient (par symétrie entre les deux suites a et b) la relation :

$$\text{pour } p \geq 0 \text{ et } q \geq 0, \text{ alors } b_{p,q} = f_q + \sum_{i=0}^{q-2} a_{q-2-i,i} f_i$$

Étape 2 : on prouve que si u est analytique à l'origine, alors l'ensemble de réels défini par $S = \left\{ \left(\frac{|a_{2p,0}|}{(2p)!} \right)^{1/(2p)} / p \in \mathbb{N} \right\}$ est borné.

C'est en fait une conséquence directe du lemme d'Hadamard (lemme 21 en annexe) qui exprime le rayon de convergence d'une série formelle. Toutefois, cela peut se prouver directement.

Si u est analytique à l'origine, il existe deux réels strictement positifs r et s tels que $\sum_{(p,q)\in\mathbb{N}^2} \frac{a_{p,q}}{p!q!} r^p s^q$ converge. Ainsi, il existe un réel positif (qu'on peut supposer plus grand que 1) tel que $\frac{|a_{p,q}|}{p!q!} r^p s^q \leq M$ pour tous p et q entiers (une condition nécessaire de convergence d'une série est que ses termes soient bornés). Par conséquent, pour $p \geq 1$ on a $\frac{|a_{p,0}|}{p!} \leq M r^p$ for $p \geq 1$ qui entraîne $\left(\frac{|a_{p,0}|}{p!} \right)^{1/p} \leq M^{1/p} r \leq Mr$ car $M \geq 1$. Ceci conclut l'étape 2.

Étape 3 : on prouve que l'ensemble S n'est pas borné.

Par une preuve par récurrence, on montre immédiatement que tous les $a_{i,j}$ et les $b_{i,j}$ sont positifs. Ainsi pour $p \geq 2$ et $q \geq 2$, on déduit de **F** les inégalités $a_{p,q} \geq b_{0,p-2+q} f_{p-2}$ et (par symétrie) $b_{p,q} \geq a_{p-2+q,0} f_{q-2}$. Par conséquent, pour $p \geq 2$, on a:

$$a_{2p,0} \geq f_{2p-2} b_{0,2p-2} \geq f_{2p-2} f_{2p-4} a_{2p-4,0} \geq \cdots \geq f_{2p-2} f_{2p-4} \cdots f_2 K$$

où K vaut $a_{2,0}$ ou $b_{0,2}$. Dans les deux cas, K vaut 3.

En utilisant la formule générale de la suite de Fibonacci, on a : $f_n \sim_{n\to\infty} \frac{1}{\sqrt{5}}\left(\frac{2}{\sqrt{5}-1}\right)^{n+1}$. Par un raisonnement simple, on en déduit qu'il existe deux réels C et r vérifiant :

- $C > 0$ et $r > 1$;
- $f_n \geq Cr^n$ pour $n \geq 0$.

Ainsi, $a_{2p,0} \geq C^{p-1}(r^{2p-2}\cdots r^2)\times 3 \geq C^{p-1}(r^{p-1}\cdots r)^2 = C^{p-1}(r^{\frac{p(p-1)}{2}})^2 = C^{p-1}r^{p(p-1)}$.

$$\begin{aligned}
\ln\left(\left(\tfrac{a_{2p,0}}{(2p)!}\right)^{1/(2p)}\right) &= \tfrac{1}{2p}\ln\tfrac{a_{2p,0}}{(2p)!} \\
&\geq \tfrac{1}{2p}\ln\left(\tfrac{C^{p-1}r^{p(p-1)}}{(2p)!}\right) \\
&= \tfrac{1}{2p}\big((p-1)\ln C + p(p-1)\ln r - \ln((2p)!)\big) \\
&= \tfrac{p(p-1)}{2p}\left(\tfrac{\ln C}{p} + \ln r - \tfrac{\ln((2p)!)}{p(p-1)}\right) \\
&= \tfrac{(p-1)}{2}\underbrace{\left(\frac{\ln C}{p} + \ln r - \frac{\ln((2p)!)}{p(p-1)}\right)}_{A(p)}
\end{aligned}$$

Intéressons-nous aux trois termes de la somme $A(p)$ quand p tend vers l'infini : le premier $\frac{\ln C}{p}$ tend vers 0, le deuxième $\ln r$ est constant et strictement positif car $r > 1$. Si le troisième terme tend vers 0 (démonstration plus bas), la quantité $\frac{p-1}{2}A(p)$ tend vers l'infini. Ainsi la quantité $\left(\frac{a_{2p,0}}{(2p)!}\right)^{1/(2p)}$ tend vers l'infini et S n'est donc pas bornée, ce qui prouve que u n'est pas analytique.

Pour terminer, on prouve que le troisième terme de la somme $A(p)$ tend vers 0 quand p tend vers zéro.

La formule de Stirling donne : $(2p)! \sim_{p\to\infty} \left(\frac{2p}{e}\right)^{2p}\sqrt{4\pi p}$ (formule d'équivalence quand p tend vers l'infini). On en déduit qu'il existe un entier p_0 tel que $p \geq p_0$ implique $(2p)! \leq 2\left(\frac{2p}{e}\right)^{2p}\sqrt{4\pi p}$.

Ainsi, si $p \geq p_0$:

$$\frac{\ln((2p)!)}{p(p-1)} \leq \frac{\ln 2 + 2p\ln\frac{2p}{e} + \frac{1}{2}\ln(4\pi p)}{p(p-1)} = \frac{\ln 2}{p(p-1)} + \frac{2(\ln 2 + \ln p - 1)}{p-1} + \frac{1}{2}\frac{\ln(4\pi p)}{p(p-1)}$$

De cette inégalité, on déduit que $\lim_{p\to\infty}\frac{\ln((2p)!)}{p(p-1)} = 0$ ce qui termine la preuve. □

3.6 Différences avec la preuve de Riquier

Le théorème 16 et le théorème d'analycité de Riquier ont des hypothèses de départ très proches et démontrent le même résultat. J'explique dans cette section les différences entre la preuve du théorème 16 et la preuve, donnée par Janet, du théorème d'analycité de Riquier. Je me réfère plutôt à la preuve de Janet car celle de Riquier dans [51] est très littérale, et difficile à comprendre. Selon Greg Reid (communication privée), la preuve donnée par Riquier démontre simultanément le problème de l'existence, de l'unicité et de l'analycité, rendant la démonstration complexe.

La preuve de Janet se trouve dans le chapitre II (page 32) et dans la note I (page 109) de [24].

Lemme d'évaluation des monômes. Le lemme d'évaluation de monômes fourni précédemment est identique à celui donné par Janet. Toutefois, Janet en donne une preuve non constructive (qui est insuffisante pour espérer estimer le domaine de convergence des solutions).

Application du lemme d'évaluation des monômes. Janet applique son lemme d'évaluation des monômes d'une façon différente. En effet, les monômes utilisés par Janet comportent en plus des variables de dérivation les indéterminées différentielles. Ceci se justifie car un classement de Riquier peut être décrit par un système de poids sur les indéterminées différentielles et les dérivées. Cette variante a une conséquence sur le point suivant.

Preuve d'inversibilité de la matrice $I - M_a D$. À peu de choses près, Janet doit également inverser une matrice de la forme $I - M_a D$. Toutefois, en raison de la variante sur le lemme d'évaluation des monômes, la matrice D de Janet est différente de celle fournie dans ma preuve.

La construction de D serait trop fastidieuse à expliquer ici. Nous en détaillons cependant un détail important : Janet introduit une matrice $n \times n$ arbitraire (appelons-là J) vérifiant la propriété $||J||_\infty < 1$. De cette matrice J, Janet construit la matrice D de telle manière que $||M_a D||_\infty < 1$. Cela implique d'après la propriété 9 que $I - M_a D$ est inversible.

Ainsi, deux différences sont à signaler :

- l'introduction d'une matrice arbitraire J qui n'est pas nécessaire dans ma preuve ;
- l'utilisation d'une propriété $||M_a D||_\infty < 1$ qui est plus contraignante que la condition $\rho(M_a D) < 1$ car on sait que $||M_a D||_\infty < 1$ implique $\rho(M_a D) < 1$ (mais la réciproque est fausse).

La liberté du choix de la matrice J est à mes yeux surprenante. En effet, le système majorant dépend de la matrice J et on ne sait pas quelles conditions doivent vérifier J pour obtenir un bon système majorant du système initial. En effet, plus le système majorant $\overline{\Sigma}$ majore le système de départ Σ, plus le domaine de convergence de la solution de $\overline{\Sigma}$ est restreint. Ainsi, la liberté du choix de J risque de nuire à l'estimation du domaine de convergence de la solution de Σ.

Ce raisonnement concernant l'estimation du domaine de convergence de la solution n'est bien sûr pas confirmé, et mérite qu'on se penche dessus.

3.7 Démonstration d'analycité sur des exemples

Voici quelques exemples de systèmes qui permettent de mieux comprendre la démonstration du théorème 16. Dans chacun des exemples, nous montrons comment se ramener au théorème de Cauchy-Kovalevskaya dans le cas particulier où il n'y a qu'une dérivation.

Le traitement de ces exemples ne suit pas exactement la preuve du théorème 16. En effet, dans les exemples qui suivent, il y a toujours une seule équation par indéterminée différentielle. Ainsi, la construction du système $\overline{\Sigma}$ se simplifie car on peut éviter la multiplication par les constantes m_i^k.

3.7.1 Exemples à une indéterminée et une équation

3.7.1.1 Exemple 1

$U = \{u\}$, $X = \{x,y\}$.

On considère le classement $\mathcal{R}$ commençant par : $u < u_y < u_x < u_{yy} < u_{xy} < u_{xx} < \cdots$.

$$\Sigma : u_{xx} = 2\,u_{yy} - u_y - u + 1$$

Les dérivées sous l'escalier sont fixées à 0 et on cherche à montrer que la solution à l'origine est analytique (à l'origine).

Soit le système $\overline{\Sigma}$ (qui majore Σ) :

$$u_{xx} = 2\,u_{yy} + a^2(u_y + u + 1)$$

où a est un réel supérieur à 1 dont la valeur sera choisie plus tard. Le nombre a^2 correspond au terme $\theta_{1,1}(\beta)$ de la preuve.

On cherche une solution analytique de $\overline{\Sigma}$ qui majore la fonction nulle. Si une telle solution existe, elle majore la solution en série formelle f de Σ ce qui implique que f est analytique.

On cherche une solution de la forme $u(x,y) = g(a\,x + b\,y)$ avec a et b supérieurs à 1. Nécessairement, il faut (en posant $t = a\,x + b\,y$) :

$$a^2 g''(t) = 2\,b^2 g''(t) + a^2(b\,g'(t) + g(t) + 1)$$

qui donne :

$$(a^2 - 2\,b^2)g''(t) = a^2(b\,g'(t) + g(t) + 1)$$

Si on fixe $g(0) = g'(0) = 0$, on peut appliquer le théorème de Cauchy-Kovalevskaya qui implique que g est analytique. De plus, si on trouve des valeurs de a et b telles que $a^2 - 2\,b^2$ soit strictement positif, la propriété 19 implique que g majore la série formelle nulle.

En posant $a = 2$ et $b = 1$, on a bien $a^2 - 2\,b^2 = 2 > 0$

Sur cet exemple, le choix de a et b était on ne peut plus simple. Ce n'est pas le cas sur des exemples plus complexes comme celui qui suit.

3.7.1.2 Exemple 2

$U = \{u\}$, $X = \{x,y,z\}$.

On considère le classement $\mathcal{R}$ contenant la séquence : $u_{xxx} > u_{xxy} > u_{xxz} > u_{xyy} > u_{xyz} > u_{yyy} > u_{xzz} > u_{yyz} > u_{yzz} > u_{zzz} > \cdots > u$

Ce classement étrange est fourni par la matrice :

$$M = \begin{array}{c} \begin{array}{cccc} x & y & z & u \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

$$\Sigma : u_{xyz} = 2\,u_{yyy} + u_{xzz} + u_{yzz} + u + 1$$

De nouveau, on fixe à 0 les dérivées sous l'escalier et on veut montrer que la solution à l'origine est analytique.

Soit le système $\overline{\Sigma}$ (qui majore Σ) :

$$\overline{\Sigma} : u_{xyz} = 2\,u_{yyy} + u_{xzz} + u_{yzz} + abc(u+1)$$

où a, b, c sont trois réels supérieurs à 1.

En cherchant une solution de la forme $u(x,y,z) = g(a\,x + b\,y + c\,z)$, on a (en posant $t = ax + by + cz$) :

$$(abc - 2\,b^3 - ac^2 - bc^2)g^{(3)}(t) = abc(g(t)+1)$$

On cherche alors des valeurs pour a, b et c telles que $abc - 2\,b^3 - ac^2 - bc^2$ soit positif. De telles valeurs existent car on peut appliquer le lemme d'évaluation des monômes 13 sur les opérateurs de dérivation ordonnés par l'ordre admissible donné par la matrice :

$$\overline{M} = \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{array}$$

Remarque : cette matrice $\overline{M}$ est composée des trois premières colonnes de M.

Soit $\alpha > 1$ un réel. Le lemme 13 et la propriété 22 fournissent des valeurs a, b et c supérieures à 1 telles que les rapports $b^3/(abc)$, $ac^2/(abc)$ et $bc^2/(abc)$ soient inférieurs à $1/\alpha$.

Ainsi, on a :

$$\begin{aligned} abc - 2\,b^3 - ac^2 - bc^2 &= abc(1 - 2\,b^3/(abc) - ac^2/(abc) - bc^2/(abc)) \\ &\geq abc\,(1 - 2/\alpha - 1/\alpha - 1/\alpha) \\ &\geq abc\,(1 - 4/\alpha) \end{aligned}$$

Si on choisit $\alpha = 5$, on a : $abc - 2\,b^3 - ac^2 - bc^2 \geq abc\,(1 - 4/5) > 0$. On conclut alors de la même manière que dans l'exemple précédent.

Remarque : le calcul des valeurs de a, b et c est détaillé dans l'exemple qui suit la propriété 22.

3.7.2 Exemples à deux indéterminées et deux équations

Le cas d'un équation à une indéterminée se comprend assez bien dès que l'on a compris le lemme d'évaluation des monômes. Le cas de deux équations à deux indéterminées révèle quelques surprises.

Dans le cas de deux équations (et plus), la condition scalaire de positivité (des deux exemples précédents) se transforme en une condition sur les matrices.

3.7.2.1 Exemple 1

Commençons par un exemple simple.

Soit $\mathcal{R}$ un classement commençant par : $v < u < v_z < u_z < v_y < u_y < v_x < u_x < \cdots$.

$$\Sigma \left\{ \begin{array}{rcl} u_x & = & v_x + u_y + u + 1 \\ v_y & = & u_z + v_z + v + 1 \end{array} \right.$$

Soit le système $\overline{\Sigma}$ (qui majore Σ) :

$$\overline{\Sigma} \left\{ \begin{array}{rcl} u_x & = & v_x + u_y + a(u+1) \\ v_y & = & u_z + v_z + b(v+1) \end{array} \right.$$

avec a et b réels supérieurs à 1.

On cherche une solution $u(x,y,z) = g(ax+by+cz)$ et $v(x,y,z) = h(ax+by+cz)$ avec c réel supérieur à 1. Le système $\overline{\Sigma}$ donne (en posant $t = ax+by+cz$) :

$$\left\{ \begin{array}{rcl} ag'(t) & = & ah'(t) + bg'(t) + a(g(t)+1) \\ bh'(t) & = & cg'(t) + ch'(t) + b(h(t)+1) \end{array} \right.$$

que l'on réécrit (en normalisant les dérivées de gauche) en :

$$\left\{ \begin{array}{rcl} g' & = & h' + (b/a)g' + g + 1 \\ h' & = & (c/b)g' + (c/b)h' + h + 1 \end{array} \right.$$

On reformule ce système matriciellement :

$$(I - D)(g',h')^t = (g+1,h+1)^t$$

où I est la matrice identité 2×2 et où D est la matrice :

$$D = \begin{pmatrix} b/a & 1 \\ c/b & c/b \end{pmatrix}$$

Il faut alors montrer que la matrice $I - D$ est inversible, et que son inverse E est à coefficients tous positifs. En effet, on est alors ramené au système :

$$(g',h')^t = E(g+1,h+1)^t$$

dont la solution (en fixant $g(0) = h(0) = 0$) est à coefficients tous positifs d'après la propriété 19.

En choisissant a, b et c de manière à ce que les rapports b/a et c/b soient petits (fixons $1/10$), la matrice $I - D$ vaut alors :

$$I - D = \begin{pmatrix} 9/10 & -1 \\ -1/10 & 9/10 \end{pmatrix}$$

dont l'inverse E est :

$$E = \begin{pmatrix} 90/71 & 100/71 \\ 10/71 & 90/71 \end{pmatrix}$$

On notera au passage que $||D||_1$ et $||D||_\infty$ sont strictement supérieurs à 1 (à cause du coefficient 1), quelles que soient les valeurs attribuées a, b et c.

3.7.2.2 Exemple 2

$U = \{u,v\}$, $X = \{x,y,z\}$.

On considère le classement $\mathcal{R}$ contenant la séquence : $u_{xx} > u_{xy} > u_{yy} > v_{xx} > u_{xz} > v_{xy} > u_{yz} > v_{yy} > v_{xz} > u_{zz} > v_{yz} > v_{zz}$

Un calcul montre que la séquence précédente est obtenue pour n'importe quelle matrice M dont les deux premières lignes sont :

$$\begin{array}{c} \begin{array}{ccccc} x & y & z & u & v \end{array} \\ \left(\begin{array}{ccccc} 1 & 1 & 1 & 0 & 0 \\ 1.1 & 1 & 0 & 1.01 & 0 \end{array} \right) \end{array}$$

Considérons le système :

$$\Sigma \left\{ \begin{array}{rcl} u_{yy} & = & u_{zz} + v_{xx} + u + 1 \\ v_{xy} & = & u_{yz} + v_{xz} + v + 1 \end{array} \right.$$

Soit le système $\overline{\Sigma}$ (qui majore Σ) :

$$\overline{\Sigma} \left\{ \begin{array}{rcl} u_{yy} & = & u_{zz} + v_{xx} + b^2(u + 1) \\ v_{xy} & = & u_{yz} + v_{xz} + ab(v + 1) \end{array} \right.$$

où a et b sont réels et supérieurs à 1.

On cherche une solution de $\overline{\Sigma}$ de la forme $u(x,y,z) = g(ax + by + cz)$ et $v(x,y,z) = h(ax + by + cz)$ avec c réel et supérieur à 1. On obtient (avec $t = ax + by + cz$) :

$$\left\{ \begin{array}{rcl} b^2 g'' & = & c^2 g'' + a^2 h'' + b^2(g + 1) \\ abh'' & = & bcg'' + ach'' + ab(h + 1) \end{array} \right.$$

que l'on réécrit (en normalisant les dérivées de gauche) en :

$$\left\{ \begin{array}{rcl} g'' & = & (c^2/b^2)g'' + (a^2/b^2)h'' + g + 1 \\ h'' & = & (bc/ab)g'' + (ac/ab)h'' + h + 1 \end{array} \right.$$

On reformule ce système matriciellement :

$$(I - D)(g'',h'')^t = (g + 1,h + 1)^t$$

où I est la matrice identité 2×2 et où D est la matrice :

$$D = \left(\begin{array}{cc} c^2/b^2 & a^2/b^2 \\ bc/ab & ac/ab \end{array} \right)$$

Nous voulons prouver que $I - D$ est inversible et que son inverse E est à coefficients positifs.

L'ordre sur les opérateurs de dérivation induit par $\mathcal{R}$ est : $x^2 > xy > y^2 > xz > yz > z^2$. Si on applique le lemme d'évaluation des monômes 13 et la propriété 22, on obtient des valeurs a, b et c supérieurs à 1 qui vérifient :

$$a^2/(ab) \geq \alpha \quad ab/(b^2) \geq \alpha \quad b^2/(ac) \geq \alpha \quad ac/(bc) \geq \alpha \quad bc/c^2 \geq \alpha$$

En raisonnant comme dans les exemples précédents, on cherche une valeur de α suffisamment grande pour que $I - D$ soit inversible. L'exemple est intéressant car un des coefficients de D vaut a^2/b^2. Ce coefficient est supérieur à α^2 et augmente donc si α augmente.

Malgré ce terme a priori embarrassant, la matrice $I - D$ est tout de même inversible d'inverse $I + D + D^2 + \cdots$, qui est bien une matrice à coefficients positifs. Pour montrer que $I - D$ est inversible, on montre que le rayon spectral de D est inférieur à 1 pour α suffisamment grand. Le polynôme caractéristique $p(x)$ de D est :

$$p(x) = \det(D - xI) = x^2 - (c^2/b^2 + ac/ab)x + (c^2/b^2)(ac/ab) - (bc/ab)(a^2/b^2)$$

Le terme $c^2/b^2 + ac/ab$ est inférieur à $1/\alpha^3 + 1/\alpha$. Le terme $(c^2/b^2)(ac/ab)$ est inférieur à $1/\alpha^2$. Le dernier terme $(bc/ab)(a^2/b^2)$ contenant le terme gênant (a^2/b^2) peut être réécrit (en échangeant les dénominateurs) en faisant apparaître des rapports inférieurs à $1/\alpha$:

$$(bc/ab)(a^2/b^2) = (bc/b^2)(ab/a^2)$$

Ce terme est lui aussi inférieur à $1/\alpha^2$. Par conséquent, les coefficients du polynôme caractéristique de D peuvent être rendus arbitrairement petits. Pour une valeur suffisamment grande de α, on applique le lemme 11 de majoration des racines qui nous assure que le rayon spectral de D est strictement inférieur à 1. On termine le raisonnement avec les lemmes 8 et 9 qui impliquent que $I - D$ est inversible d'inverse $I + D + D^2 + \cdots$.

Chapitre 4

L'algorithme regCaractéristique

Sommaire

L'algorithme regCaractéristique est une alternative à la phase algébrique de Rosenfeld–Gröbner. Il a été publié dans l'article [10]. Partant d'un système différentiel régulier $A = 0$, $S \neq 0$ vérifiant $H_A \subset S$, cet algorithme calcule t présentations caractéristiques $C_1, \ldots, C_t$ vérifiant :

$$[A] : S^\infty = [C_1] : {H_{C_1}}^\infty \cap \cdots \cap [C_t] : {H_{C_t}}^\infty$$

De plus, la décomposition $C_1, \ldots, C_t$ est non redondante i.e. tout premier minimal de $[A] : S^\infty$ est un premier minimal d'un seul $[C_i] : {H_{C_i}}^\infty$. Cet algorithme remplace les calculs de base de Gröbner en manipulant des ensembles triangulaires.

L'algorithme regCaractéristique réduit d'abord le problème à un problème en dimension zéro[21]. La technique a déjà été évoquée : elle consiste à faire passer dans le corps des coefficients les dérivées de $A \cup S$ qui ne sont dérivées dominantes d'aucun des polynômes de A. Cette étape est purement formelle. On applique ensuite un sous–algorithme, appelé satTriangular, qui calcule t ensembles triangulaires fortement normalisés $T_1, \ldots, T_t$ qui (presque immédiatement) fournissent les présentations caractéristiques désirées $C_1, \ldots, C_t$

L'algorithme satTriangular a un fonctionnement proche de celui de lextriangular [32, page 129, algorithme D5lextriangular] [41] et [39, page 133] qui applique le mécanisme D5 [18]. Citons [32, page 129] : lextriangular prend en entrée une base de Gröbner B d'un idéal de dimension zéro de l'anneau des polynômes en $X_1, \ldots, X_n$ (pour l'ordre lexicographique induit par $X_1 < \cdots < X_n$) classée par monômes de tête croissants et calcule un nombre fini d'ensembles triangulaires $T_1, \ldots, T_t$ vérifiant :

$$V(B) = V(T_1) \cup \cdots \cup V(T_t)$$

où $V(T_i)$ désigne l'ensemble des zéros communs des éléments de T_i dans la clôture algébrique du corps de base.

Notre implantation de satTriangular est directement inspirée de [41, 39] (nous n'apportons aucune amélioration algorithmique) : elle utilise un algorithme de sous–résultants dans l'anneau quotient défini par l'ensemble triangulaire en construction au lieu de calculer la suite génériquement et de la spécialiser ensuite.

Il y a toutefois des différences théoriques importantes entre satTriangular and lextriangular : nous travaillons avec un système d'équations polynomiales $\overline{A} = 0$, $\overline{S} \neq 0$ qui n'est pas une base de Gröbner[22] ; de plus, les propriétés de la sortie de satTriangular (propriétés **P1** à **P5** formulées en section 4.2) sont plus fortes que celles de la sortie lextriangular. Pour cette raison, nous avons dû écrire des preuves adaptées à satTriangular.

Nous avons implanté deux versions de Rosenfeld–Gröbner basés sur regCaractéristique, l'une en Maple Vr5 (moi-même), l'autre en C++ (F. Boulier). Comparons maintenant les méthodes existantes (écrites en Maple) à notre algorithme regCaractéristique.

Wang et Li résolvent le même problème dans [34] en utilisant l'algorithme SimSys [63] qui manipule des systèmes polynômiaux généraux. Ils affirment [34, p. 59] qu'un algorithme plus spécialisé que SimSys pourrait être appliqué : l'algorithme regCaractéristique en est un exemple.

21. Comme le font [8] et [23]

22. Cela est anecdotique car les conséquences algorithmiques du théorème de Gianni et Kalkbrener ne s'appliquent pas dans notre cas

Dans [8], l'étape algébrique est résolue en calculant d'abord une base de Gröbner de l'idéal localisé $S^{-1}(A)$. Ce calcul est coûteux et ne prend pas en compte le caractère déjà triangulaire du système A. De plus, ce calcul de base de Gröbner calcule explicitement tous les inverses des éléments de S, alors que seuls les inverses des initiaux de A sont utiles.

L'algorithme 7.1 dans [23] utilise exactement les mêmes principes que regCaractéristique. La seule différence est que cet algorithme calcule une base de Gröbner de $S^{-1}(A)$ au lieu d'appeler satTriangular. Il souffre donc des mêmes inconvénients mentionnés ci–dessus pour [8]. Notons que l'article [23] est le premier à prouver complètement que le calcul de présentations caractéristiques à partir d'un système différentiel régulier est un problème purement algébrique de dimension zéro. Ceci était seulement énoncé dans [8, page 35].

Pour finir, tester l'inversibilité de polynômes différentiels modulo un ensemble triangulaire pour construire des ensembles caractéristiques était déjà appliqué dans [36, 12]. Toutefois, la méthode est différente de la nôtre, car elle est basée sur un calcul de base de Gröbner (voir [12, page 7] et [36, page 29]).

Dans tout ce chapitre, on ne considère qu'un seul classement $\mathcal{R}$. Ce classement ne sera donc pas explicitement rappelé car aucune confusion n'est possible.

4.1 Spécification

Soit $A = 0$, $S \neq 0$ un système différentiel régulier de R tel que $H_A \subset S$. L'algorithme regCaractéristique calcule t ensembles $C_1, \ldots, C_t$ vérifiant :

A1 chaque C_i est la présentation caractéristique de $[C_i] : {H_{C_i}}^\infty$;

A2 $[A] : S^\infty = [C_1] : {H_{C_1}}^\infty \cap \cdots \cap [C_t] : {H_{C_t}}^\infty$;

A3 l'intersection **A2** est non redondante i.e. si $\mathfrak{p}$ est un idéal premier différentiel minimal de $[A] : S^\infty$, alors $\mathfrak{p}$ est un premier différentiel minimal d'un et d'un seul $[C_i] : {H_{C_i}}^\infty$.

4.2 L'algorithme

4.2.1 regCaractéristique

On note X l'ensemble des dérivées des polynômes de $A \cup S$, L l'ensemble des dérivées dominantes des polynômes de A et on pose $N = X \setminus L$. On pose $G = K(N)$.

Voici les trois étapes de regCaractéristique :

1. Plonger le système $A = 0$, $S \neq 0$ dans $K(N)[L]$. On note $\overline{A} = 0$, $\overline{S} \neq 0$ le système obtenu. Cette étape est purement formelle ;
2. Appliquer l'algorithme satTriangular à $\overline{A} = 0$, $\overline{S} \neq 0$. On récupère un ensemble (éventuellement vide) de t ensembles autoréduits normalisés sans-carrés $\{T_1, \ldots, T_t\}$;
3. Pour $1 \leq i \leq t$, construire C_i à partir de T_i de la façon suivante : C_i est l'ensemble des parties primitives sur $K[N]$ des numérateurs des éléments de T_i. Les systèmes $C_1, \ldots, C_t$ sont les présentations caractéristiques recherchées.

4.2.2 satTriangular

L'algorithme satTriangular prend en entrée un système algébrique $\overline{A} = 0$, $\overline{S} \neq 0$ vérifiant $H_{\overline{A}} \subset \overline{S}$. Il calcule un ensemble (éventuellement vide) de t chaînes régulières normalisées[23] sans-carré $\{T_1, \ldots, T_t\}$ vérifiant :

P1 si $t = 0$ (l'ensemble est vide), $\overline{A} : \overline{S}^\infty = G[L]$;
P2 $\overline{A} : \overline{S}^\infty = (T_1) \cap \cdots \cap (T_t)$;
P3 si $i \neq j$, alors $(T_i) + (T_j) = (1) = G[L]$;
P4 pour $1 \leq i \leq t$, on a $(T_i) = (T_i) : {H_{T_i}}^\infty$;
P5 $\mathrm{ld}\, A = \mathrm{ld}\, T$.

Nous ne présentons pas l'algorithme sous forme de pseudo-code mais d'une manière mettant en avant les deux idées–clés : traiter une inéquation et normaliser un polynôme.

L'algorithme satTriangular construit une séquence finie $(\mathcal{F}_i)_{1 \leq i \leq r}$ de r ensembles d'équations et d'inéquations de la manière suivante :

Initialement, prendre $\mathcal{F}_0 = \{(\overline{A} = 0, \overline{S} \neq 0)\}$. On suppose qu'on a construit l'ensemble $\mathcal{F}_i$. L'un des deux cas peut se produire :

- Posons $\mathcal{F}_i = \{(T_1 = 0, S_1 \neq 0), \ldots, (T_t = 0, S_t \neq 0)\}$. Si chaque T_i est un ensemble normalisé et que chaque S_i est vide, l'algorithme s'arrête en renvoyant le résultat : $\{T_1, \ldots, T_t\}$;
- $\mathcal{F}_i$ contient un système $(A = 0, S \neq 0)$ tel que A contienne un polynôme non normalisé ou tel que S soit non vide. Transformer $(A = 0, S \neq 0)$ en utilisant l'une ou l'autre des règles **R1** ou **R2** décrite ci-dessous. Ces deux règles renvoient un ensemble $\mathcal{F}$ de zéro, un ou deux systèmes d'équations et d'inéquations. Prendre alors $\mathcal{F}_{i+1} = \mathcal{F}_i \setminus \{(A = 0, S \neq 0)\} \cup \mathcal{F}$.

Dans les deux règles qui suivent, on pose $L = \{X_1, \ldots, X_m\}$ avec $X_1 < \cdots < X_m$.

R1 : essayer de normaliser un polynôme Si A contient un ensemble triangulaire normalisé $\{p_1, \ldots, p_{k-1}\}$ de $G[X_1, \ldots, X_{k-1}]$ et un polynôme p_k non unitaire de variable principale X_k, alors trois cas sont possibles :

R1.1 L'initial de p_k est nul modulo l'idéal $(p_1, \ldots, p_{k-1})$.
Prendre $\mathcal{F} = \emptyset$;

R1.2 inverse trouve un inverse q de l'initial i_{p_k} modulo $(p_1, \ldots, p_{k-1})$.
Prendre $\mathcal{F} = \{A' = 0, S \neq 0\}$ où $A' = A \setminus \{p_k\} \cup \{\mathsf{prem}(q\, p_k, \{p_1, \ldots, p_{k-1}\})\}$;

R1.3 inverse ne trouve pas l'inverse de i_{p_k} modulo $(p_1, \ldots, p_{k-1})$ mais découvre une factorisation $p_j = g\, h \mod (p_1, \ldots, p_{j-1})$ avec $1 \leq j < k$.
Prendre $\mathcal{F} = \{(A_g = 0, S \neq 0), (A_h = 0, S \neq 0)\}$ où $A_g = A \setminus \{p_j\} \cup \{g\}$ et $A_h = A \setminus \{p_j\} \cup \{h\}$.

23. Comme on travaille en dimension zéro, toute chaîne régulière normalisée est fortement normalisée.

R2 : essayer d'inverser une inéquation Si A contient un ensemble triangulaire normalisé $\{p_1, \ldots, p_k\}$ de $G[X_1, \ldots, X_k]$ et si S contient une inéquation s telle que $\mathrm{ld}\, s = \mathrm{ld}\, p_k = X_k$, alors trois cas sont possibles :

R2.1 s vaut 0 modulo $(p_1, \ldots, p_k)$.
Prendre $\mathcal{F} = \emptyset$;

R2.2 inverse trouve l'inverse de s modulo $(p_1, \ldots, p_k)$.
Prendre $\mathcal{F} = \{(A = 0,\ S' \neq 0)\}$ où $S' = S \setminus \{s\}$;

R2.3 inverse ne trouve pas l'inverse de s modulo $(p_1, \ldots, p_k)$ mais découvre une factorisation $p_j = g\, h \mod (p_1, \ldots, p_{j-1})$ avec $1 \leq j \leq k$.
Prendre $\mathcal{F} = \{(A_g = 0,\ S \neq 0), (A_h = 0,\ S \neq 0)\}$ où $A_g = A \setminus \{p_j\} \cup \{g\}$ et $A_h = A \setminus \{p_j\} \cup \{h\}$.

4.3 Preuve de regCaractéristique

L'algorithme regCaractéristique se prouve en montrant les points **A1**, **A2** et **A3**. De ces trois points, le point **A1** (chaque C_i est la présentation caractéristique de $[C_i] : {H_{C_i}}^{\infty}$) est particulièrement important et intéressant.

En effet, ce point précise que les ensembles C_i obtenus ont, en particulier, leurs paires critiques résolues. Ceci est remarquable car le traitement purement algébrique appliqué à $A = 0,\ S \neq 0$ va conserver une propriété différentielle à savoir que les paires critiques sont résolues. Évelyne Hubert est la première à avoir démontré ce point dans [23] (le lecteur pourra se référer aux théorèmes 3.10 et 6.2 de [23]). Nous fournissons toutefois une preuve complète de regCaractéristique qui a l'avantage d'être adaptée aux notations de cette thèse.

La preuve qui suit suppose que l'on dispose de l'algorithme satTriangular qui est fourni dans les prochaines sous–sections. Nous démontrons d'abord quelques lemmes utiles avant de prouver les trois points.

Soit Φ l'injection canonique $K[X] = K[N,L] \to G[L] = K(N)[L]$.

Lemme 15 $(A) : S^{\infty} = (C_1) : {H_{C_1}}^{\infty} \cap \cdots \cap (C_t) : {H_{C_t}}^{\infty}$

Preuve :

La relation ci-dessus s'obtient en appliquant Φ^{-1} (composante par composante) sur la relation **P2** (reformulée en utilisant **P4**) : $(\overline{A}) : \overline{S}^{\infty} = (T_1) : {H_{T_1}}^{\infty} \cap \cdots \cap (T_t) : {H_{T_t}}^{\infty}$.

En effet, Φ^{-1} conserve les intersections d'après [21, proposition 2.2]. De plus, les éléments non nuls de $K[N]$ n'appartiennent à aucun des idéaux premiers minimaux de $(A) : S^{\infty}$ (resp. $(T_i) : {H_{T_i}}^{\infty}$) d'après le lemme 2 (resp. d'après le lemme 2 et d'après **P5**). Ainsi, en utilisant de nouveau [21, proposition 2.2] et ce qui précède, Φ^{-1} envoie $(\overline{A}) : \overline{S}^{\infty}$ sur $(A) : S^{\infty}$ et les $(T_i) : {H_{T_i}}^{\infty}$ sur les $(C_i) : {H_{C_i}}^{\infty}$ □

Lemme 16 *Un idéal premier* $\mathfrak{b}$ *est un premier minimal de* $(A) : S^{\infty}$ *si et seulement si* $\mathfrak{b}$ *est un premier minimal de l'un des* $(C_i) : {H_{C_i}}^{\infty}$.

Preuve :

D'après **P5** et le lemme 2, les idéaux premiers minimaux de $(A) : S^\infty$ et ceux des $(C_i) : {H_{C_i}}^\infty$ ont tous même dimension. Le lemme est conséquence du lemme 15 et de la propriété suivante : si $\mathfrak{b} \subset \mathfrak{b}'$ sont deux idéaux premiers de même dimension, alors $\mathfrak{b} = \mathfrak{b}'$

□

Lemme 17 *Chaque système $C_i = 0$, $H_{C_i} \neq 0$ est un système différentiel régulier.*

Preuve :

On prouve les 3 conditions **C1**, **C2** et **C3** de la définition d'un ensemble différentiel régulier. D'après **P5**, la condition **C1** est remplie. La condition **C2** est également vérifiée.

Il suffit donc de prouver **C3** (propriété de cohérence). Soit $\{p,p'\} \in$ paires_critiques(C_i). Soit $v = \mathrm{ppdc}(\mathrm{ld}\, p, \mathrm{ld}\, p')$. On doit prouver qu'il existe $w < v$ tel que $\Delta(p,p') \in (C_{iw}) : {H_{C_i}}^\infty$. Il suffit en fait de montrer que $\mathsf{reste\_complet}(\Delta(p,p'),C_i) \in (C_i) : {H_{C_i}}^\infty$ ce qui équivaut à $\mathsf{reste\_complet}(\Delta(p,p'),C_i) \in \mathfrak{b}$ pour tout premier minimal $\mathfrak{b}$ sur $(C_i) : {H_{C_i}}^\infty$.

D'après les lemmes 4 et 16, un premier minimal $\mathfrak{b}$ sur $(C_i) : {H_{C_i}}^\infty$ est l'intersection d'un premier différentiel $\mathfrak{p}$ minimal sur $[A] : S^\infty$ avec $K[X]$. Comme p et p' sont dans $\mathfrak{p}$ et $C_i \subset \mathfrak{p}$, on a $\mathsf{reste\_complet}(\Delta(p,p'),C_i) \in \mathfrak{p}$. Comme $\mathsf{reste\_complet}(\Delta(p,p'),C_i)$ est réduit par rapport à C_i et d'après **P5**, on a $\mathsf{reste\_complet}(\Delta(p,p'),C_i) \in K[X]$ et donc $\mathsf{reste\_complet}(\Delta(p,p'),C_i) \in (K[X] \cap \mathfrak{p}) = \mathfrak{b}$ □

Lemme 18 *Soit $1 \leq i \leq n$. L'ensemble C_i est une chaîne régulière sans carré.*

Preuve :

En utilisant le théorème 1 et la propriété 5, il suffit de prouver l'équivalence suivante : $p \in (C_i) : {H_{C_i}}^\infty \iff \mathsf{prem}(p,C_i) = 0$ pour tout p de $K[X]$.

L'implication de droite à gauche découle immédiatement des propriétés de réduction d'un polynôme par un ensemble.

L'implication de gauche à droite résulte des quatre propriétés suivantes :

- $p \in (C_i) : {H_{C_i}}^\infty \iff \Phi(p) \in (T_i) : {H_{T_i}}^\infty = (T_i)$ (d'après **P4**) ;
- $\mathsf{prem}(p,C_i) = 0 \iff \mathsf{prem}(\Phi(p),T_i) = 0$;
- $\mathsf{prem}(\Phi(p),T_i) = 0 \iff \Phi(p) \xrightarrow[T_i]{*} 0$ car[24] les éléments de T_i sont unitaires ;
- T_i est une base de Gröbner (pour l'ordre lexicographique induit par l'ordre sur L) de (T_i) d'après [4, lemme 5.66, premier critère de Buchberger] et T_i réduit donc à 0 tous les éléments de (T_i) d'après [4, proposition 5.38].

□

Nous pouvons maintenant prouver les conditions **A1**, **A2** et **A3**.

Proposition 1 *(condition **A1**)*

Soit $1 \leq i \leq t$. L'ensemble C_i est une présentation caractéristique de l'idéal $[C_i] : {H_{C_i}}^\infty$.

24. La flèche représente la réduction au sens des bases de Gröbner

Preuve :
D'après les lemmes 17 et 18, C_i est une chaîne différentielle régulière. L'ensemble C_i est autoréduit parce que C_i vérifie **P5** et que A est autoréduit ; la condition **D1** est donc vérifiée. Tous les polynômes de C_i sont fortement normalisés car ils sont obtenus en multipliant des polynômes unitaires de $G[L]$ par des polynômes de $K[N]$; ainsi **D2** est vérifiée. Les polynômes de C_i sont primitifs par construction. Ainsi, C_i satisfait la condition **D3**. □

Lemme 19 *Un idéal différentiel premier $\mathfrak{p}$ est mininal sur $[A] : S^\infty$ si et seulement si c'est un premier minimal sur l'un des $[C_i] : {H_{C_i}}^\infty$.*

Preuve :
C'est une conséquence des lemmes 16, 17 et 4. □

Proposition 2 *(condition **A2**)*

$$[A] : S^\infty = [C_1] : {H_{C_1}}^\infty \cap \cdots \cap [C_t] : {H_{C_t}}^\infty$$

Preuve :
Cette proposition découle du lemme 19. □

Proposition 3 *(condition **A3**)*
Si $\mathfrak{p}$ est un premier différentiel minimal de $[A] : S^\infty$, alors $\mathfrak{p}$ est un premier minimal d'exactement un des $[C_i] : {H_{C_i}}^\infty$.

Preuve :
D'après le lemme 19, $\mathfrak{p}$ est un premier minimal d'au moins l'un des $[C_i] : {H_{C_i}}^\infty$. Supposons que $\mathfrak{p}$ soit un premier minimal de $[C_i] : {H_{C_i}}^\infty$ et de $[C_j] : {H_{C_j}}^\infty$. D'après le lemme 4, l'idéal $\mathfrak{b}$ donné par $\mathfrak{b} = \mathfrak{p} \cap K[X]$ est un premier minimal de $(C_i) : {H_{C_i}}^\infty$ et $(C_j) : {H_{C_j}}^\infty$. Ainsi, $(\Phi(\mathfrak{b}))$ est un idéal premier minimal de (T_i) et de (T_j). En supposant $i \neq j$ et en utilisant **P3**, on a $(\Phi(\mathfrak{b})) = G[L]$ ce qui est contradictoire. Ainsi, $i = j$ ce qui termine cette preuve. □

4.4 Preuve de satTriangular

La preuve de satTriangular utilise essentiellement des raisonnements sur les variétés algébriques. Ces derniers sont simples car on travaille en dimension 0.

Lemme 20 *Soit I un idéal de $G[L]$ de dimension 0. Soit S une famille finie d'éléments de $G[L]$. Alors $I = I : S^\infty$ ssi pour chaque $s \in S$ et pour tout $z \in V(I)$, on a $s(z) \neq 0$.*

Preuve :
On peut supposer, pour alléger la preuve, que l'ensemble S est réduit à un seul élément s. D'après le théorème de Lasker–Nœther (théorème 3), l'idéal I est l'intersection, supposée minimale, de m idéaux primaires $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$.

$$I : \{s\}^\infty = \mathfrak{q}_1 : \{s\}^\infty \cap \cdots \cap \mathfrak{q}_m : \{s\}^\infty$$

La décomposition étant minimale, les idéaux primaires $\mathfrak{q}_i$ sont de dimension 0.

En outre, pour tout $z \in V(I)$, on a $s(z) \neq 0$. Comme I est de dimension 0, s n'appartient à aucun des premiers associés à I qui sont $\sqrt{\mathfrak{q}_1}$, ..., $\sqrt{\mathfrak{q}_m}$.

On peut alors appliquer la propriété $s \notin \sqrt{\mathfrak{q}_i} \implies \mathfrak{q}_i : \{s\}^\infty = \mathfrak{q}_i$ qui implique que :

$$I : \{s\}^\infty = \mathfrak{q}_1 : \{s\}^\infty \cap \cdots \cap \mathfrak{q}_m : \{s\}^\infty = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m = I$$

□

Proposition 4 *Pour $1 \leq i \leq r$, $\mathcal{F}_i$ vérifie les quatre relations invariantes (que nous appellerons par la suite invariants) suivantes. On note $\mathcal{F}_i = \{(A_1 = 0,\ S_1 \neq 0), \ldots, (A_t = 0,\ S_t \neq 0)\}$.*

I1 $\bigcap_{1 \leq i \leq t} (A_l) : {S_l}^\infty = (\overline{A}) : \overline{S}^\infty$;

I2 $(A_l) : {S_l}^\infty = (A_l) : (S_l \cup H_{A_l})^\infty$ *pour* $1 \leq l \leq t$;

I3 $(A_l) : {S_l}^\infty + (A_{l'}) : {S_{l'}}^\infty = G[L]$ *pour* $1 \leq l < l' < t$;

I4 A_l *est triangulaire et* $\operatorname{ld} A_l = L$ *pour* $1 \leq l \leq t$.

Preuve :

Les invariants **I1**, **I2** et **I3** permettent de prouver la sortie de l'algorithme.

L'invariant **I4** a un rôle uniquement algorithmique. Il est nécessaire pour affirmer la chose suivante : si $(A = 0,\ S \neq 0) \in \mathcal{F}_i$ avec A non normalisé ou S non vide, alors l'une des deux règles **R1** ou **R2** s'applique. En effet, ces deux règles ne s'appliquent que si A contient un sous–ensemble triangulaire normalisé, ce qui est le cas si l'invariant **I4** est vérifié.

La preuve se fait par récurrence sur l'indice i des $\mathcal{F}_i$. $\mathcal{F}_0$ vérifie bien évidemment les quatre invariants. Supposons que $\mathcal{F}_i$ vérifie les quatre invariants. On va prouver que $\mathcal{F}_{i+1}$ vérifie également les quatre invariants. Pour ce faire, on distingue six cas, qui correspondent aux six manières dont peut être construit $\mathcal{F}_{i+1}$. Notez que l'invariant **I4** est évident dans chacun des cas qui suivent, et ne sera donc pas évoqué.

R1.1 Il suffit de prouver que $(A) : S^\infty = G[L]$. L'initial de p_k appartient à (A) et à H_A. Ainsi $(A) : (S \cup H_A)^\infty = G[L]$. Par l'invariant **I2**, on a $(A) : S^\infty = G[L]$.

R1.2 On a $(A) = (A')$ car $q\, p_k \in (A)$ et $p = i_{p_k}\, q\, p_k \mod (p_1, \ldots, p_{k-1})$. En saturant par S, on a $(A) : S^\infty = (A') : S^\infty$ ce qui prouve **I1** et **I3**.

Il reste à prouver **I2** pour $\mathcal{F}_{i+1}$. D'après **I2** (pour $\mathcal{F}_i$), on a $(A) : S^\infty = (A) : (S \cup H_a)^\infty$. Le lemme 20 implique que les polynômes de H_A ne s'annulent pas sur les zéros de $(A) : S^\infty$. Comme $H_{A'} = H_A \setminus \{i_{p_k}, s_{p_k}\} \cup \{1, \overline{s}\}$ avec $\overline{s} = q\, s_{p_k} \mod (p_1, \ldots, p_{k-1})$, les polynômes de $H_{A'}$ ne s'annulent pas non plus sur les zéros de $(A) : S^\infty$.

Ainsi, en utilisant le lemme 20, on a

$$(A) : S^\infty = (A) : (S \cup H_{A'})^\infty = (A') : S^\infty = (A') : (S \cup H_{A'})^\infty$$

ce qui prouve **I2**.

R1.3 Une factorisation a été détectée : $p_j = g\,h \mod (p_1,\ldots,p_{j-1})$ avec $1 \leq j < k$. Comme p_j, g et h ont même variable principale, on a $s_{p_j} = s_g\,h + g\,s_h \mod (p_1,\ldots,p_{j-1})$.

Notons $I = (A) : S^\infty$, $I_g = (A_g) : S^\infty$ et $I_h = (A_h) : S^\infty$.

*On prouve **I3** :* Il suffit de prouver :

$$V(I_g) \cup V(I_h) = V(I) \tag{4.1}$$
$$V(I_g) \cap V(I_h) = \emptyset \tag{4.2}$$

On a $V(I) \supset V(I_g) \cup V(I_h)$ car $I \subset I_g$ et $I \subset I_h$.

Inversement, soit $z \in V(I)$. On a :

$$\begin{aligned} g(z)\,h(z) &= 0 \\ s_g(z)\,h(z) + g(z)\,s_h(z) &\neq 0 \end{aligned} \tag{4.3}$$

Ainsi, si $g(z) = 0$ alors $s_g(z) \neq 0$ et $h(z) \neq 0$. De même, si $g(z) \neq 0$, alors $s_h(z) = 0$ et $h(z) = 0$. Cela implique que z est soit zéro de I_g, soit zéro de I_h et qu'il ne peut pas être zéro des deux. Cela prouve les relations (4.1) et (4.2) et **I3** est donc prouvé.

*On prouve **I2** :* En utilisant l'invariant **I2** de $\mathcal{F}_i$ et le lemme 20, les polynômes de H_A ne s'annulent pas sur $V(I)$. D'après la relation (4.1), ils ne s'annulent pas non plus sur $V(I_g)$. Le polynôme s_g ne s'annule pas sur $V(I_g)$ d'après (4.3). On a $H_{A_g} = H_A \setminus \{s_{p_j}\} \cup \{s_g\}$. Ainsi, d'après le lemme 20, $(A_g) : S^\infty = (A_g) : (S \cup H_{A_g})^\infty$. La même preuve s'applique pour l'idéal I_h. Ceci prouve donc l'invariant **I2**.

*On prouve **I1** :* En utilisant le théorème des zéros, $\sqrt{I} = \sqrt{I_g} \cap \sqrt{I_h}$. D'après l'invariant **I2** et le lemme 2, les trois idéaux I, I_g et I_h sont radicaux. Ainsi, $I = I_g \cap I_h$ et l'invariant **I1** est vérifié.

R2.1 La preuve est similaire au cas **R1.1**.

R2.2 L'inéquation s admet un inverse q. On a donc $s\,q = 1 \mod (p_1,\ldots,p_k)$. Ainsi, s ne s'annule pas sur les zéros de $(A) : S^\infty$ (car un zéro de $(A) : S^\infty$ annule $p_1,\ldots,p_k$). Grâce au lemme 20, on a $(A) : S^\infty = (A) : S'^\infty$ ce qui prouve **I1**, **I2** et **I3**.

R2.3 La preuve est similaire au cas **R1.3**.

La proposition 4 est donc démontrée. □

Proposition 5 *Preuve d'arrêt de l'algorithme.*

Preuve :

Associons à chaque système $\Sigma = (A = 0,\ S \neq 0)$ la somme des degrés des éléments de A en leur variable principale, du nombre de polynômes non unitaires de A et du cardinal de S. Appelons $v(\Sigma)$ cet entier strictement positif.

Quand un système Σ est réécrit en une famille de systèmes $\mathcal{F}$, on a $v(\Sigma) < v(\Sigma')$ pour $\Sigma' \in \mathcal{F}$. D'après [29, Satz 6.6] (tout arbre infini localement fini contient une branche

de longueur infinie), l'algorithme s'arrête car toute branche est finie d'après la propriété $v(\Sigma) > 0$. □

Proposition 6 *La sortie* $\{T_1, \ldots, T_t\}$ *de l'algorithme vérifie* ***P1****,* ..., ***P5****.*

Preuve :
C'est la conséquence immédiate des quatre invariants **I1**, ..., **I4**. □

4.5 Optimisations et variantes

L'algorithme satTriangular est basé sur la fonction inverse. Si l'on désire coder satTriangular, il faut bien entendu tenir compte des conseils d'implantation de inverse donnés en section 1.6 du chapitre 1.

La règle R2.3 peut être spécialisée quand $j = k$. Dans ce cas, le système $A_g = 0, S \neq 0$ est inconsistant. La même optimisation s'applique pour la règle R1.3 quand $j = k - 1$.

Il est intéressant d'inverser les séparants des équations dès que possible. En effet, dès que les séparants de toutes les équations de A sont inversés, l'idéal (A) est radical (d'après le lemme de Lazard). Cela donne une autre optimisation de la règle R2.3 quand $j = k$. Dans ce cas, s est nécessairement inversible modulo (A_h) et peut donc être retiré de S.

Une bonne stratégie consiste à appliquer **R2** dans le cas où **R1** et **R2** s'appliquent tous les deux. En effet, l'inversion d'une inéquation pourrait scinder un système en d'autres systèmes, qui sont plus faciles à manipuler. C'est cette stratégie qui a été choisie dans les implantations de regCaractéristique (en `Maple Vr5` et en `C`).

Variante de regCaractéristique L'algorithme regCaractéristique calcule des présentations caractéristiques qui sont (en outre) des chaînes différentielles régulières autoréduites fortement normalisées. On peut assouplir les spécifications de regCaractéristique de manière à calculer non pas des présentations caractéristiques mais des chaînes différentielles régulières.

Dans ce cas, on n'est plus obligé de normaliser les polynômes de $\overline{A}$ (en calculant les inverses des initiaux de $\overline{A}$) : il suffit de tester que les initiaux sont inversibles (voir section 1.5 du chapitre 1). Ainsi, on évite le calcul d'inverse des initiaux des éléments de A.

4.5.1 Expérimentations

D'autres algorithmes ayant la même spécification que regCaractéristique sont implantés en Maple (voir [8] and [23]). Ces deux algorithmes sont toutefois moins efficaces que regCaractéristique : la première étape de ces deux algorithmes consiste à calculer une base de Gröbner de l'idéal $S^{-1}(A)$. Ce n'est pas a priori la meilleure solution car l'algorithme de Buchberger ne tient pas compte du caractère triangulaire de l'entrée et calcule les inverses de toutes les inéquations, qui (excepté les inverses des initiaux) ne sont pas utiles.

Notre méthode est surtout avantageuse lorsque Rosenfeld–Gröbner passe une majeure partie de son temps dans la phase algébrique du traitement des idéaux différentiels réguliers.

Le système suivant nécessite un traitement algébrique important :

$$v\,u_{xx} + u_{xx}^2 + u_x, \quad u_{yy} + u_y$$

pour le classement de l'ordre total

$$\cdots > u_{xx} > u_{xy} > u_{yy} > v_{xx} > v_{xy} > v_{yy} > u_x > u_y > v_x > v_y > u > v.$$

Nous avons utilisé, pour les calculs, le logiciel Maple Vr5 sur une station Sun Ultra 5 à 333Mhz et 128Mo de mémoire.

Notre version "privée" de Rosenfeld–Gröbner produit six sorties en 75 secondes, dont 62 sont utilisées par la phase algébrique.

Les autres implantations de Rosenfeld–Gröbner (celle en Maple Vr5 et sa variante par Hubert) ne résolvent pas cet exemple : l'algorithme s'arrête par un dépassement de mémoire.

Chapitre 5

L'algorithme Pardi

Sommaire

Ce chapitre est essentiellement la traduction de l'article [9]. Nous proposons un algorithme qui résout le problème suivant : étant donné une chaîne différentielle régulière C pour un classement $\mathcal{R}$, telle que l'idéal $\mathfrak{a} = [C] : {H_C}^\infty$ soit premier, et un classement $\overline{\mathcal{R}}$, déterminer une chaîne différentielle régulière $\overline{C}$ pour le classement $\overline{\mathcal{R}}$ vérifiant $[C] : {H_C}^\infty = [\overline{C}] : {H_{\overline{C}}}^\infty$.

L'algorithme que nous présentons, appelé Pardi (Prime pARtial Differential Ideal), s'applique à des systèmes polynomiaux aux dérivées partielles. Il se spécialise pour les systèmes polynomiaux différentiels ordinaires pour donner l'algorithme Podi (Prime Ordinary Differential Ideal). Il se spécialise également pour les systèmes algébriques pour donner Palgie (Prime ALGebraic IdEal[25]).

À notre connaissance, Ollivier a été le premier à résoudre le problème. Nous pouvons citer [44, page 95]: "one can [design] a method for constructing a characteristic set of a finitely generated prime differential ideal as soon as one can effectively test membership to this ideal". Un algorithme est donné en SCRATCHPAD dans [44, page 97].

Un tel problème est également traité dans [6]. Toutefois, les algorithmes présentés dans [6] calculent des polynômes différentiels qui ne font pas nécessairement partie de la chaîne différentielle régulière désirée $\overline{C}$ mais qui aident à calculer $\overline{C}$. Ces algorithmes sont complémentaires à Pardi.

La restriction aux idéaux premiers est réaliste. En effet, la plupart des systèmes différentiels provenant de problèmes réels engendrent des idéaux premiers. De même, les systèmes algébriques en dimension positive génèrent souvent des idéaux premiers. Si toutefois le système considéré n'engendre pas un idéal premier, on peut essayer d'appliquer un algorithme de décomposition en idéaux premiers.

Supposer que l'on dispose d'une chaîne différentielle régulière est également une hypothèse réaliste. En effet, dans le cas différentiel, il arrive souvent (par exemple pour les systèmes dynamiques en automatique non linéaire) que les équations du système initial constituent déjà une chaîne différentielle régulière pour un classement judicieusement choisi.

Pour conclure sur le caractère réaliste des hypothèses, on peut rappeler qu'on peut décider de la primalité de l'idéal $[C]{:}{H_C}^\infty$ (resp. $(C){:}{I_C}^\infty$) si C est une chaîne différentielle régulière (resp. une chaîne régulière).

L'algorithme que nous proposons se généralise aux idéaux non premiers. Toutefois, pour les raisons précédentes et la lisibilité de ce chapitre, nous préférons nous restreindre aux idéaux premiers.

Notre algorithme peut aussi s'adapter facilement pour résoudre le problème un peu plus complexe (en reprenant les notations précédentes) : déterminer une chaîne différentielle régulière $\overline{C}$ pour le classement $\overline{\mathcal{R}}$ telle que $[\overline{C}] : {H_{\overline{C}}}^\infty = \phi([C] : {H_C}^\infty)$, où ϕ est un changement linéaire inversible sur les variables dépendantes et indépendantes. Un tel changement de variables induit un isomorphisme entre deux anneaux différentiels $\phi : R \to \overline{R}$, et une bijection entre les idéaux différentiels de R et ceux de $\overline{R}$.

L'intérêt de cette variante est que la simple image $\phi(C)$ (où C est une chaîne différentielle régulière) n'est en général pas une chaîne différentielle régulière (pour un quelconque

25. ou aussi Polynomiale Algie diront les inconditionnels des systèmes linéaires, pris de douleur à la vue d'un exposant !

classement). L'idée est d'appliquer Pardi sur l'ensemble $\phi(C)$ et de tester l'appartenance d'un élément p à $\phi([C] : {H_C}^\infty)$ en testant l'appartenance de $\phi^{-1}(p)$ à $[C] : {H_C}^\infty$.

Notre approche offre plusieurs avantages. Elle identifie les sous–problèmes algébriques rencontrés dans les calculs différentiels et les résout par une méthode purement algébrique. Cela améliore le contrôle de la taille des coefficients et évite de nombreux calculs provenant de considérations différentielles. Cet avantage très important, par rapport à d'autres méthodes, nous a permis de traiter des problèmes jusqu'ici non résolus, et ce en n'utilisant qu'une implantation préliminaire.

Les trois variantes ont été implantées : Pardi en `Maple` (moi-même), Podi en `C` (F. Boulier) et Palgie en `Maple` (moi-même), `C` (F. Boulier) et `Aldor` (M. Moreno Maza). L'application au changement de variable a été implantée en Maple.

Une dernière contribution de ce chapitre est la simplicité conceptuelle de notre algorithme, qui contraste avec le caractère beaucoup plus technique de son implantation. Chacun sait que les racines communes de deux polynômes univariés sur un corps sont données par leur pgcd. Notre algorithme utilise cette propriété en remplaçant (lorsque le cas se présente) deux polynômes de même dérivée dominante par leur pgcd au dessus du corps de fraction d'un certain anneau quotient. Cette idée a nettement plus de sens que de considérer des restes complets comme dans d'autres approches.

Des méthodes de décomposition d'idéaux quelconques (premiers ou non) en ensembles triangulaires sont aussi formulées en termes de pgcd [26, 31, 40]. L'utilisation de ces pgcd est toutefois plus compliquée que dans Pardi. En effet, dans ces méthodes, l'idéal modulo lequel sont calculés les pgcd évolue durant le calcul car il dépend des équations déjà calculées. Ce n'est pas le cas dans notre contexte. Ainsi, nous espérons, par la simplicité de notre approche, aider à populariser ces méthodes.

Les fonctions présentées dans ce chapitre sont écrites en pseudo–code. Elles ont la particularité de modifier leurs arguments. Comme en `ADA`, les paramètres des fonctions sont précédés des mots–clés in, out and in out, suivant qu'ils sont en lecture seule, en écriture seule ou en lecture-écriture.

Dans les différentes fonctions, on écrira souvent le test $p \in \mathfrak{a}$ où p est un polynôme différentiel et $\mathfrak{a}$ est l'idéal $[C] : {H_C}^\infty$. Ce test peut être réalisé de différentes manières. La première qui vient à l'esprit est d'utiliser la chaîne différentielle régulière C en évaluant le test reste_complet$(p,C) = 0$. D'autres méthodes, plus efficaces, sont présentées en section 5.8.

5.1 L'ancien algorithme

L'algorithme Rosenfeld–Gröbner, implanté dans le paquetage `diffalg` de `Maple Vr5`, résout le problème posé dans ce chapitre. Voir [8] pour les preuves et [17] pour le pseudo-code de Rosenfeld–Gröbner.

Dans le cas général, Rosenfeld–Gröbner scinde les solutions du système courant en deux ensembles de solutions : celles qui annulent un certain polynôme différentiel p et celles qui n'annulent pas p. Le polynôme p est en général l'initial ou le séparant d'un polynôme utilisé lors de la réduction de Ritt. Quand la chaîne différentielle régulière C est connue et que l'idéal $\mathfrak{a} = [C] : {H_C}^\infty$ est premier, une seule branche a besoin d'être considérée : la

première si $p \in \mathfrak{a}$ et la seconde si $p \notin \mathfrak{a}$.

La fonction spé_Rosenfeld–Gröbner est le pseudo-code spécialisé de Rosenfeld–Gröbner. Elle manipule des quadruplets $\langle A,D,P,S\rangle$ où :

- A est l'ensemble des polynômes différentiels déjà traités ;
- D est l'ensemble des paires critiques à traiter ;
- P est l'ensemble des polynômes différentiels à traiter ;
- S est l'ensemble des inéquations.

Pour présenter les invariants de boucle, on a besoin de la définition de paire critique *presque résolue* par un quadruplet $\langle A,D,P,S\rangle$.

Afin de présenter la version simplifiée de Rosenfeld–Gröbner, deux axiomes sont nécessaires pour définir une paire critique presque résolue. Il faudrait trois axiomes pour en présenter une version avec critères d'élimination de paires critiques (équivalents des critères de Buchberger).

Une paire critique est presque résolue par $\langle A,D,P,S\rangle$ si l'une des deux conditions est remplie :

1. elle est résolue par $A \cup \Delta(D) = 0$, $S \neq 0$;
2. elle appartient à l'ensemble D.

Voici les invariants de la boucle principale :

1. $\mathfrak{a} = [A \cup \Delta(D) \cup P] : S^\infty$;
2. l'ensemble des rangs de A est autoréduit ;
3. les paires critiques paires_critiques(A) sont presque résolues par $\langle A,D,P,S\rangle$ (utile uniquement pour les EDP) ;
4. $H_A \subset S$.

fonction spé_Rosenfeld–Gröbner(in $C,\mathcal{R},\overline{\mathcal{R}}$)
début
  $\langle A,D,P,S\rangle := \langle\emptyset,\emptyset,C,H_C\rangle$
      (H_C est relatif au classement $\mathcal{R}$)
      (à partir de maintenant, $\overline{\mathcal{R}}$ est implicitement utilisé)
  tant que $D \neq \emptyset$ ou $P \neq \emptyset$ faire
    prendre et retirer une équation $p \in P$ ou une paire critique $\{p_1,p_2\} \in D$.
        Dans le deuxième cas, prendre $p = \Delta(p_1,p_2)$
    $p :=$ reste_complet(p,A)
    $p :=$ ancienAssureRang(p,C,P,S)
    si $p \neq 0$ alors
      $\langle A,D,P,S\rangle :=$ complète($\langle A,D,P,S\rangle,p$)
    fin si
  fait
  retourner spé_regCaractéristique(A,S)
fin

À la fin de la boucle principale, $\langle A,D,P,S\rangle = \langle A,\emptyset,\emptyset,S\rangle$ est tel que A est cohérent (car D est vide et d'après le troisième invariant). La fonction spé_regCaractéristique calcule la chaîne différentielle régulière $\overline{C}$ désirée.

Remarquez que la fonction spé_regCaractéristique est une version spécialisée de l'algorithme regCaractéristique. Toutefois, dans les différentes versions du paquetage `diffalg`, la fonction spé_regCaractéristique n'est pas codée et c'est le calcul de base de Gröbner (décrit dans la sous–section 2.9.2) qui est utilisée.

La fonction suivante simplifie p tant que son initial ou son séparant est dans $\mathfrak{a}$.

fonction ancienAssureRang(in p,C, in out P,S)
début
  tant que $p \notin K$ et ($i_p \in \mathfrak{a}$ ou $s_p \in \mathfrak{a}$) faire
    si $i_p \in \mathfrak{a}$ alors
      $P := P \cup \{i_p\}$
      $p :=$ queue(p)
    sinon
      $P := P \cup \{s_p\}$
      $S := S \cup \{i_p\}$
      $p := d\,p - v\,s_p$ où $v^d = \operatorname{rang} p$
    fin si
  fait
  retourner p
fin

La fonction complète qui suit est simple. Elle insère une nouvelle équation p dans A et retire de A les équations dont la dérivée dominante est une dérivée de celle de p (ainsi l'invariant 2 est maintenu). Elle ajoute dans D les paires critiques entre p et les équations de A. Elle insère dans S l'initial et le séparant de p. Remarquez que les équations retirées de A se retrouvent dans des paires de réduction. Ainsi, l'invariant 1 est conservé car :

$$[A \cup \{p\} \cup \Delta(D) \cup P] : S^\infty = [A' \cup \Delta(D') \cup P'] : S'^\infty.$$

fonction complète(in$\langle A, D, P, S\rangle$, p)
début
  $A' := \{p\} \cup \{q \in A \mid \operatorname{ld} q$ n'est pas une dérivée de $\operatorname{ld} p\}$
  $D' := D \cup \{\{q, p\} \mid q \in A$ et $\{q, p\}$ est une paire critique$\}$
  $P' := P$
  $S' := S \cup \{i_p, s_p\}$
  retourner $\langle A', D', P', S'\rangle$
fin

5.2 Les sous–problèmes algébriques

On dit que la fonction spé_Rosenfeld–Gröbner rencontre un *sous–problème algébrique* lorsque le polynôme différentiel p (appelons le $p_2 = p$ pour des raisons de commodité) passé à la fonction complète a la même dérivée dominante qu'un polynôme p_1 de A.

Voyons comment complète se comporte dans cette situation. Posons $\operatorname{rang} p_1 = v^{d_1}$ et $\operatorname{rang} p_2 = v^{d_2}$. Puisque $p_1 \in A$ et que p_2 est réduit par rapport à A, on a $d_2 < d_1$. Le

polynôme p_2 est rangé dans A, le polynôme p_1 est retiré de A et la paire $\{p_1,p_2\}$ est stockée dans D. Après quelques tours de boucle, spé_Rosenfeld–Gröbner extrait la paire $\{p_1,p_2\}$ de D et calcule $\Delta(p_1,p_2)$. Comme p_1 et p_2 ont même dérivée dominante v,

$$\Delta(p_1,p_2) = \mathsf{prem}(p_1,p_2,v).$$

Appelons p_3 ce pseudo–reste et posons $\operatorname{rang} p_3 = v^{d_3}$. On a $d_3 < d_2$. En raisonnant comme ci–dessus, on voit que p_3 est stocké dans A, que p_2 est retiré de A et que la paire $\{p_2,p_3\}$ est stockée dans D. En résumant : la fonction spé_Rosenfeld–Gröbner commence à calculer une suite de pseudo–restes très naïve (et mauvaise) quand elle rencontre un sous–problème algébrique.

$$\begin{aligned} p_1 &\in A, \\ p_2 &= p_2, \\ p_3 &= \mathsf{prem}(p_1,p_2,v), \\ p_4 &= \mathsf{prem}(p_2,p_3,v), \\ &\vdots \end{aligned}$$

De plus, à chaque étape i :

- de nombreuses paires critiques entre le reste courant p_i et les éléments de A sont générées (et pas seulement la paire de réduction avec p_{i-1}) ;
- le séparant de p_i (et pas seulement l'initial) est stocké dans S.

Les deux points précédents relèvent de considérations différentielles. Nous allons voir qu'ils sont en fait inutiles dans le cas algébrique.

Le raisonnement tenu dans cette sous–section est également valable lorsque que l'on introduit les critères d'élimination de paires critiques (équivalents des critères de Buchberger).

5.3 Les idées–clés de Pardi

L'algorithme Pardi repère les sous–problèmes algébriques qui se produisent lors du traitement différentiel. Il optimise le calcul de la suite de pseudo–restes et évite les calculs inutiles relevant de considérations différentielles (comme expliqué précédemment).

Reprenons le cas où l'on traite un polynôme p_2 qui a la même dérivée dominante v qu'un polynôme p_1 de A. Pardi repose sur les deux idées–clés suivantes :

Première idée : Remplacer p_1 et p_2 par leur "*pgcd*" g dans $(R^-/\mathfrak{a}^-)[v]$ où $R^- = K[w \in \Theta U \mid w < v]$ et $\mathfrak{a}^- = \mathfrak{a} \cap R^-$.

En fait, g est le "*lsr*" c'est–à–dire le *dernier sous–résultant* non nul de p_1 et p_2 dans $(R^-/\mathfrak{a}^-)[v]$.

C'est aussi un des pgcd de p_1 et p_2 dans $G[v]$ où G est le corps de fractions de $R^-/\mathfrak{a}^-$ (légitime car $\mathfrak{a}^-$ étant premier, $R^-/\mathfrak{a}^-$ est intègre).

Pour des raisons de commodité, nous parlerons *du* pgcd de p_1 et de p_2 dans $(R^-/\mathfrak{a}^-)[v]$ même si cela est légèrement incorrect.

Remarque importante : le polynôme g aura toujours un degré positif en v (propriété (iii) de lsr1, fonction décrite plus loin).

Deuxième idée : Il s'agit d'une relation maître à élève. La chaîne différentielle régulière C est le maître car elle sait tester l'appartenance à $\mathfrak{a}$. L'ensemble en construction A est l'élève. Dès qu'une quantité est réduite à 0 par C mais pas par A, on l'insère dans l'ensemble des polynômes à traiter P. L'ensemble P et l'ensemble D des paires critiques constituent ce que l'élève A doit encore apprendre.

Intuitivement, quand P et D sont vides, A sait calculer aussi bien que son maître et A est donc une chaîne différentielle régulière.

5.4 Calcul du pgcd (mais c'est le lsr pardi!)

Les idées–clés pour calculer le pgcd sont les suivantes :

1. Partir d'un (bon) algorithme de calcul de suite de pseudo–restes (utilisant la méthode des sous–résultants par exemple). Nous avons choisi l'algorithme de Lionel Ducos [20] mais l'algorithme de [35] conviendrait tout aussi bien.
2. Vérifier à chaque étape i si le coefficient principal du pseudo–reste p_i est nul modulo $R^-/\mathfrak{a}^-$ (en utilisant une réduction par C par exemple).

   - s'il n'est pas nul, on poursuit l'algorithme de [20] normalement. On *ne* modifie *pas* le pseudo–reste (en essayant de le normaliser par exemple). Voir le commentaire sur le deuxième point ci–après ;
   - s'il est nul, on réamorce une nouvelle suite de pseudo–restes (ce qui revient à lancer un nouveau calcul de pgcd) entre le reste précédent p_{i-1} et $\mathsf{queue}(p_i)$. Remarque : en pratique, on prendra la queue de p_i autant de fois que nécessaire pour obtenir un polynôme à coefficient principal non réduit à 0 par C. C'est le rôle de la fonction assure_coeff1.

3. À chaque étape, ne pas insérer le séparant de p_i dans S mais uniquement le coefficient principal. Ne générer aucune paire critique (gain important si le nombre de boucles est important).

Les premier et troisième points montrent l'avantage de Pardi par rapport à l'algorithme spé_Rosenfeld–Gröbner :

- la croissance des coefficients est contrôlée de manière efficace grâce à [20] ;
- les traitements différentiels sont complètement évités lors des sous–problèmes algébriques.

Revenons au deuxième point. L'idée est simple mais très importante, et Marc Moreno Maza la met en pratique dans [40]. Elle permet, en effet, d'appliquer l'algorithme [20] (et d'autres algorithmes similaires) dans l'anneau quotient $(R^-/\mathfrak{a}^-)[v]$.

Pour mettre en œuvre cet algorithme, on a besoin de l'addition, de la multiplication et de la division exacte dans $R^-/\mathfrak{a}^-$. L'opération difficile est, a priori, la division exacte dans $R^-/\mathfrak{a}^-$. En ne modifiant pas les pseudo–restes (c'est–à–dire sans les normaliser ni les

réduire par C), on peut effectuer les divisions comme si on calculait la suite des pseudo–restes dans $R^-[v]$, ce qui est facile (simple division de polynômes multivariés à coefficients dans $\mathbb{Z}$).

La seule précaution à prendre est de s'assurer que le coefficient principal de chaque pseudo–reste p_i est non nul. Si c'est le cas, les coefficients principaux par lesquels on divise sont non nuls (modulo $\mathfrak{a}$).

En théorie, on pourrait continuer l'algorithme de [20] dans le cas où l'on a remplacé un pseudo–reste p_i par $\mathsf{queue}(p_i)$. Toutefois, les représentants ne seraient plus commodes à utiliser et les divisions exactes dans $R^-/\mathfrak{a}^-$ seraient beaucoup plus complexes (nécessité d'inverser des quantités modulo une chaîne régulière).

Une autre solution, beaucoup plus simple[26], consiste à réamorcer une suite de pseudo–restes entre p_{i-1} et $\mathsf{queue}(p_i)$. C'est ce que nous faisons dans Pardi.

Observons au passage qu'un algorithme de [41] effectue des divisions exactes dans $R^-/\mathfrak{a}^-$ en normalisant (au sens de [31]) les polynômes de la suite des pseudo–restes. Toutefois, l'adaptation de cette stratégie ne semble pas efficace en pratique selon [3].

Voyons maintenant l'implantation. Le code est une légère modification de [19] et [40]. Les fonctions Lazard2 et nsr sont disponibles dans le paquetage en `Axiom` [19, fonctions Lazard2 et next_sousResultant2].

Voici les spécifications de la fonction lsr1(in p,q,v,C,A, in out P,S). Les paramètres p et q vérifient les propriétés suivantes : ils ont la même dérivée dominante v et appartiennent à $\mathfrak{a}$. Leurs coefficients principaux et leurs séparants ne sont pas dans $\mathfrak{a}$. Les paramètres A, P et S proviennent d'un quadruplet semblable à ceux utilisés dans spé_Rosenfeld–Gröbner. En particulier, les coefficients principaux de A appartiennent à S. De plus, on suppose p et q partiellement réduits par rapport à A.

Le dernier sous–résultant non nul g renvoyé par la fonction lsr1 vérifie les propriétés suivantes :

(i) le coefficient principal de g (vu comme polynôme univarié en v) n'appartient pas à $\mathfrak{a}$.

Tous les sous–résultants calculés appartiennent à l'idéal (p,q) de l'anneau $(R^-/\mathfrak{a}^-)[v]$. En d'autres termes, ils appartiennent à l'idéal $(p,q)+\mathfrak{a}^-$ de l'anneau $R^-[v]$ et, comme $p,q \in \mathfrak{a}$, on a:

(ii) $g \in \mathfrak{a}$;
(iii) $\mathrm{ld}\, g = v$.

Le point (iii) vient du fait que g ne peut être le résultant de p et q. En effet, le résultant de p et q appartient à $\mathfrak{a}$ (c'est un des sous–résultants) et il appartient aussi à R^-. Ainsi, le résultant est nul dans $(R^-/\mathfrak{a}^-)[v]$.

D'après (iii), g est de degré au moins 1 en v. Il s'ensuit, d'après (i), que l'initial de g n'appartient pas à $\mathfrak{a}$. De plus, comme les séparants de p et q n'appartiennent pas à $\mathfrak{a}$, et que g est un pgcd de p et q dans $G[v]$ (où G est le corps des fractions de $R^-/\mathfrak{a}^-$), le séparant de g n'appartient pas non plus à $\mathfrak{a}$. On a donc :

(iv) l'initial et le séparant de g n'appartiennent pas à $\mathfrak{a}$.

26. selon Lionel Ducos lui même, que nous remercions pour ses commentaires.

La fonction lsr1 ajoute dans P tous les coefficients nuls dans $R^-/\mathfrak{a}^-$ qui ne sont pas réduits par A. Elle ajoute dans S les initiaux $i_1, \ldots, i_n = i_g$ des sous–résultants calculés (après s'être assuré qu'ils n'étaient pas dans $\mathfrak{a}$).

Appelons j l'idéal $((A \cup P) \cap R^-) : (S \cap R^-)^\infty$ où les ensembles A, P et S sont ceux obtenus à la fin de lsr1. On a :

(v) $(p,q) \subset (g) : (i_1 \cdots i_n)^\infty$ in $(R^-/\mathfrak{j})[v]$.

Pour prouver cela, on s'inspire de la propriété classique $(p,q) \subset (g) : (i_1 \cdots i_n)^\infty$ dans $(R^-/\mathfrak{a}^-)[v]$.

Le point (v) est vérifié si l'on prouve que tous les coefficients principaux par lesquels on a simplifié les pseudo–restes (c'est–à–dire, ceux appartenant à $\mathfrak{a}^-$) appartiennent à j.

L'un quelconque de ces coefficients principaux est soit enregistré dans P (par la fonction assure_coeff1), soit réduit à 0 par A. Dans le premier cas, il appartient à l'idéal $(P \cap R^-)$. Dans le deuxième cas, il est dans $(A \cap R^-) : (S \cap R^-)^\infty$ car il appartient à R^- et car S contient les initiaux de A. Ainsi, tous les coefficients principaux qui ont servi lors des simplifications appartiennent à j, ce qui prouve le point (v).

```
fonction lsr1(in p,q,v,C,A, in out P,S)
début
  si deg(p,v) < deg(q,v) alors échanger p et q fin si
  trouvé := faux
  tant que non trouvé faire
    δ := deg(p,v) − deg(q,v)
    s := i_q^δ
    S := S ∪ {−i_q}
    (p,q) := (q, prem(p, − q,v))
    z := p
    chute_rang := faux
    tant que non trouvé et non chute_rang faire
      q := assure_coeff1(q,C,A,v,P,chute_rang)
      si q = 0 alors
        trouvé := vrai
      sinon si non chute_rang alors
        S := S ∪ {coeff_principal(q,v)}
        δ := deg(p,v) − deg(q,v)
        z := Lazard2(q, coeff_principal(q,v),s,δ)
             (calcule q (i_q/s)^(δ−1))
        si deg(z,v) = 0 alors
          trouvé := vrai
        sinon
          (p,q) := (q,nsr(p,q,z,s))        (calcule le sous–résultant suivant)
          s := i_z
        fin si
      fin si
    fait
  fait
```

```
  retourner z
fin
```

La fonction qui suit peut être légèrement optimisée (un test d'appartenance peut être évité) car $\deg(p,v) = 0$ implique $p \in \mathfrak{a}$.

```
fonction assure_coeff1(in p,C,A,v, in out P, out chute_rang)
début
  chute_rang := faux
  tant que p ≠ 0 et coeff_principal(p,v) ∈ 𝔞 faire
    chute_rang := vrai
    si prem(coeff_principal(p,v),A) ≠ 0 alors
      P := P ∪ {coeff_principal(p,v)}
    fin si
    p := queue(p)
  fait
  retourner p
fin
```

5.5 La fonction Pardi

La fonction Pardi manipule des quadruplets $\langle A,D,P,S\rangle$ de la même manière que l'algorithme spé_Rosenfeld–Gröbner et maintient les mêmes invariants. Il y a toutefois une petite différence (qui simplifie les preuves) avec spé_Rosenfeld–Gröbner : les éléments de chaque paire critique ont des dérivées dominantes différentes (i.e. il n'y a pas de paires critiques "algébriques"). C'est une conséquence logique du traitement spécial des sous–problèmes algébriques.

Remarquer que l'on pourrait remplacer les restes partiels par des restes complets. Toutefois, ce n'est pas souhaitable car, dans le cas d'un sous–problème algébrique, une réduction complète réaliserait la première pseudo–division normalement effectuée par l'algorithme [20]. Ceci rendrait donc l'algorithme [20] moins efficace.

```
fonction Pardi(in C,ℛ,ℛ̄)
début
  ⟨A,D,P,S⟩ := ⟨∅,∅,C,H_C⟩
       (H_C est relatif au classement ℛ)
       (à partir de maintenant, ℛ̄ est implicitement utilisé)
  tant que D ≠ ∅ ou P ≠ ∅ faire
    prendre et retirer une équation p ∈ P ou une paire critique {p1,p2} ∈ D.
         Dans le deuxième cas, prendre p = Δ(p1,p2)
    p := reste_partiel(p,A)
    p := AssureRang(p,C,A,P)
    si p ≠ 0 alors
      si ∃q ∈ A tel que ld p = ld q alors
        g := lsr1(p,q, ld p,C,A,P,S)
```

```
        si rang g ≠ rang q alors
          ⟨A,D,P,S⟩ := complète(⟨A \ {q},D,P,S⟩,g)
                (on remplace p et q par leur "pgcd")
        fin si
      sinon
        ⟨A,D,P,S⟩ := complète(⟨A,D,P,S⟩,p)
      fin si
    fin si
  fait
  retourner spé_regCaractéristique(A,S)
fin
```

La fonction suivante simplifie le polynôme différentiel p tant que son initial ou son séparant appartient à $\mathfrak{a}$. Les initiaux et séparants ainsi détectés sont stockés dans P.

```
fonction AssureRang(in p,C,A, in out P)
début
  tant que p ∉ K et (i_p ∈ 𝔞 ou s_p ∈ 𝔞) faire
    si i_p ∈ 𝔞 alors
      si prem(i_p,A) ≠ 0 alors P := P ∪ {i_p} fin si
      p := queue(p)
    sinon
      si prem(s_p,A) ≠ 0 alors P := P ∪ {s_p} fin si
      p := d p − v s_p où v^d = rang p
    fin si
  fait
  retourner p
fin
```

5.6 Exemples

5.6.1 Exemple détaillé

Le système C suivant est une chaîne différentielle régulière pour le classement de l'ordre total $\mathcal{R}$:

$$\cdots > u_{xx} > u_{xy} > u_{yy} > v_x > v_y > u_x > u_y > v > u.$$

dans l'anneau $\mathbb{Q}\{u,v\}$ muni des dérivations par rapport à x et y. De plus, l'idéal $[C]:{H_C}^\infty$ est premier. Les rangs apparaissent en partie gauche. Les dénominateurs de la partie droite sont les initiaux.

$$C \begin{cases} v_{xx} = u_x, \\ v_y = (u_x\, u_y + u_x\, u_y\, u)/(4\, u), \\ u_x^2 = 4\, u, \\ u_y^2 = 2\, u. \end{cases}$$

Nous cherchons une chaîne différentielle régulière $\overline{C}$ pour le classement d'élimination $\overline{\mathcal{R}}$

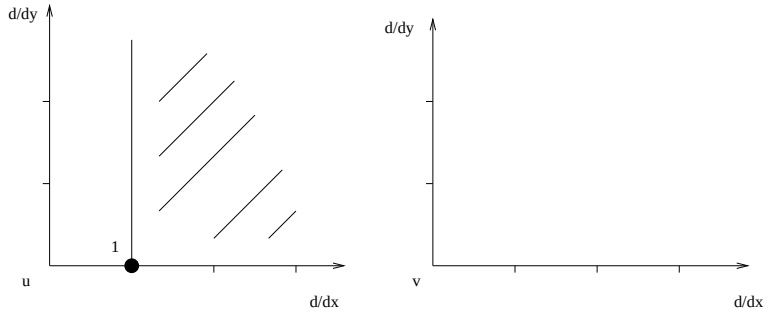
$$\cdots > u_x > u_y > u > \cdots > v_{xx} > v_{xy} > v_{yy} > v_x > v_y > v.$$

telle que $[C] : {H_C}^{\infty} = [\overline{C}] : {H_{\overline{C}}}^{\infty}$.

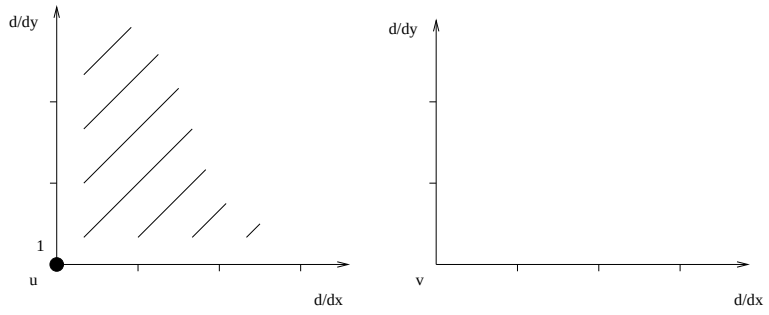
Dans l'analyse qui suit, nous ne fournissons que les rangs des polynômes différentiels. Sur les diagrammes, les cercles noirs représentent les dérivées dominantes des éléments de A et les entiers désignent les degrés des éléments de A en leur dérivée dominante.

Initialement, on a $A = D = \emptyset$ et $S = \{4\,u, 2\,u_x, 2\,u_y\}$ contient H_C (pour le classement $\mathcal{R}$). On a $P = C$. L'ensemble des rangs de P (pour $\overline{\mathcal{R}}$ et nous n'utiliserons plus que $\overline{\mathcal{R}}$) est $\operatorname{rang} P = \{u_x, u_x, u_x^2, u_y^2\}$. L'implantation de Pardi, que j'ai écrite en `Maple VI`, choisit d'abord les nouvelles équations dans P et ne traite une paire critique de D que si P est vide. Nous adaptons ici la même stratégie. La version de l'algorithme utilisée dans cet exemple, diffère légérement de l'algorithme présenté précédemment car elle opère, dans la boucle principale, des réductions totales au lieu de réductions partielles. Nous avons choisi cette variante car elle rend la description de l'exemple plus courte.

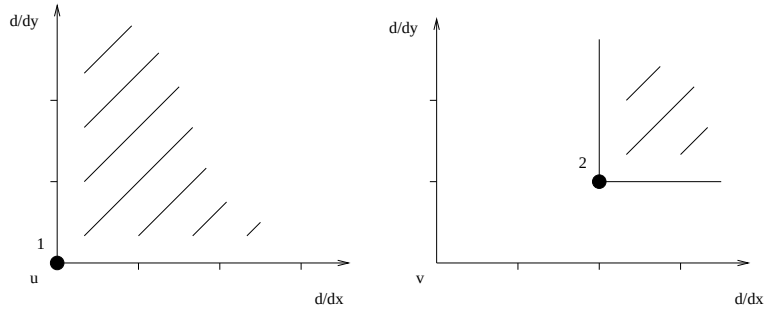
Premièrement, une équation de rang u_x est retirée de P et stockée dans A.



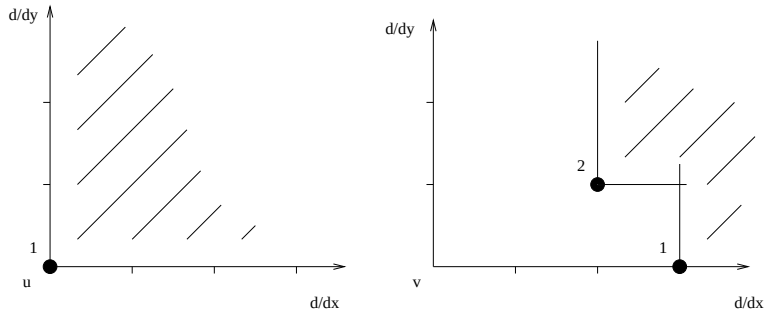
Maintenant, $\operatorname{rang} P = \{u_x, u_x^2, u_y^2\}$. Une nouvelle équation de rang u_x^2 est retirée de P. Après une réduction complète, son rang est u. Elle forme une paire critique avec l'équation précédente, qui est supprimée de A.



Maintenant, $\operatorname{rang} P = \{u_x, u_y^2\}$ et $\operatorname{rang} D = \{\{u, u_x\}\}$. Une nouvelle équation de rang u_y^2 est retirée de P. Après réduction complète, son rang est v_{xxy}^2.

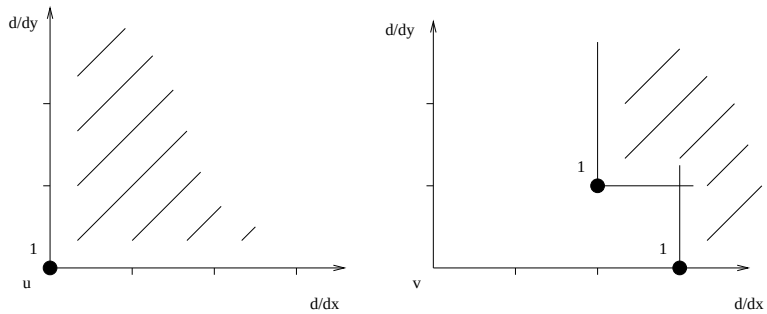


Maintenant, rang $P = \{u_x\}$ et rang $D = \{\{u, u_x\}\}$. Une nouvelle équation de rang u_x est retirée de P. Après réduction complète, son rang est v_{xxx}. Elle forme une paire critique avec l'équation précédente.



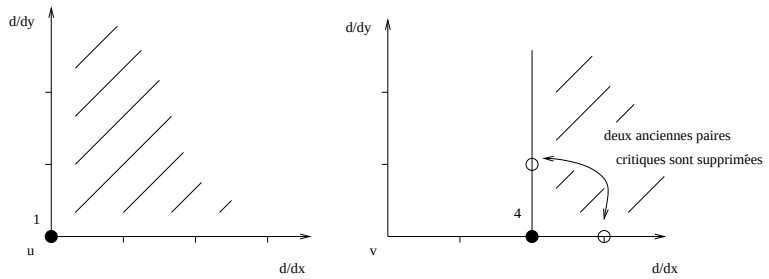
Maintenant, P est vide rang $D = \{\{u, u_x\}, \{v_{xxx}, v_{xxy}^2\}\}$. La première paire critique est retirée de D. Après réduction complète, le Δ-polynôme a pour rang v_{xxy}. Nous sommes en présence d'un sous–problème algébrique. Cette situation est très simple car l'un des polynômes a pour degré 1 et l'autre est de degré 2. Pour cette raison, l'algorithme des sous–résultants n'apporte pas d'amélioration car il n'effectue, comme le ferait Rosenfeld–Gröbner, qu'une seule pseudo-division. Le pgcd (c'est–à–dire le dernier sous–résultant non nul) de ces polynômes est donc le polynôme de degré 1.

Il remplace dans A le polynôme de degré 2 et génère une paire critique avec le polynôme de rang v_{xxx}. À la fin du calcul de pgcd, le résultant des deux polynômes, qui a pour rang v_{xx}^4, est nul dans l'anneau quotient $(R^-/(\mathfrak{a} \cap R^-))[v_{xx}]$, mais n'est pas réduit à zéro par A (où $R^- = K[w \in \Theta U \mid w < v_{xx} \text{ pour } \overline{\mathcal{R}})$. Il est donc stocké dans P.

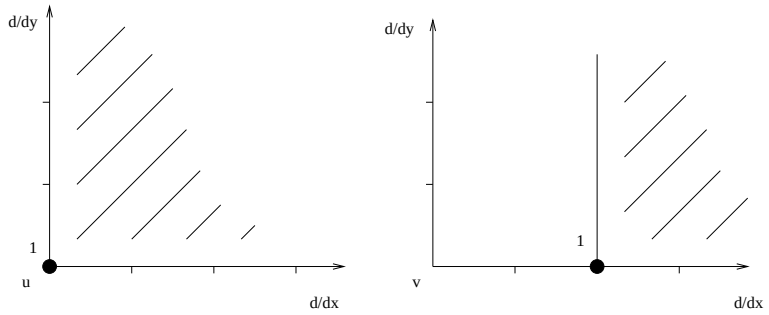


Maintenant rang $P = \{v_{xx}^4\}$ et rang $D = \{\{v_{xxx}, v_{xxy}^2\}, \{v_{xxx}, v_{xxy}\}\}$. Le résultant de rang v_{xx}^4 (calculé précédemment) est retiré de P. Deux nouvelles paires critiques sont générées entre ce polynôme et deux des polynômes de A. Ces deux polynômes sont supprimés de A.

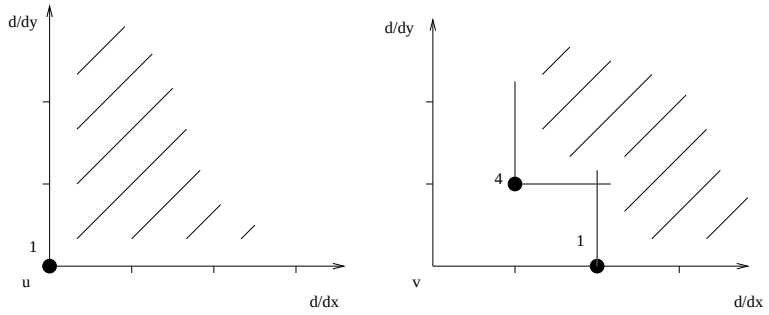
La version avancée de complète (utilisant les analogue des critères de Buchberger) permet d'éliminer les deux anciennes paires critiques de D.



Maintenant, P est vide et $\operatorname{rang} D = \{\{v_{xxx}, v_{xx}^4\}, \{v_{xxy}, v_{xx}^4\}\}$. La première paire critique est retirée de D. Après réduction totale, le Δ-polynôme a pour rang v_{xx}^3. Il s'agit encore d'un sous–problème algébrique. Le pgcd entre ce polynôme et l'élément de A ayant pour rang v_{xx}^4 est de degré 1 en v_{xx}. Le polynôme de rang v_{xx}^4 est remplacé par le pgcd. Durant le calcul du pgcd, aucune paire critique n'a été générée, ce qui constitue un avantage certain par rapport à spé_Rosenfeld–Gröbner. À la fin du calcul le résultant, qui a pour rang v_{xy}^4, n'est pas réduit à zéro. Il est donc stocké dans P. Aucune nouvelle paire critique n'est générée.

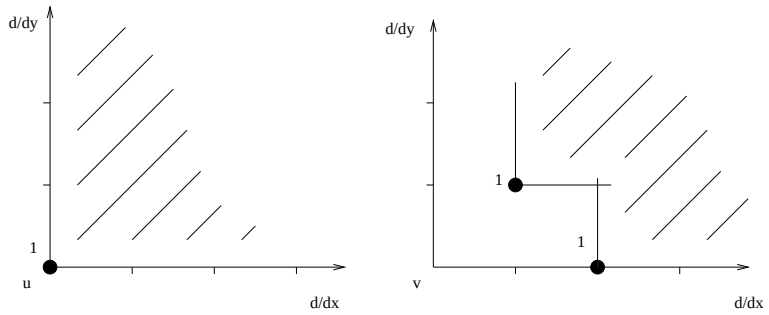


Maintenant, $\operatorname{rang} P = \{v_{xy}^4\}$ et $\operatorname{rang} D = \{\{v_{xxy}, v_{xx}^4\}\}$. Une nouvelle équation de rang v_{xy}^4 est retirée de P. Elle est placée dans A et aucune nouvelle paire critique n'est générée.

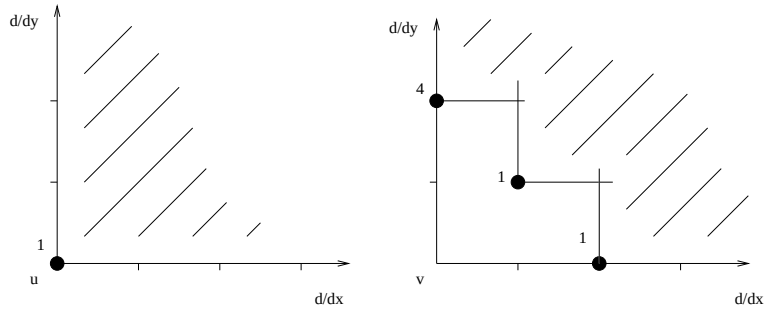


P est vide et $\operatorname{rang} D = \{\{v_{xx}, v_{xy}^4\}, \{v_{xxy}, v_{xx}^4\}\}$. La première paire critique est retirée de D. Après réduction complète par A, le Δ-polynôme a pour rang v_{xy}^2. Il s'agit encore d'un sous–problème algébrique. Le pgcd entre ce polynôme et l'élément de A de rang v_{xy}^4

a pour rang v_{xy}. Ce pgcd remplace dans A le polynôme de rang v^4_{xy}. Une nouvelle paire critique est générée. Le résultant, de rang v^4_{yy} est stocké dans P.



rang $P = \{v^4_{yy}\}$ et rang $D = \{\{v_{xx}, v_{xy}\}, \{v_{xxy}, v^4_{xx}\}\}$. Le résultant (précédent) est retiré de P et placé dans A. Les analogues des critères de Buchberger permettent de ne générer qu'une seule nouvelle paire critique (la paire $\{v^4_{yy}, v_{xx}\}$ est évitée).



P est vide, rang $D = \{\{v_{xy}, v^4_{yy}\}, \{v_{xx}, v_{xy}\}, \{v_{xxy}, v^4_{xx}\}\}$. Les trois Δ–polynômes sont réduits à zéro par A. Après avoir appliqué l'algorithme spé_regCaractéristique, on obtient :

$$\overline{C} \begin{cases} u = v^2_{yy}, \\ v_{xx} = 2\, v_{yy}, \\ v_{xy} = (v^3_{yy} - v_{yy})/v_y, \\ v^4_{yy} = 2\, v^2_{yy} + 2\, v^2_y - 1. \end{cases}$$

Notons que l'algorithme spé_Rosenfeld–Gröbner de `diffalg` (en `Maple Vr5`) ne traite pas l'exemple précédent (la version en `Maple VI` ne le traite pas non plus à cause d'un bogue).

Même si c'était le cas, l'analyse de l'exemple aurait été beaucoup plus difficile. En effet, nous avons présenté les calculs en termes de pgcd et de résultants. Cette méthode, à notre avis, a plus de sens que d'utiliser uniquement les réductions de Ritt, ce que fait l'algorithme spé_Rosenfeld–Gröbner.

5.6.2 Équations d'Euler pour un fluide parfait en 2D

Exprimées comme des polynômes différentiels, les équations d'Euler pour un fluide parfait en deux dimensions sont :

$$\Sigma \begin{cases} v^1_t + v^1 v^1_x + v^2 v^1_y + p_x = 0, \\ v^2_t + v^1 v^2_x + v^2 v^2_y + p_y = 0, \\ v^1_x + v^2_y = 0. \end{cases}$$

Il y a trois indéterminées différentielles v^1, v^2 (les deux composantes de la vitesse) et la pression p. Elles dépendent de trois variables : les deux variables d'espace x et y et le temps t.

Pour le classement lex(p,v^1,v^2) avec $t > x > y$, Rosenfeld–Gröbner fournit (quasiment sans calcul) la chaîne différentielle régulière C :

$$C \begin{cases} p_{xx} = -2\, v^2_x\, v^1_y - 2\,(v^2_y)^2 - p_{yy}, \\ v^1_t = -v^2\, v^1_y - p_x + v^2_y\, v^1, \\ v^1_x = -v^2_y, \\ v^2_t = -v^1\, v^2_x - v^2\, v^2_y - p_y. \end{cases}$$

Pour le classement (qui élimine p et v_1) $(p, v^1) \gg$ degrevlex(v^2) avec $t > x > y$, l'implantation de Pardi calcule la chaîne différentielle régulière $\overline{C}$. Cet ensemble est un peu trop imposant pour être écrit ici (le fichier fait environ 600 Ko). Il contient 7 équations comprenant plus de 50 dérivées différentes. Les calculs intermédiaires ont nécessité plus de 500 Mo de mémoire et une dizaine d'heures de calcul sur les ordinateurs de l'UMS MEDICIS (Laboratoire GAGE de l'École Polytechnique).

Pour information, le rang de $\overline{C}$ est :

$$\operatorname{rang} \overline{C} = \{p_x, p_y, v^1, v^2_{xxxxt}, v^2_{xxxtt}, v^2_{xxytt}, v^2_{xxxyyt}\}.$$

L'escalier de l'indéterminée v^2 peut se visualiser[27] sur la figure[28] 5.1.

Cet exemple n'avait, à notre connaissance, jamais été traité auparavant. Toutefois, il n'y a qu'un sous–problème algébrique qui se présente lors des calculs.

Il est intéressant de remarquer que, si les derniers Δ–polynômes ne sont pas traités (c'est–à–dire sont purement et simplement ignorés), alors le système obtenu (qui est incorrect) est gros de 1500 Ko (contre les 600 Ko du résultat correct). Cela est plutôt étonnant car les calculs des delta–polynômes ignorés (nécessitant dérivations et pseudo–restes) devraient, en toute logique, faire encore grossir le résultat intermédiaire.

Ce phénomène est proche du grossissement des données intermédiaires (bien connu pour le calcul du pgcd de deux polynômes) suivi d'une fonte de la taille des données. Cela laisse espérer que des techniques modulaires et p–adiques donneraient d'excellents résultats.

Observons que Pommaret avait calculé, à la main, l'équation d'ordre 6 dépendant uniquement de v^2 et de ses dérivées [47]. François Boulier avait pu déterminer une des

27. Merci à Marc Giusti pour ses conseils sur la visualisation d'escalier
28. figure générée automatiquement avec Maple

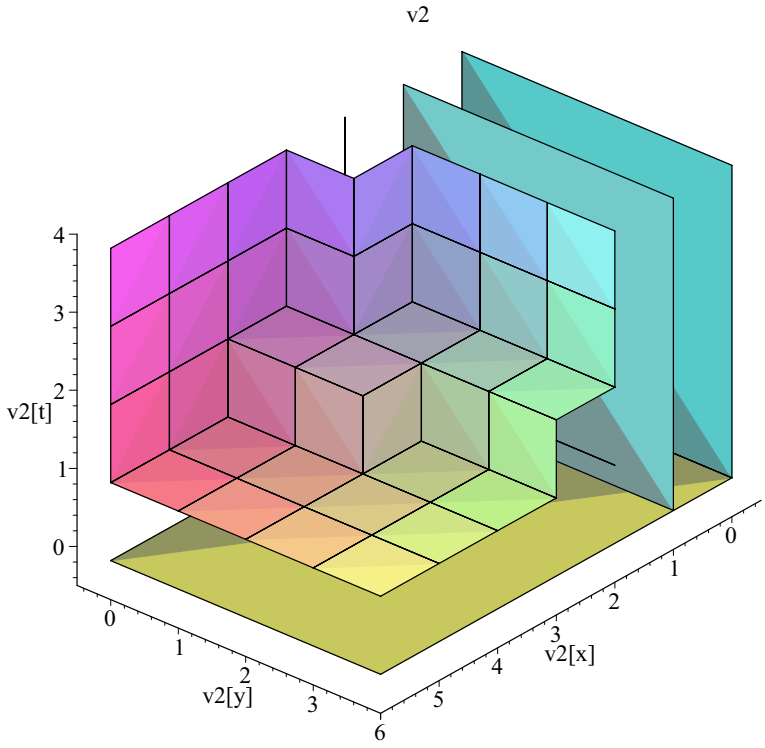


FIG. 5.1 – *Escalier de* v^2

équations d'ordre 5 en v^2 dans sa thèse [5]. Les deux équations restantes en v^2 étaient quant à elles inconnues.

Un autre défi (de Pommaret) est de calculer une chaîne différentielle régulière $\overline{C}$ pour un classement éliminant v^1 et v^2, telle que $\sqrt{[\Sigma]} = [\overline{C}] : H_{\overline{C}}{}^{\infty}$. Le défi reste ouvert.

5.7 Les fonctions complète et spé_regCaractéristique

Les deux fonctions spé_Rosenfeld–Gröbner et Pardi font appel à la fonction complète. Une version simple de cette fonction a été donnée dans les pages précédentes. Une version plus sophistiquée, décrite dans [8], met en pratique l'analogue des critères de Buchberger. Comme dans le cas des bases de Gröbner, ces critères permettent de supprimer certains éléments de l'ensemble des paires critiques non encore traitées. Le pseudo-code de cette fonction peut être trouvé dans [17].

La fonction spé_regCaractéristique est une version sans scindages de la fonction regCaractéristique : c'est encore la chaîne différentielle régulière initiale C qui permet de décider dans quelle branche il faut poursuivre le calcul. Contrairement à l'algorithme regCaractéristique, spé_regCaractéristique ne normalise pas les polynômes. Ainsi l'ensemble obtenu est une chaîne différentielle régulière et non une présentation caractéristique.

La fonction estRégulier vérifie si un polynôme est régulier modulo le saturé par ses initiaux d'une chaîne régulière. Soit elle renvoie *vrai*, soit elle lève une exception indiquant

qu'une factorisation a été découverte. Son fonctionnement est expliqué dans la section 1.5.

```
fonction spé_regCaractéristique(in A,S,C)
début
  Ā := A
  S̄ := S \ {K ∪ I_A}
  S̄ := reste_partiel(S̄,Ā)    (Ā = 0, S̄ ≠ 0 est alors un système différentiel régulier)
  C̄ := ∅
  tant que Ā ≠ ∅ faire
    prendre p ∈ Ā de dérivée dominante minimale
    tant que non(estRégulier(i_p,C̄)) faire
      récupérer la factorisation g × h d'un élément p_l de C̄
      si g ∉ 𝔞 alors
        remplacer p_l par g dans C̄
      sinon
        remplacer p_l par h dans C̄
      fin si
    fait
    Ā := Ā \ {p}
    C̄ := C̄ ∪ {reste_complet(p,C̄)}
  fait
  tant que S̄ ≠ ∅ faire
    retirer s de S̄
    tant que non(estRégulier(s,C̄)) faire
      récupérer la factorisation g × h d'un élément p_l de C̄
      si g ∉ 𝔞 alors
        remplacer p_l par g dans C̄
      sinon
        remplacer p_l par h dans C̄
      fin si
    fait
  fait
  autoréduire C̄
  retourner C̄
fin
```

5.8 Variantes

Il est intéressant en pratique de maintenir la propriété supplémentaire : A est une chaîne régulière. Lors de la phase différentielle, cela permet de rendre régulière toute nouvelle inéquation ajoutée à S. Ainsi, soit A demeure inchangé, soit A diminue de taille (car un diviseur de zéro a été détecté puis éliminé). Toutefois, les inéquations ainsi traitées doivent être conservées dans S : en effet, il se peut qu'une inéquation de S soit non diviseur de zéro modulo $(A) : {I_A}^{\infty}$ à une certaine étape mais le devienne ultérieurement.

Au final, on a soit perdu du temps de calcul (la régularisation n'a pas modifié A), soit diminué la taille des données, ce qui est appréciable car le grossissement excessif des données fait très souvent échouer les calculs.

Stratégie de choix Dans la fonction Pardi, on est amené à choisir un polynôme de P ou une paire critique de D. La stratégie, que j'ai adoptée dans mon implantation, consiste à choisir une équation dans $P \cup \Delta(D)$ de taille minimale (la taille étant le nombre de monômes de l'équation), dans l'espoir de limiter le grossissement des données. On pourrait également choisir de tirer l'équation de plus petite dérivée dominante.

Justifier telle ou telle stratégie est un problème difficile car il n'existe certainement pas une stratégie "meilleure" que les autres dans tous les cas. Toutefois, on peut imaginer qu'il existe des bonnes stratégies pour certaines classes de systèmes.

Test d'appartenance Le test d'appartenance à $\mathfrak{a} = [C] : {H_C}^\infty$ est très souvent utilisé. La méthode la plus simple pour tester $p \in \mathfrak{a}$ consiste à tester si reste_complet(p,C) vaut zéro. Voici deux méthodes permettant d'améliorer le test d'appartenance à $\mathfrak{a}$.

La première consiste à étudier p, vu comme polynôme univarié en sa dérivée dominante v. Si p s'écrit $p = a_n v^n + \cdots + a_0$ et si la variable v est réduite par rapport à C, alors p est réduit à 0 par C si et seulement si chaque a_i est réduit à 0 par C. Par conséquent, dès qu'un des coefficients a_i n'est pas réduit à zéro, on en déduit immédiatement que p n'appartient pas à $\mathfrak{a}$. Dans le cas où v n'est pas réduite, il suffit de réécrire v dans p et de reprendre le raisonnement. Bien entendu, on utilise recursivement la même méthode pour tester si chaque a_i est dans $\mathfrak{a}$.

La deuxième méthode est l'heuristique suivante : on attribue aux dérivées sous l'escalier des dérivées dominantes de C une valeur entière dans $\mathbb{Z}/n\mathbb{Z}$ (où n est premier). Si le polynôme p (évalué sur les valeurs entières choisies aléatoirement) ne se réduit pas à zéro, alors p n'est pas réduit à 0 par C. Si le polynôme p évalué est réduit à zéro, on ne peut conclure et il faut alors tester par un autre moyen si p est réduit ou non à zéro par C. Notez qu'on peut, en cas d'échec, essayer à nouveau l'heuristique sur des valeurs entières différentes.

Réduction d'un polynôme Lorsque l'on réduit un polynôme p par un ensemble triangulaire A, il peut être intéressant de considérer d'abord les équations "simples" de A.

Exemple ▷ Si l'ensemble A contient une équation $k_t = 0$ (k est une fonction ne dépendant pas du temps), il est particulièrement intéressant de l'utiliser en premier pour réduire le polynôme $p = q_1\, k_{ttt} + q_2\, k_t + q_3$, où les q_i sont des polynômes.

En effet, une fois la règle $k_t = 0$ appliquée, la partie $q_1\, k_{ttt} + q_2\, k_t$ a disparu. Le gain peut être important si les polynômes q_1 et q_2 sont de grande taille. ◁

Calcul des delta-polynômes Le calcul des delta-polynômes peut être particulièrement coûteux et mérite d'être analysé finement.

Le delta–polynôme $\Delta(p_1,p_2)$ d'une paire critique $\{p_1,p_2\}$ (qui n'est pas une paire de réduction) est de la forme $s_1\theta_1 p_1 - s_2\theta_2 p_2$ où θ_1 et θ_2 sont deux opérateurs de dérivation.

Au moment ou l'on calcule un tel delta–polynôme dans l'algorithme Pardi, les polynômes s_1 et s_2 appartiennent à l'ensemble des inéquations. Ainsi, au lieu de considérer le delta–polynôme, on peut considérer le polynôme $(s_1/g)\theta_1 p_1 - (s_2/g)\theta_2 p_2$, où g est le pgcd de s_1 et s_2. On réduit ainsi la taille du polynôme à traiter.

En général, le calcul d'un delta–polynôme est suivi d'une réduction par un ensemble triangulaire A. Il est possible de calculer le delta-polynôme en appliquant, à la volée, des réductions par A. L'idée est que le calcul de $\theta_1 p_1$ et $\theta_2 p_2$ peut faire apparaître un nombre important de dérivées qui nécessiteront un nombre important de réductions. Dans certains cas, en appliquant à la volée des réductions par A, on limite ce nombre de dérivées et on peut espérer limiter la taille des données ainsi que le nombre de réductions.

Pour ce faire, il suffit de trouver deux opérateurs de dérivations θ' et θ'' tels que $\theta_1 = \theta'\theta''$ et $\theta'' p_1$ n'est pas réduit par rapport à A. Au lieu de calculer $\theta_1 p_1$, on calcule θ' reste_complet$(\theta'' p_1, A)$ et on recommence le raisonnement.

Traitement des inéquations Rendre régulière une inéquation s est d'autant plus facile que l'inéquation s est de petite taille. Il y a, au moins, deux façons de faciliter les régularisations.

Tout d'abord, on peut considérer la partie sans carrés de s. Par exemple, il est équivalent de rendre réguliers les polynômes $(x+1)^3(x+2)^2(x+5)$ et $(x+1)(x+2)(x+5)$. Le gain peut être particulièrement important. En effet, il est arrivé, dans un exemple, qu'on ait à rendre régulier le polynôme $x^{64}(x+1)$. Rendre régulier la partie sans carrés (à savoir $x(x+1)$) était presque instantané alors que rendre régulier $x^{64}(x+1)$ était extrêmement coûteux.

On peut également factoriser l'inéquation s et rendre régulier chacun des facteurs. Il faut cependant garder à l'esprit que, contrairement à l'algorithme de partie sans carrés, l'algorithme de factorisation est complexe et peut être très coûteux. L'utilisation de la factorisation est donc sujette à discussion.

Conclusion

Cette thèse fournit des outils pour étudier les systèmes d'équations aux dérivées partielles polynomiales. Les nouveaux résultats obtenus sont aussi bien théoriques que pratiques.

D'un point de vue théorique, nous avons une meilleure compréhension des outils mathématiques utilisés dans cette thèse. Premièrement, le parallèle entre les chapitres 1 et 2 illustre le lien qui existe entre le cas algébrique et le cas différentiel. On retiendra, en particulier, l'introduction de la notion de *chaîne différentielle régulière* qui étend naturellement la notion de chaîne régulière pour le cas algébrique. Deuxièmement, l'étude du caractère analytique des solutions des systèmes différentiels réguliers a montré (contre-exemple de la section 3.5) que l'utilisation d'un classement de Riquier était capitale, contrairement à ce que l'on conjecturait.

D'un point de vue pratique, nous avons donné une méthode de calcul de la forme normale d'un polynôme (modulo une chaîne différentielle régulière) ainsi que deux nouveaux algorithmes utiles pour calculer des chaînes différentielles régulières. Le premier, regCaractéristique, a remplacé, dans l'algorithme Rosenfeld–Gröbner, le calcul des bases de Gröbner par des techniques algébriques triangulaires, mieux adaptées.

Le second algorithme, Pardi, est une alternative à l'algorithme Rosenfeld–Gröbner. L'atout essentiel de cet algorithme est de repérer les sous–problèmes algébriques et de les traiter de manière algébrique (par un calcul de pgcd).

Ces deux algorithmes ont permis d'accélérer les temps de calcul, et surtout de traiter des exemples jusqu'ici non résolus, notamment par une meilleure maîtrise de la croissance de la taille des données.

Tous ces résultats vont me permettre de mettre à jour le paquetage `diffalg`. Les deux algorithmes regCaractéristique et Pardi vont y être intégrés, ainsi que le calcul de forme normale de polynômes. Ce travail sera réalisé lors de mon post-doctorat qui aura lieu dans l'équipe ORCCA de l'université du Western Ontario (London, Canada).

Actuellement, mes travaux portent sur l'étude des solutions des chaînes différentielles régulières. Je tente d'affiner les résultats déjà obtenus sur l'analycité des solutions, pour obtenir une estimation des domaines de convergence des solutions. J'espère également, dans le cas où une solution n'est pas analytique, pouvoir déterminer si cette solution appartient à une certaine classe de séries formelles (notamment celle des séries formelles Gevrey).

Parallèlement, je prendrai part à la collaboration entre l'équipe de Calcul Formel de Lille et Greg Reid, membre de l'équipe ORCCA. Nous espérons mieux comprendre les

liens existant entre l'algèbre différentielle et la géométrie différentielle (dont Greg Reid est un spécialiste) afin de tirer parti des avantages des deux approches.

Annexe A

Compléments mathématiques

A.1 Lemme d'Hadamard

Il s'agit d'un théorème puissant, exprimant le domaine de convergence d'une série formelle. Le lemme qui suit est tiré de [55, page 106].

Lemme 21 (Lemme d'Hadamard généralisé) *Soit la série formelle S en $x_1, \ldots, x_m$ notée $S = \sum_{\alpha \in \mathbb{N}^m} c_\alpha x^\alpha$. Pour $k \in \mathbb{N}$, on définit $c_k = \max_{|\alpha|=k} |c_\alpha|$, où $|\alpha| = \alpha_1 + \cdots + \alpha_m$. Soit r un réel strictement positif. Les trois points sont équivalents :*

1. *la série formelle S converge dans l'ouvert $\{x \in \mathbb{C}^m \mid |x_i| < r \text{ pour } 1 \leq i \leq m\}$*
2. *la série formelle de la variable z complexe $\sum_{k=0}^{\infty} c_k z^k$ converge pour $|z| < r$*
3. $\limsup_k c_k^{\frac{1}{k}} \leq \frac{1}{r}$

Annexe B

Évolution du paquetage `diffalg`

Le paquetage `diffalg` va faire l'objet de multiples changements. Parmi ceux-ci, certains sont à l'étude et ne seront apportés que dans des versions futures de `diffalg`.

regCaractéristique Le remplacement du calcul de bases de Gröbner par regCaractéristique a déjà été réalisé dans une version beta et sera donc facilement intégré à `diffalg`. Cette modification sera logiquement complètement transparente pour l'utilisateur.

Pardi L'algorithme Pardi est un peu plus complexe d'utilisation que Rosenfeld–Gröbner car il nécessite en entrée une chaîne différentielle régulière et non un système quelconque. Pour cette raison, Pardi sera certainement accompagné de fonctions d'aide à l'utilisateur.

Formes normales Le calcul des formes normales devrait se faire sans encombres. Il faut cependant veiller à gérer correctement les calculs d'inverses des initiaux et des séparants qui peuvent provoquer des scindages. Une méthode simple est de précalculer les inverses de ces initiaux et séparants pour éviter tout scindage intempestif.

Analycité des solutions Grâce aux résultats du chapitre 3, on dispose du théorème 17 garantissant l'analycité d'une solution sous certaines conditions. Ces conditions peuvent être testées algorithmiquement. Ainsi, on peut coder une fonction qui assure, en vérifiant les hypothèses du théorème d'analycité, que la solution est analytique. Comme le théorème d'analycité ne fournit que des conditions suffisantes, la réponse ne sera que partielle.

Dans le cas où la solution est analytique, j'espère pouvoir intégrer une fonction capable de donner une estimation du domaine de convergence. Ceci pourrait être utile pour une éventuelle évaluation numérique de la solution.

Index

Bibliographie

[1] Philippe Aubry, *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.*, Ph.D. thesis, Université Paris VI, 1999. *(cité p. v, 13)*

[2] Philippe Aubry, Daniel Lazard, and Marc Moreno Maza, *On the theories of triangular sets*, Journal of Symbolic Computation **28** (1999), 105–124. *(cité p. 7, 11, 13, 23, 32, 33)*

[3] Philippe Aubry and Marc Moreno Maza, *Triangular Sets for Solving Polynomial Systems: A Comparative Implementation of Four Methods*, Journal of Symbolic Computation **28** (1999), no. 1–2, 125–154. *(cité p. 109)*

[4] Thomas Becker and Volker Weispfenning, *Gröbner Bases: a computational approach to commutative algebra*, Graduate Texts in Mathematics, vol. 141, Springer Verlag, 1991. *(cité p. 95)*

[5] François Boulier, *Étude et implantation de quelques algorithmes en algèbre différentielle*, Ph.D. thesis, Université Lille I, 59655 Villeneuve d'Ascq France, 1994. *(cité p. 44, 45, 77, 118)*

[6] ———, *Efficient computation of regular differential systems by change of rankings using Kähler differentials*, Tech. Report LIFL 1999–14, Université Lille I, 59655 Villeneuve d'Ascq France, `http://www.lifl.fr/LIFL1/publications.html`, November 1999, (presented at the MEGA2000 conference). *(cité p. iv, 23, 24, 36, 103)*

[7] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot, *Representation for the radical of a finitely generated differential ideal*, proceedings of ISSAC'95 (Montréal, Canada) (A.H.M. Levelt, ed.), ACM Press, 1995, pp. 158–166. *(cité p. 7, 13, 14, 23, 44, 45)*

[8] ———, *Computing representations for radicals of finitely generated differential ideals*, Tech. Report IT306, Université Lille I, LIFL, 59655 Villeneuve d'Ascq France, 1997, (version published in the habilitation thesis of Michel Petitot, december 1998). *(cité p. vii, 7, 14, 23, 32, 34, 35, 44, 45, 91, 92, 99, 104, 118)*

[9] François Boulier, François Lemaire, and Marc Moreno Maza, *PARDI!*, proceedings of ISSAC'01 (London, Ontario, Canada) (Bernard Mourrain, ed.), ACM Press, 2001, pp. 38–47. *(cité p. v, 103)*

[10] François Boulier and François Lemaire, *Computing canonical representatives of regular differential ideals*, proceedings of ISSAC 2000 (St Andrews, Scotland) (Carlo Traverso, ed.), ACM Press, 2000, pp. 37–46. *(cité p. iv, v, 35, 36, 91)*

[11] François Boulier and Sylvain Neut, *Cartan's characters and stairs of characteristic*

sets, Tech. Report LIFL 2001–02, Université Lille I, LIFL, 59655 Villeneuve d'Ascq France, `http://www.lifl.fr/LIFL1/publications.html`, 2001. *(cité p. vii)*

[12] Driss Bouziane, Abdelilah Kandri Rody, and Hamid Maârouf, *Unmixed-dimensional decomposition of a finitely generated perfect differential ideal*, Journal of Symbolic Computation **31** (2001), no. 6, 631–649. *(cité p. 23, 44, 92)*

[13] M. Caboara and M. Silevstri, *Compatible module orderings*, ISSAC'96 Poster Session Abstracts, unpublished, 1996, pp. 17–22. *(cité p. 58)*

[14] Giuseppa Carra-Ferro, *Gröbner bases and differential ideals*, Proceedings of AAECC-5 (Menorca, Spain), Lecture Notes in Computer Science, vol. 356, Springer Verlag, 1987, pp. 129–140. *(cité p. 44)*

[15] Henri Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, Hermann, 1961. *(cité p. 54)*

[16] Philippe G. Ciarlet, *Introduction à l'analyse numérique matricielle et à l'optimisation*, Dunod, 1980. *(cité p. 51, 52)*

[17] Jean Della Dora (ed.), *Triangularisation de systèmes différentiels (par François Boulier)*, série IC2 (Information, Commande, Communication), Hermès, 2000, (to publish, in French). *(cité p. 104, 118)*

[18] Jean Della Dora, Claire Dicrescenzo, and Dominique Duval, *About a new method for computing in algebraic number fields*, Proceedings of EUROCAL'85, vol. 2 (B. F. Caviness, ed.), Lecture Notes in Computer Science, vol. 204, Springer Verlag, 1985, pp. 289–290. *(cité p. 91)*

[19] Lionel Ducos, *source of the axiom package pseudoremaindersequence*, *http://mathrs.sp2mi.univ-poitiers.fr/cgi-bin/cgiwrap/~ducos/page?travaux*, 1995, (last updated: may 1999). *(cité p. 109)*

[20] ———, *Optimizations of the subresultant algorithm*, Journal of Pure and Applied Algebra **145** (2000), 149–163. *(cité p. 18, 108, 109, 111)*

[21] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, vol. 150, Springer Verlag, 1995. *(cité p. 12, 13, 94)*

[22] Jean-Charles Faugère, Patricia Gianni, Daniel Lazard, and Teo Mora, *Efficient computation of Gröbner bases by change of orderings*, Journal of Symbolic Computation **16** (1993), 329–344. *(cité p. iv, 24, 36)*

[23] Évelyne Hubert, *Factorization free decomposition algorithms in differential algebra*, Journal of Symbolic Computation **29** (2000), no. 4,5, 641–662. *(cité p. 15, 23, 32, 35, 44, 45, 91, 92, 94, 99)*

[24] Maurice Janet, *Leçons sur les systèmes d'équations aux dérivées partielles*, Cahiers Scientifiques, vol. IV, Gauthier–Villars, Paris, 1929. *(cité p. 68, 70, 81)*

[25] Mickael Kalkbrener, *Three contributions to elimination theory*, Ph.D. thesis, Johannes Kepler University, Linz, 1991. *(cité p. 7, 10)*

[26] ———, *A Generalized Euclidean Algorithm for Computing Triangular Representations of Algebraic Varieties*, Journal of Symbolic Computation **15** (1993), 143–167. *(cité p. v, 104)*

[27] Donald Erwin Knuth, *The art of computer programming*, Addison–Wesley, 1966, Second edition. *(cité p. 8)*

[28] Ellis R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973. *(cité p. iii, 23, 24, 25, 31, 44)*

[29] D. König, *Theorie der endlichen und unendlichen Graphen*, Chelsea publ. Co., New York, 1950. *(cité p. 98)*

[30] Sophia Kovalevskaya, *Zur Theorie der partiellen Differentialgleichungen*, J. Reine Agnew. Math. **80** (1875), 1–32. *(cité p. 49, 67)*

[31] Daniel Lazard, *A new method for solving algebraic systems of positive dimension*, Discrete Applied Mathematics **33** (1991), 147–160. *(cité p. v, 7, 16, 36, 104, 109)*

[32] ———, *Solving Zero–dimensional Algebraic Systems*, Journal of Symbolic Computation **13** (1992), 117–131. *(cité p. v, 91)*

[33] François Lemaire, *An orderly linear PDE system with analytic initial conditions with a non analytic solution*, Tech. Report LIFL 2001–10, Université Lille I, LIFL, 59655 Villeneuve d'Ascq France, `http://www.lifl.fr/LIFL1/publications.html`, 2001, (submitted to the JSC Special Issue on Computer Algebra and Computer Analysis). *(cité p. 77)*

[34] Ziming Li and Dongming Wang, *Coherent, regular and simple systems in zero decompositions of partial differential systems*, Systems Science and Mathematical Sciences **12** (1999), 43–60. *(cité p. 44, 91)*

[35] Henri Lombardi, Marie-Françoise Roy, and Mohab Safey El Din, *New structure theorem for subresultants*, Journal of Symbolic Computation **29** (2000), no. 4,5, 663–690. *(cité p. 18, 108)*

[36] Hamid Maârouf, *Étude de Quelques Problèmes Effectifs en Algèbre Différentielle*, Ph.D. thesis, Université Cadi Ayyad, Morocco, 1996. *(cité p. 44, 92)*

[37] E. L. Mansfield, G. J. Reid, and P. A. Clarkson, *Nonclassical reductions of a 3+1-cubic nonlinear schrödinger system*, Computer Physics Communications **115** (1998), 460–488. *(cité p. 44)*

[38] Elizabeth L. Mansfield, *Differential Gröbner Bases*, Ph.D. thesis, University of Sydney, Australia, 1991. *(cité p. 44)*

[39] Marc Moreno Maza, *Calculs de Pgcd au–dessus des Tours d'Extensions Simples et Résolution des Systèmes d'Équations Algébriques*, Ph.D. thesis, Université Paris VI, France, 1997. *(cité p. 18, 91)*

[40] ———, *On Triangular Decompositions of Algebraic Varieties*, Tech. Report 1999–04, NAG, 2000, (presented at the MEGA2000 conference). *(cité p. v, 7, 104, 108, 109)*

[41] Marc Moreno Maza and Renaud Rioboo, *Polynomial gcd computations over towers of algebraic extensions*, Proceedings of AAECC-11, Lecture Notes in Computer Science, vol. 948, Springer Verlag, 1995, pp. 365–382. *(cité p. v, 16, 91, 109)*

[42] Sally Morrison, *Pseudo–Reduction, Second Preliminary Draft*, private communication, december 1995. *(cité p. 13, 14)*

[43] ———, *The Differential Ideal* $[P] : M^\infty$, Journal of Symbolic Computation **28** (1999), 631–656. *(cité p. 7, 13)*

[44] François Ollivier, *Le problème de l'identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité*, Ph.D. thesis, École Polytechnique, Palaiseau, France, 1990. *(cité p. 23, 36, 44, 103)*

[45] Ariane Péladan-Germa, *Tests effectifs de Nullité dans des extensions d'anneaux différentiels*, Ph.D. thesis, École Polytechnique, Palaiseau, France, 1997. *(cité p. vii, 49, 67, 68)*

[46] I. G. Petrovsky, *Lectures on Partial Differential Equations*, Interscience Publishers, 1950. *(cité p. 54, 67, 68, 70)*

[47] Jean-François Pommaret, *New Perspectives in Control Theory for Partial Differential Equations*, IMA Journal of Mathematics Control and Information **9** (1992), 305–330. *(cité p. 117)*

[48] G. J. Reid and C. J. Rust, *Rankings on partial derivatives*, proceedings of ISSAC 1997 (Maui,Hawaii, USA), ACM Press, 1998, pp. 9–16. *(cité p. 25, 56, 58, 77)*

[49] Gregory J. Reid, Ping Lin, and Allan D. Wittkopf, *Differential Elimination–Completion Algorithms for DAE and PDAE*, Studies in Applied Mathematics **106** (2001), no. 1, 1–45. *(cité p. 44, 45)*

[50] Gregory J. Reid, Allan D. Wittkopf, and Alan Boulton, *Reduction of systems of nonlinear partial differential equations to simplified involutive forms*, Eur. J. of Applied Math. **7** (1996), 635–637. *(cité p. 44, 76)*

[51] Charles Riquier, *Les systèmes d'équations aux dérivées partielles*, Gauthier–Villars, Paris, 1910. *(cité p. vii, 49, 68, 81)*

[52] Joseph Fels Ritt, *Differential Algebra*, Dover Publications Inc., New York, 1950. *(cité p. iii, 23, 24, 44, 68)*

[53] L. Robbiano, *Term orderings on the polynomial rings*, Proceedings of EUROCAL'85, vol. 2 (Linz, Austria) (B. F. Caviness, ed.), Lecture Notes in Computer Science, vol. 204, Springer Verlag, 1985, pp. 513–517. *(cité p. 56)*

[54] Azriel Rosenfeld, *Specializations in differential algebra*, Trans. Amer. Math. Soc. **90** (1959), 394–407. *(cité p. 31)*

[55] C. J. Rust, *Rankings on derivatives for elimination algorithms and formal solvability of analytic partial differential equations*, Ph.D. thesis, University of Chicago, 1998. *(cité p. vii, 60, 125)*

[56] C. J. Rust, Gregory J. Reid, and Allan D. Wittkopf, *Existence and Uniqueness Theorems for Formal Power Series Solutions of Analytic Differential Systems*, proceedings of ISSAC'99 (Vancouver, Canada) (Sam Dooley, ed.), ACM Press, 1999. *(cité p. 44)*

[57] Brahim Sadik, *A Bound for the Order of Characteristic Set Elements of an Ordinary Prime Differential Ideal and some Applications*, Journal of AAECC **10** (2000), 251–268. *(cité p. 44)*

[58] ———, *Une note sur les algorithmes de décomposition en algèbre différentielle*, Comptes Rendus de l'Académie des Sciences **330** (2000), 641–646. *(cité p. 44)*

[59] Josef Schicho and Ziming Li, *A construction of radical ideals in polynomial algebra*, Tech. report, RISC, Johannes Kepler University, Linz, Austria, august 1995. *(cité p. 14)*

[60] Abraham Seidenberg, *An elimination theory for differential algebra*, Univ. California Publ. Math. (New Series) **3** (1956), 31–65. *(cité p. 44)*

[61] ———, *Abstract differential algebra and the analytic case*, Proc. Amer. Math. Soc. **9** (1958), 159–164. *(cité p. 39)*

[62] G. Trevisan, *Classificazione dei semplici ordinamenti di un gruppo libero con N generatori*, Rend. Sem. Mat. Univ. Padova **22** (1953), 143–156. *(cité p. 56)*

[63] Dongming Wang, *Decomposing polynomial systems into simple systems*, Journal of Symbolic Computation **25** (1998), 295–314. *(cité p. 91)*

[64] V Weispfenning, *Admissible and linear forms*, AAECC-5 (Menorca, Spain), Lecture Notes on Computer Science, vol. 356, Springer Verlag, 1987, pp. 408–417. *(cité p. 56)*

[65] Wu Wen Tsün, *On the foundation of algebraic differential geometry*, Mechanization of Mathematics, research preprints **3** (1987), 1–26. *(cité p. 44)*

[66] L. Yang and J. Zhang, *Searching dependency between algebraic equations: an algorithm applied to automated reasoning.*, Artificial intelligence in mathematics (1994), 147–156. *(cité p. 7, 10)*

[67] M Zaĭceva, *On the set of orderings of Abelian groups (in Russian)*, Math. USSR Doklady **8** (1953), 135–137. *(cité p. 56)*

Résumé :

Cette thèse est consacrée à l'étude des systèmes d'équations différentielles non linéaires aux dérivées partielles. L'approche choisie est celle de l'algèbre différentielle. Étant donné un système d'équations différentielles, nous cherchons à obtenir des renseignements sur ses solutions. Pour ce faire, nous calculons une famille d'ensembles particuliers (appelés chaînes différentielles régulières) dont la réunion des solutions coïncide avec les solutions du système initial.

Les nouveaux résultats relèvent principalement du calcul formel. Le chapitre 2 clarifie le lien entre les chaînes régulières et les chaînes différentielles régulières. Deux nouveaux algorithmes (chapitres 4 et 5) viennent optimiser les algorithmes existants permettant de calculer ces chaînes différentielles régulières. Ces deux algorithmes intègrent des techniques purement algébriques qui permettent de mieux contrôler le grossissement des données et de supprimer des calculs inutiles. Des problèmes jusqu'à présent non résolus ont ainsi pu être traités. Un algorithme de calcul de forme normale d'un polynôme différentiel modulo une chaîne différentielle régulière est exposé dans le chapitre 2.

Les derniers résultats relèvent de l'analyse. Les solutions que nous considérons sont des séries formelles. Le chapitre 3 fournit des conditions suffisantes pour qu'une solution formelle soit analytique. Ce même chapitre présente un contre-exemple à une conjecture portant sur l'analycité des solutions formelles.

Mots-Clés : calcul formel, informatique, EDP non linéaires, algèbre différentielle, idéal différentiel, ensembles caractéristiques, chaînes différentielles régulières, formes normales, analycité, théorie de Riquier-Janet, théorème de Cauchy-Kovalevskaya.

Abstract:

This thesis is dedicated to the study of nonlinear partial differential equations systems. The chosen approach is using differential algebra. Given a system of differential equations, we seek information about its solutions. To do so, we first compute particular systems (called differential regular chains) such that the union of their solutions coincide with the solutions of the initial system.

This thesis mainly presents new results in symbolic computation. Chapter 2 clarifies the link between regular chains and differential regular chains. Two new algorithms (given in chapters 4 and 5) improve existing algorithms for computing these differential regular chains. These algorithms involve purely algebraic techniques which help reduce expression swell and help avoid unnecessary computations. Previously intractable problems have been solved using these techniques. An algorithm computing the normal form of a differential polynomial modulo a differential regular chain is described in chapter 2.

The last results deal with analysis. The solutions we consider are formal power series. Chapter 3 gives sufficient conditions for a solution to be analytic. The same chapter presents a counter-example to a conjecture dealing with the analyticity of formal solutions.

Keywords: symbolic computation, computer science, nonlinear PDE, differential algebra, differential ideal, characteristic sets, differential regular chains, normal forms, analyticity, Riquier-Janet theory, Cauchy-Kovalevskaya theorem.