Décomposition et intégrales premières rationnelles: algorithmes et complexité

Guillaume Chèze

28 octobre 2015

Préface

- Tu vois, j'aimerais ne pas mourir idiot.
- Ben essaye de pas mourir.
Lindingre, Larcenet*, chez Francisque.*

L'objectif de ces notes est de présenter quelques résultats sur la décomposition des fractions rationnelles ainsi que sur le calcul des intégrales premières rationnelles d'un champ de vecteurs polynomiales du plan. La plupart des résultats présentés ici sont publiés et accessibles. L'objectif est donc de mettre en évidence les idées à l'origine de ceux-ci et les relations entre chacun d'eux.
Ces notes ne prétendent pas être exhaustives. Certaines preuves sont données données afin de faciliter la compréhension du texte mais aussi pour permettre au lecteur de développer une certaine intuition vis à vis des objets manipulés. Les résultats non démontrés sont toujours accompagnés d'une indication bibliographique.

La structure du document est la suivante : Dans une première partie nous présentons le cadre général de ce cours. Dans la seconde partie nous présentons des résultats effectifs permettant de calculer les objets présentés dans la première partie.

Une version préliminaire de ce texte a bénéficié d'une lecture approfondie de Moulay Barkatou, Marc Giusti et Jean-Claude Yakoubsohn. Je les remercie pour leurs remarques et précieux conseils.

Enfin, je remercie les organisateurs des JNCF 2015 de m'offrir l'opportunité de présenter ces résultats dans le cadre d'une école jeunes chercheurs.

Table des matières

Première partie

Contexte général du cours

Chapitre 1

Prélude : Factorisation absolue des polynômes à plusieurs variables

Ce prélude présente certains résultats classiques à propos de la factorisation absolue des polynômes en plusieurs variables. Ces résultats seront utilisés par la suite dans différents contextes et étendus aux polynômes et fractions indécomposables.

Définition 1. *Soit $f \in \mathbb{K}[X_1, \ldots, X_n]$, la factorisation absolue de f est sa factorisation en irréductibles dans $\overline{\mathbb{K}}[X_1, \ldots, X_n]$, où $\overline{\mathbb{K}}$ est une clôture algébrique de $\mathbb{K}$.*

L'ensemble des polynômes absolument réductibles forme une variété algébrique comme le montre le théorème d'E. Noether, [115] suivant :

Théorème 1 (Noether, 1922)**.** *Soit f un polynôme de $\mathbb{K}[X_1, \ldots, X_n]$ de degré au plus d, donné par :*

$$f(X_1, \ldots, X_n) = \sum_{i_1+\cdots+i_n \leq d} c_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}.$$

Considérons des variables $C_{i_1,\ldots,i_n}$ avec $i_1+\cdots+i_n \leq d$. Il existe des polynômes $\Phi_1, \ldots, \Phi_M$ en les $C_{i_1,\ldots,i_n}$ tels que :
f est réductible sur $\overline{\mathbb{K}}$ ou de degré strictement inférieur à d si et seulement si pour tout m tels que $1 \leq m \leq M$ nous avons $\Phi_m(\underline{c}) = 0$, où $\underline{c} = (\ldots, c_{i_1,\ldots,i_n}, \ldots)$.

De plus ces polynômes dépendent uniquement de d et de n et sont indépendants du corps $\mathbb{K}$, plus précisément :
Si $\mathbb{K}$ est de caractéristique nulle alors ils sont à coefficients dans $\mathbb{Z}$, et si $\mathbb{K}$ est de caractéristique $p > 0$ alors ils sont obtenus par réduction modulo p de ces mêmes coefficients.

Ce théorème sera l'outil de base du Chapitre 3. Nous donnerons aussi un résultat similaire pour les polynômes indécomposables dans le Chapitre 4. Comme un des objectifs de ce mémoire est de donner des bornes effectives sur les objets manipulés, nous utiliserons une version effective de ce résultat. De nombreuses versions existent, voir [29, 135], à l'heure actuelle le résultat le plus fin est le suivant :

Théorème 2 (Ruppert, 1986)**.** *Si $\mathbb{K}$ est de caractéristique 0 alors pour $1 \leq m \leq M$ nous avons :*

$$\deg(\Phi_m) \leq d^2 - 1 \ \text{ et } \ \|\Phi_m\|_1 \leq d^{3d^2-3} \left[\binom{n+d}{n} 3^d \right]^{d^2-1}.$$

Nous rappelons que la norme $\|f\|_1$ est définie ainsi : $\|f\|_1 = \sum_{i_1+\cdots+i_n\leq d} |c_{i_1,\ldots,i_n}|$, lorsque $f(X_1,\ldots,X_n) = \sum_{i_1+\cdots+i_n\leq d} c_{i_1,\ldots,i_n} X_1^{i_1}\cdots X_n^{i_n}$.

Dans son livre [135], Schinzel montre que la borne sur $\|\Phi_m\|_1$ peut être améliorée en remplaçant 3^d par 2^d. Nous pouvons d'ores et déjà signaler que l'optimalité de ces bornes n'est pas connue.

Il est intéressant de préciser les grandes lignes de la preuve de Ruppert. En effet, cette preuve sera reprise dans la suite de ce mémoire afin d'obtenir une description précise de certains objets. De plus, cela fait apparaître le lien existant entre la factorisation absolue et l'étude des équations différentielles. Ce lien sera repris dans le Chapitre 2.

La stratégie de Ruppert repose sur l'étude du premier groupe de cohomologie de de Rham du complémentaire d'une courbe algébrique plane et sur l'utilisation du théorème de Bertini. Commençons par étudier le complémentaire d'une courbe plane, nous énoncerons ensuite le théorème de Bertini et verrons comment l'utiliser.

Soit $f \in \mathbb{K}[X,Y]$, où $\mathbb{K}$ est un corps de caractéristique nulle. Soit $f = f_1^{e_1}\cdots f_r^{e_r}$ sa factorisation absolue. On désigne par $\mathcal{V}(f)$ l'ensemble des zéros de f dans $\overline{\mathbb{K}}^2$. Par définition, $\mathcal{H}^1\big(\overline{\mathbb{K}}^2\setminus\mathcal{V}(f)\big)$ est le quotient des 1-formes différentielles fermées $\omega \in \Omega_{\overline{\mathbb{K}}[X,Y]_f/\overline{\mathbb{K}}}$ par les 1-formes exactes. Une propriété classique de $\mathcal{H}^1\big(\overline{\mathbb{K}}^2 \setminus \mathcal{V}(f)\big)$ est que cet espace vectoriel a pour base : $\frac{df_1}{f_1},\ldots,\frac{df_r}{f_r}$, voir [47, Chapter 4, Corollary 1.4], ou [133, 131]. Ainsi l'irréductibilité absolue de f se voit sur la dimension de $\mathcal{H}^1\big(\overline{\mathbb{K}}^2 \setminus \mathcal{V}(f)\big)$. Ruppert a donc été amené à étudier la structure des formes fermées. Il a alors donné le résultat suivant :

Proposition 1. *Soit ω une forme fermée de $\overline{\mathbb{K}}[X,Y]_f$. Il existe alors p et q dans $\overline{\mathbb{K}}[X,Y]$ et c_i dans $\overline{\mathbb{K}}$ tels que :*

$$\omega = \sum_i c_i \frac{df_i}{f_i} + d\Big(\frac{p}{q}\Big).$$

Ce résultat sur la structure d'une forme fermée était déjà connu de Picard, voir [124]. A partir de cette proposition, et de l'étude du degré des formes exactes $d(\frac{p}{q})$ nous pouvons alors ramener l'étude des formes closes à celles des formes closes de degré inférieur ou égale à $d-1$ du type $\frac{g}{f}dX + \frac{h}{f}dY$ avec $\deg(Xg+Yh) \leq d-1$. On considère alors l'espace vectoriel et l'application linéaire suivante :

Définition 2. *Soit $f \in \mathbb{K}[X,Y]$ un polynôme de degré d. On note $\mathcal{E}$ l'espace vectoriel suivant :*

$$\mathcal{E} = \{(g,h) \in \mathbb{K}[X,Y]^2_{d-1} \mid \deg(Xg+Yh) \leq d-1\}.$$

On note $\mathcal{R}up(f)$ l'application linéaire suivante :

$$\begin{array}{rcl} \mathcal{R}up(f) : \mathcal{E} & \longrightarrow & \mathbb{K}[X,Y]_{2d-3} \\ (g,h) & \longmapsto & f^2.\Big[\partial_X\Big(\frac{h}{f}\Big) - \partial_Y\Big(\frac{g}{f}\Big)\Big] \end{array}$$

Le résultat fondamental de Ruppert est le suivant :

Théorème 3. *Soit $f \in \mathbb{K}[X,Y]$ un polynôme de degré d. Nous avons l'équivalence suivante :*

$$\dim_{\mathbb{K}} \ker \mathcal{R}up(f) = 0 \iff f \text{ est absolument irréductible.}$$

Ce résultat se comprend de la manière suivante : $\dim_{\mathbb{K}} \ker \mathcal{R}up(f) = 0$ signifie qu'il n'existe pas de formes closes du type $\frac{g}{f}dX + \frac{h}{f}dY$ avec $(g,h) \in \mathcal{E}$. Le polynôme f ne peut donc pas être réductible. En effet, comme nous l'avons mentionné plus haut, dans ce cas il existerait un facteur f_i de f donnant un élément $\frac{df_i}{f_i}$ dans $\mathcal{H}^1\big(\overline{\mathbb{K}}^2 \setminus \mathcal{V}(f)\big)$. Cet élément donnerait alors une forme close du type $\frac{g_i}{f}dX + \frac{h_i}{f}dY$ avec $(g_i,h_i) \in \mathcal{E}$, ce qui est exclus ici.
Dans le Chapitre 3 nous préciserons ce calcul et nous donnerons la dimension de $\ker \mathcal{R}up(f)$ dans le cas où f est réductible.
Nous pouvons remarquer qu'ici g et h sont à coefficients dans $\mathbb{K}$ et non dans $\overline{\mathbb{K}}$. En effet, si $g,h \in \overline{\mathbb{K}}[X,Y]$ alors en notant $\mathbb{F}$ la plus petite extension galoisienne de $\mathbb{K}$ contenant les coefficients de g et h, et $\mathcal{G}$ le groupe de Galois de $\mathbb{F}$ sur $\mathbb{K}$, alors nous avons $\tilde{g} = \sum_{\sigma\in\mathcal{G}} \sigma(g)(X,Y)$ et $\tilde{h} = \sum_{\sigma\in\mathcal{G}} \sigma(h)(X,Y)$ dans $\mathbb{K}[X,Y]$. Comme $f \in \mathbb{K}[X,Y]$, il vient $(\tilde{g},\tilde{h}) \in \ker \mathcal{R}up(f)$.

La Proposition 1 semble faire partie du folklore. Nous reviendrons sur cette propriété lorsque nous parlerons de systèmes différentiels dans le Chapitre 2. Cette propriété constituera en effet un des liens existant entre l'étude de la factorisation absolue et celle des systèmes différentiels polynomiaux.

Le Théorème 3 nous donne un moyen de calculer des formes de Noether pour les polynômes en deux variables. En effet, chaque coefficient de la matrice associée à $\mathcal{R}up(f)$ est donné par un coefficient de f. De plus, $\dim_{\mathbb{K}} \ker \mathcal{R}up(f) \neq 0$ équivaut à avoir tous les mineurs maximaux de $\mathcal{R}up(f)$ identiquement nuls. Ces mineurs sont donc des polynômes en les coefficients de f qui caractérisent l'irréductibilité absolue de f à la manière des Φ_m du Théorème 1. La borne sur le degré des Φ_m, annoncée dans le Théorème 2 provient du fait que $\dim_{\mathbb{K}} \mathcal{E} = d^2 - 1$. La borne sur la hauteur des Φ_m découle d'un calcul direct.

Pour obtenir la version effective du théorème de Noether en n variables nous devons utiliser le théorème de Bertini que nous rappelons ci-dessous. Ce théorème permet de ramener l'étude du problème de n à 2 variables.

Theorem 4 (Bertini)**.** *Soient $f \in \mathbb{K}[X_1,\ldots,X_n]$, $A_2,\ldots,A_n$, $B_2,\ldots,B_n$, $C_1,\ldots,C_n$ des variables indépendantes sur $\mathbb{K}$, $\mathbb{L} = \mathbb{K}(C_1,A_2,B_2,C_2,\ldots,A_n,B_n,C_n)$ et*

$$f_0 = f(X + C_1, A_2X + B_2Y + C_2, \ldots, A_nX + B_nY + C_n) \in \mathbb{L}[X,Y].$$

On a alors : f_0 est absolument irréductible sur $\mathbb{L}$ si et seulement si f est absolument irréductible sur $\mathbb{K}$.

En étudiant alors l'application $\mathcal{R}up(f_0)$, nous voyons que les mineurs de cette application sont des polynômes en les coefficients de f, en les A_i, en les B_i et en les C_i. Les formes de Noether sont alors les coefficients des mineurs maximaux de $\mathcal{R}up(f_0)$ vus

comme des polynômes en les A_i, B_i, C_i et cela achève notre étude de la preuve de Ruppert.

Nous venons de voir l'utilité du théorème de Bertini. Certains auteurs attribuent à juste titre ce résultat à Hilbert, voir e.g. [81, 61]. En effet, ce résultat était connu de Hilbert, voir [76]. D'autres auteurs attribuent ce résultat à Zariski-Matsusaka et la substitution utilisée est alors du type $X_i := A_i + B_i X_n$ pour $i = 1, \ldots, n-2$, voir e.g. [90, 56]. Comme l'énoncé général de ce théorème dans le cas d'une variété algébrique est souvent attribué à Bertini, nous avons gardé ici cet usage. Nous pouvons consulter à ce propos l'introduction du livre de Jouanolou [80].
Le théorème de Bertini a été utilisé ci-dessus de manière théorique afin d'obtenir le théorème de Noether pour les polynômes en n variables. Ce théorème est aussi utilisé de manière pratique pour factoriser des polynômes en n variables. Nous obtenons alors des algorithmes probabilistes où la réduction de n à 2 variables est justifiée par un théorème de Bertini effectif. Ce genre de résultat repose sur l'utilisation du lemme de Zippel-Schwartz, voir [151, 137] que nous rappelons ci-dessous :

Lemme 1 (Zippel-Schwartz)**.** *Soit $\varphi \in A[X_1, \ldots, X_n]$ un polynôme de degré total d, où A est un anneau intègre. Soit S un sous ensemble fini de A contenant $|S|$ éléments. Nous avons alors la probabilité suivante en prenant x_i au hasard de manière uniforme dans S :*

$$\mathcal{P}\big(\varphi(x_1, \ldots, x_n) = 0 \,|\, x_i \in S\big) \leq \frac{d}{|S|}.$$

L'utilisation des formes de Noether effectives données par le Théorème 2 appliquées au polynôme f_0 nous permet d'obtenir un théorème de Bertini effectif via le lemme de Zippel-Schwartz, voir [29]. La version effective la plus fine connue à ce jour est dûe à Lecerf, voir [92] :

Théorème 5 (Bertini effectif, Lecerf 2007)**.** *Soit $f \in \mathbb{K}[X_1, \ldots, X_n]$ un polynôme irréductible de degré d, où $\mathbb{K}$ est un corps de caractéristique 0 ou supérieur à $d(d-1)+1$. Soit S un sous ensemble fini de $\mathbb{K}$.*
Lorsque nous prenons $a_1, \ldots, a_n$, $b_1, \ldots, b_n$, $c_1, \ldots, c_n$ de manière uniforme dans S, la probabilité que $f(a_1X + b_1Y + c_1, \ldots, a_nX + b_nY + c_n)$ soit réductible dans $\mathbb{K}[X, Y]$et de degré d est inférieure à $\frac{3d(d-1)+1}{|S|}$.

Ce résultat est optimal à une constante multiplicative près.

Comme autre corollaire du théorème de Noether nous pouvons obtenir un résultat dû à Ostrowski. Celui-ci avait énoncé son résultat en 1919, cela n'était donc pas à l'époque un corollaire du résultat de Noether.

Corollaire 1 (Ostrowski 1919, Ruppert 1986)**.** *Soit $f(X, Y) \in \mathbb{Z}[X, Y]$ un polynôme absolument irréductible de degré total d.*
Soit p un nombre premier tel que $p > d^{3d^2-3}\|f\|_\infty^{d^2-1}$ alors $\overline{f}(X, Y) \in \mathbb{F}_p[X, Y]$ est absolument irréductible.

Nous rappelons que $\|f\|_\infty$ désigne la hauteur de f, c'est à dire $\|f\|_\infty = \max_{i_1,\ldots,i_n} |c_{i_1,\ldots,i_n}|$, lorsque $f(X_1, \ldots, X_n) = \sum_{i_1,\ldots,i_n} c_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}$.

La preuve de ce résultat est immédiate. En effet, si f est absolument irréductible alors il existe une forme de Noether $\Phi_m(\underline{c})$ qui est non nulle. Nous pouvons majorer la taille de cet entier à l'aide de la hauteur de f et de la borne sur $\|\Phi_m\|_1$. Cette estimation est l'entier donné dans le corollaire ci-dessus. Ensuite, en prenant un premier supérieur à cet entier nous avons $\overline{\Phi_m(\underline{c})} = \Phi_m(\overline{\underline{c}})$ différent de zéro dans $\mathbb{F}_p$. C'est ce qui démontre l'irréductibilité absolue de $\overline{f}$ d'après le théorème de Noether.

Gao et Rodrigues ont amélioré ce résultat en remplaçant dans la borne ci-dessus d^2-1 par la taille du polytope de Newton de f, voir [62]. Nous rappelons ci-dessous la définition du polytope de Newton d'un polynôme. Cette notion sera utilisée régulièrement dans ce mémoire.

Définition 3. *Soit $f(X_1,\ldots,X_n) = \sum_{i_1,\ldots,i_n} c_{i_1,\ldots,i_n} X_1^{i_1}\cdots X_n^{i_n} \in \mathbb{K}[X_1,\ldots,X_n]$. Le polytope de Newton de f, noté $\mathcal{N}(f)$, est l'enveloppe convexe des points $(i_1,\ldots,i_n) \in \mathbb{R}^n$ tels que $c_{i_1,\ldots,i_n} \neq 0$.*
La taille de $\mathcal{N}(f)$ est le nombre de points à coefficients entiers dans $\mathcal{N}(f)$.

Une telle notion permet de prendre en compte le fait qu'un polynôme peut avoir beaucoup de coefficients nuls. Par exemple, si l'on considère $f(X,Y) = X^eY^e + X^{e-1}Y^e + X^eY^{e-1} + 1$ alors la taille de $\mathcal{N}(f)$ est égale à $e+3$. Ainsi dans ce cas, si on remplace $(2e)^2-1$ par la taille de $\mathcal{N}(f)$ dans la borne d'Ostrowski, celle-ci est significativement améliorée.

La figure ci-dessous représente le polytope de Newton du polynôme "creux" $X^3Y^3 + X^2Y^3 + X^3Y^2 + 1$. Le triangle représente ce que serait le polytope de Newton d'un polynôme dense de degré 6, c'est à dire un polynôme ayant tous ses coefficients non nuls.

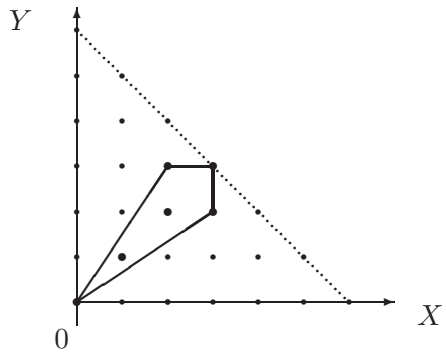

FIGURE 1.1 – $\mathcal{N}(X^3Y^3 + X^2Y^3 + X^3Y^2 + 1)$.

Chapitre 2

Équations différentielles polynomiales dans le plan

Ce chapitre a pour but de donner le cadre général de ce cours. Nous verrons ainsi que les différents concepts rencontrés au cours de ce mémoire sont issus de l'étude des solutions formelles de l'équation différentielle autonome suivante :

$$\dot{X} = A(X,Y),\ \dot{Y} = B(X,Y), \tag{2.1}$$

où $\dot{X}$ et $\dot{Y}$ représentent les dérivées par rapport au temps t, et $A, B \in \mathbb{C}[X,Y]$.
Géométriquement, l'objet associé à l'équation différentielle est le champ de vecteurs : $A(X,Y)dX+B(X,Y)dY$. Nous supposerons dans tout ce qui suit que A et B sont premiers entre eux. En effet, si ce n'est pas le cas alors le champ de vecteurs peut être simplifié en divisant par le facteur commun.
L'objet algébrique permettant d'étudier les solutions formelles de l'équation 2.1 est une dérivation.

Définition 4. *Une dérivation D sur l'anneau $\mathbb{C}[X,Y]$ est une application linéaire qui vérifie la règle de Leibniz pour le produit :*

$$D(f.g) = D(f).g + f.D(g).$$

Ainsi à l'équation différentielle 2.1 nous associons la dérivation suivante :

$$D = A(X,Y)\partial_X + B(X,Y)\partial_Y.$$

Le degré de la dérivation D est le maximum des degrés de A et de B.

Nous pouvons alors donner de manière grossière une première idée de ce que signifie résoudre formellement l'équation 2.1. Nous serons plus précis dans un instant.
Résoudre formellement l'équation 2.1 c'est trouver une "fonction" $\mathcal{F}(X,Y)$ telle que les lignes de niveaux de $\mathcal{F}$ correspondent aux orbites de l'équation 2.1.
Nous parlons de "fonctions" entre guillemets car $\mathcal{F}$ peut être une fonction multivaluée.

Soit $\big(X(t),Y(t)\big)$ une solution de l'équation 2.1, $\mathcal{F}$ doit donc vérifier $\mathcal{F}\big(X(t),Y(t)\big) = c$, où c est une constante. En dérivant on obtient : $\partial_X(\mathcal{F})\dot{X} + \partial_Y(\mathcal{F})\dot{Y} = 0$. Comme

$\big(X(t), Y(t)\big)$ est une solution de l'équation 2.1 on obtient $A\partial_X(\mathcal{F}) + B\partial_Y(\mathcal{F}) = 0$. Cela donne la définition suivante :

Définition 5. *On appelle intégrale première une fonction non constante, éventuellement multivaluée, $\mathcal{F}$ vérifiant $D(\mathcal{F}) = 0$.*

Dans ce mémoire, nous nous intéresserons plus particulièrement aux intégrales premières rationnelles, c'est à dire au cas où $\mathcal{F}(X, Y) \in \mathbb{C}(X, Y) \setminus \mathbb{C}$. Ce seront donc des fonctions univaluées. Lorsque nous manipulerons des fonctions multivaluées nous préciserons dans quelle classe de fonctions nous nous plaçons (élémentaires ou liouvilliennes voir Section 2.7).

Résoudre formellement l'équation 2.1 signifiera calculer, lorsque cela est possible, une intégrale première.

On remarque que la 1-forme $\omega = -B(X, Y)dX + A(X, Y)dY$ est exacte signifie qu'il existe une fonction $\mathcal{F}$ telle que $-B = \partial_X(\mathcal{F})$ et $A = \partial_X(\mathcal{F})$. Donc, cela signifie que $\mathcal{F}$ est une intégrale première.

Au voisinage d'un point régulier, c'est à dire un point (x, y) tel que $A(x, y) \neq 0$ ou $B(x, y) \neq 0$, il existe toujours une intégrale première. Ce résultat se déduit du théorème de Cauchy-Lipschitz (avec dépendance de la condition initiale) et du théorème des fonctions implicites, pour une preuve le lecteur peut consulter le livre de Cartan [25]. La difficulté lors de l'étude des intégrales premières est donc celle de l'existence globale.

Nous avons représenté dans la figure 2.1 le champ de vecteurs où

$$\begin{aligned} A(X,Y) &= 2\,X^4Y - 2\,Y - Y^2X^2 + X^6 - X^2 + Y^2 - X^4 + 1 + Y^2X^3 - X^7 + X^3 \\ &\quad -9\,XY^2 + 9\,X^5 - 9\,X + 2\,YX^5 - 20\,YX^3 + 18\,XY, \end{aligned}$$

$$\begin{aligned} B(X,Y) &= -9 + 9\,Y + X^8 + 9\,Y^2 - 9\,Y^3 + 30\,X^2 - 32\,X^4 + 10\,X^6 - 3\,YX^2 + 2\,XY \\ &\quad -30\,Y^2X^2 - 4\,YX^3 + 4\,Y^2X^3 + 3\,Y^3X^2 - 2\,Y^3X + 27\,X^4Y + 2\,YX^5 \\ &\quad +5\,Y^2X^4 - YX^6. \end{aligned}$$

Dans ce cas nous avons une intégrale première dont nous avons tracé une ligne de niveau à la figure 2.1. Dans les figures suivantes, nous avons tracé d'autres lignes de niveaux pour le même champ de vecteurs. Les vecteurs dessinés dans les figure 2.1 et 2.2 ont été normalisés afin d'obtenir une représentation plus agréable.

Comment avons nous fabriqué un tel exemple ? Autrement dit, étant donné une fonction $\mathcal{F}$ peut-on fabriquer aisément une dérivation D dont $\mathcal{F}$ est une intégrale première ? La dérivation $D_{\mathcal{F}} = -\partial_Y(\mathcal{F})\partial_X + \partial_X(\mathcal{F})\partial_Y$ répond à cette question. Nous appelons ce type de dérivation une dérivation jacobienne. Comme nous sommes dans un cadre où nous considérons uniquement des dérivations du type $A\partial_X + B\partial_Y$ avec $A, B \in \mathbb{C}[X, Y]$, les dérivations jacobiennes que l'on étudiera seront du type suivant :

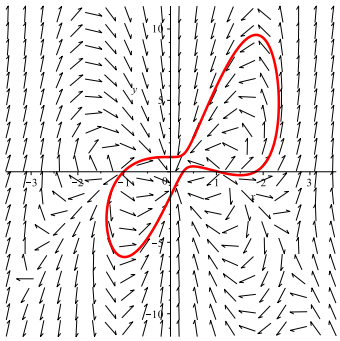

FIGURE 2.1 – Exemple d'un champ de vecteurs avec une ligne de niveau d'une intégrale première.

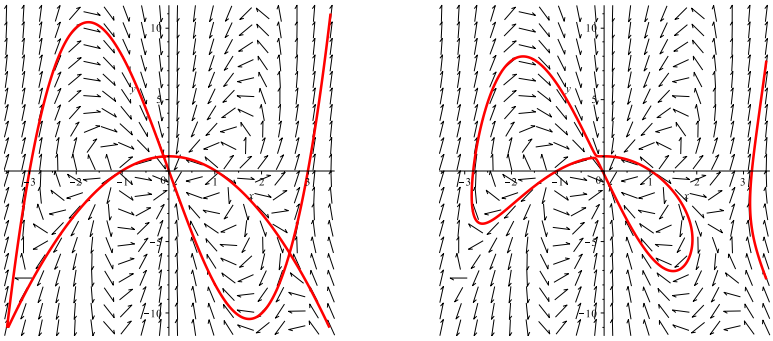

FIGURE 2.2 – Autres lignes de niveaux.

Définition 6. *Soit $F \in \mathbb{C}[X,Y]$ un polynôme.*
La dérivation : $D_F = -\partial_Y(F)\partial_X + (\partial_X F)\partial_Y$ s'appelle la dérivation jacobienne associée à F.
Soit $F_1/F_2 \in \mathbb{C}(X,Y)$ une fraction rationnelle.
La dérivation : $D_{F_1/F_2} = -\big(\partial_Y(F_1)F_2 - F_1\partial_Y(F_2)\big)\partial_X + \big(\partial_X(F_1)F_2 - F_1\partial_X(F_2)\big)\partial_Y$ s'appelle la dérivation jacobienne associée à F_1/F_2.

La propriété suivante est immédiate.

Proposition 2. *Le polynôme F est une intégrale première de D_F.*
La fraction rationnelle F_1/F_2 est une intégrale première de D_{F_1/F_2}.

Pour fabriquer l'exemple présenté aux figures 2.1 et 2.2 nous sommes partis de

$$\mathcal{F}(X,Y) = \frac{\big(Y - X(X-3)(X+3)\big)(Y + X^2 - 1)}{Y^2 + X^4 - 1}.$$

Nous allons voir dans ce chapitre comment l'étude des intégrales premières mène aux notions de polynômes de Darboux, de spectre des fractions rationnelles et de décomposition.

2.1 Les origines : Méthode de Newton et facteur intégrant

L'étude des équations différentielles remonte à l'origine du calcul différentiel. Au fil du temps les méthodes pour résoudre les équations différentielles se sont améliorées.
En 1671, dans son traité Methodus Fluxionum et Serierum Infinitarum, (Problema II, Solutio Casus II, Ex. I), Newton donne une méthode permettant d'obtenir une série formelle solution de l'équation :

$$\frac{\partial Y}{\partial X} = 1 - 3X + Y + X^2 + XY. \tag{2.2}$$

Nous remarquons au passage que les équations du type de 2.2, c'est à dire

$$\frac{\partial Y}{\partial X} = \frac{B(X,Y)}{A(X,Y)},$$

s'obtiennent à partir de celles du type 2.1 en remarquant que $\dfrac{\dot{Y}}{\dot{X}} = \dfrac{\partial Y}{\partial X}$.

La méthode de Newton permet d'obtenir une approximation d'une trajectoire, mais ne permet pas d'obtenir une intégrale première. Toutefois, cette méthode et cette remarque seront utilisées dans le Chapitre 6 afin d'obtenir un algorithme de calcul d'intégrales premières.

Plus tard, au XVIIIème siécle, Clairaut et Euler développent la méthode dite du facteur intégrant, voir [50].

Définition 7. *Soit $\mathcal{R}$ une fonction. On dit que $\mathcal{R}$ est un facteur intégrant de l'équation 2.1 lorsque :*

$$D(\mathcal{R}) = -div(A,B)\mathcal{R},$$

où $div(A,B)$ représente la divergence, i.e. $div(A,B) = \partial_X(A) + \partial_Y(B)$.

L'équation ci-dessus peut s'écrire autrement. En effet, nous avons :

$$\begin{aligned} D(\mathcal{R}) = -div(A,B)\mathcal{R} \quad &\Longleftrightarrow \quad A\partial_X(\mathcal{R}) + B\partial_Y(\mathcal{R}) = -\big(\partial_X(A) + \partial_Y(B)\big)\mathcal{R} \\ &\Longleftrightarrow \quad \partial_X(\mathcal{R}A) = -\partial_Y(\mathcal{R}B). \end{aligned}$$

L'intérêt du facteur intégrant est qu'il vérifie la relation :

$$\partial_X(\mathcal{R}A) = -\partial_Y(\mathcal{R}B).$$

Ainsi, la forme $\omega_{\mathcal{R}} = -RBdX + RAdY$ est une forme différentielle fermée, donc elle est exacte dans un ouvert simplement connexe. Puisque cette forme est exacte nous avons donc localement une primitive, notée $\int \omega_R$, c'est l'intégrale première recherchée car $\omega_{\mathcal{R}}$ est proportionnelle à ω.

Remarque 1. Nous venons de voir qu'un facteur intégrant permet d'obtenir une intégrale première. La réciproque est aussi vérifiée.
En effet, l'équation $A\partial_X(\mathcal{F}) + B\partial_Y(\mathcal{F}) = 0$ entraine $-\partial_Y(\mathcal{F})/A = \partial_X(\mathcal{F})/B$. On note cette expression $\mathcal{R}$ et nous avons : $\partial_X(\mathcal{R}A) = -\partial_Y(\mathcal{R}B)$. Donc $\mathcal{R}$ est un facteur intégrant.

Malheureusement en général le calcul d'un facteur intégrant n'est pas plus simple que celui d'une intégrale première. Afin d'obtenir un facteur intégrant, nous sommes alors amenés à le chercher sous une forme particulière. Par exemple, nous pouvons chercher des facteurs intégrants qui soient des polynômes en deux variables de degré fixé. Dans ce cas, en écrivant $\mathcal{R}$ comme un polynôme à coefficients indéterminés, la recherche d'un facteur intégrant revient à résoudre le système linéaire $D(\mathcal{R}) = -div(A,B)\mathcal{R}$. La recherche de polynômes vérifiant ce type de relation nous mène directement aux polynômes de Darboux.

2.2 Méthode de Darboux

Au XIXème siécle Darboux introduit dans [44] l'outil suivant appelé désormais polynôme de Darboux.

Définition 8. *Soit $f \in \mathbb{C}[X,Y] \setminus \mathbb{C}$. On dit que f est un* polynôme de Darboux *pour D s'il existe $g \in \mathbb{C}[X,Y]$ tel que :*

$$D(f) = g.f.$$

On dit que g est le cofacteur *de f et on le note* $\mathrm{cof}(f)$.

De nombreuses autres appellations existent pour les polynômes de Darboux. On peut trouver : eigenpolynomials, courbes algébriques invariantes, polynômes spéciaux, séparatrices ...
Le terme eigenpolynomial vient du fait que dans l'égalité $D(f) = g.f$, f joue un rôle similaire à un vecteur propre. La subtilité réside dans le fait que g est un polynôme est non pas un scalaire.
Darboux appelait ces polynômes des solutions particulières. En effet, si l'on considère la courbe $\mathcal{V}(f)$ correspondant aux zéros de f alors $\mathcal{V}(f)$ est une orbite de l'équation 2.1 .
En effet, $D(f) = g.f$ donne $A.\partial_X(f) + B\partial_Y(f) = g.f$ et donc lorsque $f = 0$ le gradient de f est orthogonal au champ de vecteurs. Ainsi, la ligne de niveau $f = 0$ est tangente au champ de vecteur ce qui signifie que $f = 0$ est une orbite.

Remarque 2. Un cofacteur est un polynôme de degré inférieur à $k-1$ lorsque k est le degré de la dérivation.
Un polynôme de Darboux de cofacteur 0 est une intégrale première.
Un polynôme de Darboux de cofacteur $-div(A,B)$ est un facteur intégrant polynomial.

La propriété suivante se déduit directement de la définition. Cette propriété sera fondamentale dans la suite de ce mémoire. Celle-ci provient du fait que nous pouvons voir les cofacteurs comme des dérivées logarithmiques puisque $\mathrm{cof}(f) = D(f)/f$. Voilà pourquoi *un cofacteur transforme un produit en somme.*

Proposition 3. *Soit $f = f_1.f_2$ où f_1, f_2 sont deux polynômes premiers entre eux. On a l'équivalence suivante : f est un polynôme de Darboux pour D si et seulement si f_1 et f_2 sont des polynômes de Darboux pour D. De plus,*

$$\mathrm{cof}(f) = \mathrm{cof}(f_1) + \mathrm{cof}(f_2).$$

Plus généralement, nous avons : $\mathrm{cof}(\prod_i f_i^{\lambda_i}) = \sum_i \lambda_i \mathrm{cof}(f_i)$, *où* $\lambda_i \in \mathbb{C}$.

L'expression $f_i^{\lambda_i}$ correspond à $e^{\lambda_i \ln(f_i)}$, les règles de dérivation usuelles donnent alors : $D(f_i^{\lambda_i}) = \lambda_i D(f_i) f_i^{\lambda_i - 1} = \lambda_i \text{cof}(f_i) f_i^{\lambda_i}$, car f_i est un polynôme de Darboux. Donc par abus de langage nous parlerons du cofacteur de $f_i^{\lambda_i}$ et de $\prod_i f_i^{\lambda_i}$.

Démonstration. Soit f un polynôme tels que $f = f_1.f_2$ avec f_1 et f_2 deux polynômes de Darboux. On a donc $D(f_1) = \text{cof}(f_1).f_1$ et $D(f_2) = \text{cof}(f_2).f_2$. Ainsi,

$$D(f) = D(f_1.f_2) = \text{cof}(f_1).f_1.f_2 + f_1\text{cof}(f_2).f_2 = \big(\text{cof}(f_1) + \text{cof}(f_2)\big)f.$$

Ainsi, f est un polynôme de Darboux et $\text{cof}(f) = \text{cof}(f_1) + \text{cof}(f_2)$.
On montre de même $\text{cof}(\prod_i f_i^{\lambda_i}) = \sum_i \lambda_i \text{cof}(f_i)$.
Réciproquement,

$$D(f_1)f_2 + f_1 D(f_2) = D(f) = \text{cof}(f).f = \text{cof(f)} f_1 f_2.$$

Ainsi, comme f_1 et f_2 sont premiers entre eux nous en déduisons que f_1 divise $D(f_1)$ et f_2 divise $D(f_2)$. □

Remarque 3. Dans la première partie de la preuve nous n'utilisons pas le fait que f_1 et f_2 sont des polynômes. Cette propriété donne alors le résultat suivant : si nous avons deux facteurs intégrant R_1 et R_2 alors le quotient R_1/R_2 est une intégrale première. En effet, le cofacteur associé à R_1 et R_2 est $-div(A, B)$. Donc le cofacteur de R_1/R_2 est $-div(A, B) + div(A, B) = 0$.

G. Darboux a proposé la méthode suivante pour trouver des intégrales premières du type $\prod_i f_i(X, Y)^{\lambda_i}$, avec $f_i(X, Y) \in \mathbb{C}[X, Y]$ et $\lambda_i \in \mathbb{C}$. Nous appellerons ce type d'intégrales premières des *intégrales premières Darbouxiennes.*

Méthode de Darboux
Entrée : Une dérivation D de degré k.
Sortie : Une intégrale première "Darbouxienne" de D non-triviale, si elle existe.

1. Trouver des polynômes de Darboux irréductibles f_i.
2. Résoudre $\sum_i \lambda_i \text{cof}(f_i) = 0$, avec $\lambda_i \in \mathbb{C}$ non tous nuls.
3. Rendre $\mathcal{F}(X, Y) = \prod_i f_i^{\lambda_i}$.

$\mathcal{F}(X, Y)$ est une intégrale première car en appliquant la Proposition 3 nous voyons que $\mathcal{F}$ a un cofacteur nul. De plus, $\mathcal{F}$ est Darbouxienne par construction.

Voyons cette méthode sur un exemple. Considérons l'équation suivante :

$$\dot{X} = X,\ \dot{Y} = -kY, \tag{2.3}$$

Cette équation différentielle correspond à la dérivation : $\mathcal{D}_1 = X\partial_X - kY\partial_Y$. Cette dérivation est de degré 1. Nous pouvons voir que X et Y sont des polynômes de Darboux irréductibles de cofacteurs respectifs 1 et $-k$. Grâce à la méthode de Darboux nous déduisons que $\mathcal{F}(X, Y) = X^k Y$ est une intégrale première.
Cet exemple montre aussi qu'il est impossible de borner le degré d'une intégrale première rationnelle en fonction uniquement du degré de la dérivation. Les coefficients doivent

nécessairement être pris en compte.

Pour la méthode de Darboux deux problèmes se posent :

1. Comment trouver, comment calculer les polynômes de Darboux irréductibles ?
2. Combien de polynômes de Darboux irréductibles sont nécessaires pour trouver une intégrale première Darbouxienne, si elle existe ?

La première question avait été soulevée par Poincaré en 1891 et est encore ouverte à l'heure actuelle. Essayons de voir pourquoi : Nous avons déjà remarqué que les cofacteurs sont des polynômes de degré borné par $k-1$. Si nous savons borner le degré des polynômes de Darboux irréductibles alors en écrivant f et $\mathrm{cof}(f)$ avec des coefficients indéterminés nous pouvons voir $D(f) = \mathrm{cof(f)}.f$ comme un système polynomial quadratique en les coefficients de f et de $\mathrm{cof}(f)$. Ainsi, calculer les polynômes de Darboux de degré borné revient immédiatement à résoudre un système polynomiale quadratique. La difficulté est donc de borner le degré des polynômes de Darboux irréductibles.
En reprenant l'exemple précédent : $\mathcal{D}_1 = X\partial_X - kY\partial_Y$, nous allons voir que ce degré ne peut pas être borné par le degré de la dérivation.

Comme X^kY est une intégrale première, $XY^k + 1$ est aussi une intégrale première. Donc $XY^k + 1$ est un polynôme de Darboux. De plus, $XY^k + 1$ est un polynôme irréductible de degré $k + 1$ alors que $\mathcal{D}_1$ est de degré 1. Donc :

Nous ne pouvons pas borner le degré des polynômes de Darboux irréductibles en fonction du degré de la dérivation.

Nous verrons au Chapitre 6 un moyen plus rapide que celui basé sur la méthode des coefficients indéterminés pour calculer les polynômes de Darboux irréductibles de degré borné.

La réponse à la deuxième question a été donnée par G. Darboux. Nous présentons ce résultat dans la section suivante.

2.3 Théorèmes de Darboux et de Jouanolou

Théorème 6 (Darboux, 1878)**.** *Soit D une dérivation de degré k.*
Si D possède au moins $k(k+1)/2+1$ polynômes de Darboux irréductibles et distincts notés f_i alors D possède une intégrale première Darbouxienne non triviale.
De plus cette intégrale première est du type :

$$\prod_i f_i^{\lambda_i}, \quad \text{où } \lambda_i \in \mathbb{C}.$$

Démonstration. Notons $f_1, \ldots, f_m$ les polynômes de Darboux. Les cofacteurs correspondant, $\mathrm{cof}(f_i)$, appartiennent au $\mathbb{C}$ espace vectoriel des polynômes de degré inférieur à $k-1$. Cet espace vectoriel est de dimension $k(k+1)/2$. Donc si nous avons $k(k+1)/2+1$ polynômes de Darboux nous avons alors $k(k+1)/2+1$ cofacteurs. Ces derniers sont donc linéairement dépendants. Nous avons donc une relation non-triviale $\sum_i \lambda_i \mathrm{cof}(f_i) = 0$, et d'après la Proposition 3, $\prod_i f_i^{\lambda_i}$ est une intégrale première.

Nous avons supposé les f_i irréductibles et distincts afin de déduire une relation non triviale entre les cofacteurs. Cette relation nous permet alors d'obtenir une intégrale première non triviale. □

A présent considérons le cas des intégrales premières rationnelles (ou polynomiales) qui seront au cœur de ce cours.

Définition 9. *On dit que $\mathcal{F}$ est une intégrale première rationnelle (respectivement polynomiale) lorsque $\mathcal{F}$ est une intégrale première et $\mathcal{F} \in \mathbb{C}(X,Y) \setminus \mathbb{C}$ (respectivement $\mathcal{F} \in \mathbb{C}[X,Y] \setminus \mathbb{C}$).*
Le corps (respectivement l'anneau) des intégrales premières rationnelles (respectivement polynomiales) se note $\mathbb{C}(X,Y)^D$ (respectivement $\mathbb{C}[X,Y]^D$).

Une intégrale première Darbouxienne $\prod_i f_i^{\lambda_i}$ avec $\lambda_i \in \mathbb{Z}$ (respectivement $\lambda_i \in \mathbb{N}$) est une intégrale première rationnelle (respectivement polynomiale).

Soit F_1/F_2 une intégrale première rationnelle. Nous pouvons supposer F_1 et F_2 premiers entre eux. Par la suite nous dirons dans ce cas que F_1/F_2 est *réduite*. Nous avons $D(F_1/F_2) = 0$ donc

$$D(F_1).F_2 = F_1.D(F_2).$$

Comme F_1 et F_2 sont premiers entre eux nous en déduisons que F_1 et F_2 sont des polynômes de Darboux. De plus, la Propriété 3 donne le corollaire suivant :

Corollaire 2. *Soit $F_1(X,Y)/F_2(X,Y) \in \mathbb{C}(X,Y) \setminus \mathbb{C}$ une fraction rationnelle réduite. On a l'équivalence suivante :*

$$F_1/F_2 \in \mathbb{C}(X,Y)^D \iff \mathrm{cof}(F_1) = \mathrm{cof}(F_2).$$

Un calcul direct montre que si $\mathrm{cof}(F_1) = \mathrm{cof}(F_2)$ alors pour tout λ, μ dans $\mathbb{C}$ nous avons : $\mathrm{cof}(\lambda F_1 - \mu F_2) = \mathrm{cof}(F_1) = \mathrm{cof}(F_2)$. Ainsi, nous en déduisons : lorsque D possède une intégrale première rationnelle, D possède alors une infinité de polynômes de Darboux de la forme $\lambda F_1 - \mu F_2$. Le théorème suivant nous dit que la réciproque est vraie.
Ce théorème est un prolongement du théorème de Darboux. En effet, nous voyons que si nous augmentons d'une unité la borne du Théorème de Darboux alors nous pouvons certifier l'existence d'une intégrale première rationnelle.

Théorème 7 (Jouanolou, 1979)**.** *Soit D une dérivation de degré k.*
Si D possède au moins $k(k+1)/2 + 2$ polynômes de Darboux irréductibles et distincts notés f_i alors D possède une intégrale première rationnelle non-triviale.
De plus cette intégrale première est du type

$$\prod_i f_i^{\lambda_i}, \quad \text{où } \lambda_i \in \mathbb{Z}.$$

Le théorème de Darboux nous assure l'existence d'une intégrale première de la forme : $\prod_i f_i^{\lambda_i}$ avec $\lambda_i \in \mathbb{C}$. La force du théorème de Jouanolou est de montrer qu'avec un polynôme de Darboux supplémentaire nous pouvons supposer les λ_i entiers.

La méthode de Darboux permet de calculer, si elle existe, une intégrale première rationnelle de D. C'est à dire, nous calculons $k(k+1)/2+2$ polynômes de Darboux puis nous cherchons une relation de dépendance linéaire à coefficients dans $\mathbb{Z}$ pour les cofacteurs. Nous verrons une autre méthode dans le Chapitre 6.

Nous avons énoncé ici les versions les plus simples des théorèmes de Darboux et de Jouanolou. Il est possible de raffiner ces résultats en prenant en compte les singularités du champ de vecteurs. Darboux lui même a donné une amélioration dans ce sens dans [44]. Une notion de multiplicités associée aux polynômes de Darboux a été donnée dans [40] par Christopher, Llibre et Pereira. Il est là encore possible de prendre en compte cette notion de multiplicité dans les théorèmes de Darboux et de Jouanolou. Une synthèse de ces énoncés et preuves se trouve dans le livre de Dumortier, Llibre et Artés [49].

Il existe aussi des énoncés pour le cas des dérivations à n variables, $D = \sum_{i=1}^{n} A_i(X_1,\dots,X_n)\partial_{X_i}$. Dans ce cadre, les définitions précédentes d'intégrales premières, et de polynômes de Darboux se généralisent aisément. Les bornes obtenues dans ce cas ne s'expriment plus en fonction de $k(k+1)/2$, la dimension de l'espace vectoriel des polynômes en deux variables de degré inférieur à k, mais en fonction de $\binom{k+n-1}{n}$ qui est la dimension de l'espace vectoriel des polynômes en n variables de degré inférieur à k. Ainsi, le théorème de Darboux devient :

Si une dérivation de degré k en n variables possède au moins $\binom{k+n-1}{n}+1$ polynômes de Darboux alors il existe une intégrale première Darbouxienne.

Le théorème de Jouanolou devient :

Si une dérivation de degré k en n variables possède au moins $\binom{k+n-1}{n}+n$ polynômes de Darboux alors il existe une intégrale première rationnelle.

Différentes preuves existent. Weil a généralisé dans [147] la preuve donnée dans le cas de deux variables par Singer [139]. Llibre et Zhang ont donné une preuve généralisant l'approche donnée ci-dessous dans [100], ils ont aussi raffiné ce théorème dans [98, 99].
Au Chapitre 6, nous verrons des théorèmes du type Darboux et Jouanolou creux. Les bornes ne seront pas exprimées en fonction du degré de la dérivation mais en fonction de la taille d'un polytope de Newton lié à la dérivation. La borne obtenue sera optimale.
A l'heure actuelle, nous ne savons pas si pour le théorème de Jouanolou la borne $k(k+1)/2+2$ est optimale.

Démonstration du théorème de Jouanolou. La preuve originale se trouve dans [79]. Une preuve à base d'algèbre différentielle se trouve en appendice de l'article de Singer [139]. Une preuve élémentaire de la première partie du théorème se trouve dans le livre de Dumortier, Llibre et Artés [49]. Nous reprenons ici cette preuve élémentaire.

Avec $k(k+1)/2+2$ polynômes de Darboux, notés $\mathcal{F}_j$, nous avons $k(k+1)/2+2$ cofacteurs, notés $\mathrm{cof}(\mathcal{F}_j)$. Donc avec le même argument de dimension que celui utilisé

dans la preuve du théorème de Darboux nous en déduisons l'existence de deux relations de dépendance linéaire sur les cofacteurs non-triviales et indépendantes. Nous avons donc pour $i = 1, 2$:

$$\sum_{j=1}^{k(k+1)/2+2} \lambda_{i,j}\mathrm{cof}(\mathcal{F}_j) = 0,$$

où les $\lambda_{i,j}$ sont des nombres complexes. Nous en déduisons alors les deux intégrales premières Darbouxiennes suivantes :

$$H_i = \prod_{j=1}^{k(k+1)/2+2} \mathcal{F}_j^{\lambda_{i,j}}.$$

On remarque alors que $\log(H_1)$ et $\log(H_2)$ sont aussi deux intégrales premières. D'après la Remarque 1, nous avons donc deux facteurs intégrants $\mathcal{R}_i$ où $i = 1, 2$ qui vérifient :

$$A\mathcal{R}_i = -\partial_Y\big(\log(H_i)\big), \quad \text{et } B\mathcal{R}_i = \partial_X\big(\log(H_i)\big).$$

Ces équations impliquent que les $\mathcal{R}_i$ sont des fractions rationnelles puisque $\partial_Y\big(\log(H_i)\big)$ et $\partial_X\big(\log(H_i)\big)$ le sont.

On considère alors $\mathcal{R}_1/\mathcal{R}_2$, qui est le quotient de deux facteurs intégrants. Cette fraction rationnelle est donc une intégrale première d'après la Remarque 3. □

Nous avons vu que lorsque F_1/F_2 est une intégrale première rationnelle alors F_1 et F_2 sont des polynômes de Darboux. Nous pouvons améliorer ce résultat de la manière suivante :

Proposition 4. *Soit D une dérivation et F_1/F_2 une intégrale première rationnelle réduite. Si G est un polynôme de Darboux irréductible alors il existe $(\lambda : \mu) \in \mathbb{P}^1(\mathbb{C})$ tel que G divise $\lambda F_1 - \mu F_2$.*

Ce résultat est classique, on le trouve dans l'article de Singer [139] et aussi dans le travail de Moulin Ollagnier [110]. Le Lemme 7 du Chapitre 6 entrainera aussi ce résultat. Cet énoncé signifie que tout polynôme de Darboux irréductible est facteur d'une ligne de niveau de l'intégrale première F_1/F_2. Ce résultat est naturel puisque lorsque nous avons une intégrale première rationnelle F_1/F_2 alors les lignes de niveaux ont des équations du type : $\lambda F_1 - \mu F_2$. Comme les polynômes de Darboux sont des équations d'orbites du système différentiel étudié, ceux-ci sont donc facteurs des lignes de niveaux.

Nous pouvons alors donner un résultat "positif" en ce qui concerne le degré des polynômes de Darboux irréductibles. Nous avons vu précédemment que nous ne pouvions pas borner leur degré en fonction du degré de la dérivation, le corollaire suivant dit que cependant une borne existe en fonction de la dérivation.

Corollaire 3. *Soit D une dérivation. Il existe un entier N dépendant de D tel que tous les polynômes de Darboux irréductibles sont de degré inférieur à N.*

Démonstration. Soit nous avons un nombre fini de polynômes de Darboux irréductibles. Dans ce cas le résultat est immédiat. Soit nous avons une infinité de polynômes de Darboux

irréductibles. Dans ce cas nous avons une intégrale première rationnelle d'après le théorème de Jouanolou. Il découle ensuite de la Proposition 4 que le degré des polynômes de Darboux irréductibles est borné par le degré d'une intégrale première. □

Poincaré a noté en 1891 dans [125] que si nous connaissions ce nombre alors "le problème de l'intégration algébrique des équations différentielles serait résolu". Ce que nous appelons de nos jours le *problème de Poincaré* revient à trouver un moyen effectif pour calculer ce nombre N.

Dans la pratique nous souhaitons calculer une intégrale première de degré minimum. Cette volonté est naturelle car nous souhaitons représenter la solution à notre problème de la façon la plus "courte" possible. Les fractions rationnelles possédant cette propriété sont étudiées dans la section suivante.

2.4 Fractions rationnelles indécomposables et clôture algébrique

Définition 10. *Soit $F(X,Y) \in \mathbb{C}(X,Y)$ une fraction rationnelle.*
S'il existe $u(T) \in \mathbb{C}(T)$ et $H(X,Y) \in \mathbb{C}(X,Y)$ tels que $F = u(H)$ et $\deg(u) \geq 2$ *alors on dit que F est* décomposable*, sinon F est dite* indécomposable*.*

Par exemple, la fraction $\dfrac{X^2}{Y^2} + \dfrac{X}{Y} + 3$, est une fraction décomposable (prendre $u(T) = T^2 + T + 3$ et $H(X,Y) = X/Y$.

Remarque 4. Lorsque nous étudions une intégrale première rationnelle nous pouvons toujours supposer celle-ci indécomposable. En effet, si $F = u(H)$ et $D(F) = 0$ alors nous déduisons $u'(H)D(H) = 0$. Comme $\deg(u) \geq 2$ nous avons $u'(H) \neq 0$ et il vient $D(H) = 0$.

Nous avons aussi le résultat suivant qui montre l'importance des fractions rationnelles indécomposables dans l'étude des intégrales premières :

Proposition 5. *Soit D une dérivation possédant une intégrale première rationnelle, nous avons :*

$$\mathbb{C}(X,Y)^D = \mathbb{C}(F),$$

où $F(X,Y) \in \mathbb{C}(X,Y)$ est une intégrale première rationnelle indécomposable.
Autrement dit, toutes intégrales premières rationnelles de D est de la forme $u(F)$ avec $u(T) \in \mathbb{C}(T)$. En particulier, deux intégrales premières rationnelles indécomposables sont égales à une homographie près.
Si on suppose $F(X,Y) \in \mathbb{C}[X,Y] \setminus \mathbb{C}$ alors nous avons : $\mathbb{C}[X,Y]^D = \mathbb{C}[F]$.

Comme nous avons $\deg(u(H)) = \deg(u).\deg(H)$, voir [74], la propriété précédente montre que si nous cherchons une intégrale première rationnelle de degré minimal, alors celle-ci est indécomposable.

Démonstration. Nous reprenons ici, la preuve que nous avons donnée dans [18].
Nous avons : $\mathbb{C} \subset \mathbb{C}(X,Y)^D \subset \mathbb{C}(X,Y)$, d'après le Théorème 39 sur les extensions intermédiaires des extensions de type fini rappelé dans l'appendice A, nous obtenons alors que $\mathbb{C}(X,Y)^D$ est de type fini sur $\mathbb{C}$ et $\mathbb{C}(X,Y)^D = \mathbb{C}(f_1, f_2, f_3)$.
Comme $A\frac{\partial f_i}{\partial X} + B\frac{\partial f_i}{\partial Y} = 0$, nous avons pour tous $i, j = 1, \ldots, 3$:

$$\frac{\partial f_i}{\partial Y}\frac{\partial f_j}{\partial X} - \frac{\partial f_i}{\partial X}\frac{\partial f_j}{\partial Y} = 0.$$

Le critère jacobien, voir Théorème 38 dans l'appendice A, implique alors que f_1, f_2, f_3 sont algébriquement dépendants et donc le degré de transcendance de $\mathbb{C}(X,Y)^D$ sur $\mathbb{C}$ est égal à un. D'après le théorème de Lüroth étendu, voir appendice A, Théorème 42, on obtient $\mathbb{C}(X,Y)^D = \mathbb{C}(F)$, pour $F \in \mathbb{C}(X,Y)$.
A présent on remarque que si F est décomposable, $F = u(H)$, avec $\deg(u) \geq 2$, alors $\mathbb{C}(F) \subsetneq \mathbb{C}(H)$, voir e.g. [74, Corollary 3]. D'après la Remarque 4, H est aussi une intégrale première rationnelle. Donc $H \in \mathbb{C}(X,Y)^D$, et $\mathbb{C}(H) \subset \mathbb{C}(X,Y)^D$. Cela donne : $\mathbb{C}(X,Y)^D = \mathbb{C}(F) \subsetneq \mathbb{C}(H) \subset \mathbb{C}(X,Y)^D$, ce qui est absurde. Donc F est indécomposable, ce qui donne le résultat désiré dans le cas où F est une fraction rationnelle.
A présent supposons $F(X,Y) \in \mathbb{C}[X,Y]$. La stratégie de preuve utilisée ci-dessus reste valable et nous avons $\mathbb{C}(X,Y)^D = \mathbb{C}(F)$. Comme F est un polynôme, il vient $\mathbb{C}[X,Y]^D = \mathbb{C}[F]$. □

Ce genre de résultat reste vrai en n variables dans le cas des fractions rationnelles. C'est à dire $\mathbb{C}(X_1, \ldots, X_n)^D$ est de type fini sur $\mathbb{C}$ d'après le Théorème 39 de l'annexe A. Cependant si nous considérons l'anneau $\mathbb{C}[X_1, \ldots, X_n]^D$ celui-ci n'est pas nécessairement de type fini, voir le résultat de Derksen [45]. Pour plus de précisions voir les travaux de Nowicki [116, Theorem 7.4.1], ou [118].

Dans la preuve ci-dessus, le théorème de Lüroth apparaît de manière naturelle. Nous verrons au Chapitre 5 un algorithme permettant de calculer un générateur donné par le théorème de Lüroth.

Nous avons aussi vu dans cette preuve que les relations algébriques entre les éléments jouent un grand rôle. Continuons dans cette direction et remarquons le résultat suivant :

Proposition 6. *Soit D une dérivation, alors $\mathbb{C}(X,Y)^D$ (respectivement $\mathbb{C}[X,Y]^D$) est algébriquement clos (respectivement intégralement clos) dans $\mathbb{C}(X,Y)$ (respectivement $\mathbb{C}[X,Y]$).*

Démonstration. Soit $F \in \mathbb{C}(X,Y)$ un élément algébrique sur $\mathbb{C}(X,Y)^D$, et soit $\mathcal{P}(T) = a_r T^r + \cdots + a_0 = 0$ le polynôme minimal de F sur $\mathbb{C}(X,Y)^D$.
On a $P(F) = 0$ et donc $D(P(F)) = 0 = P'(F)D(F)$. Comme P est le polynôme minimal de F, nous avons $P'(F) \neq 0$ donc $D(F) = 0$. Ainsi, $F \in \mathbb{C}(X,Y)^D$.
La même preuve est valable pour les polynômes. □

En fait ce genre de situation est caractéristique. Nowicki a montré sous certaines hypothèses que si un anneau est intégralement clos alors c'est le noyau d'une dérivation, voir [116, Theorem A].

A présent, résumons la caractérisation obtenue :

Théorème 8. *Soit $F \in \mathbb{C}(X,Y)$ (respectivement $F \in \mathbb{C}[X,Y]$) une intégrale première d'une dérivation D. Les assertions suivantes sont équivalentes :*

1. *$F = u(H)$ avec $u \in \mathbb{C}(T)$, $H \in \mathbb{C}(X,Y)$ indécomposable, (respectivement $u \in \mathbb{C}[T]$, $H \in \mathbb{C}[X,Y]$ indécomposable).*
2. *$\mathbb{C}(X,Y)^D = \mathbb{C}(H)$, (respectivement $\mathbb{C}[X,Y]^D = \mathbb{C}[H]$).*
3. *$\mathbb{C}(H)$ est la clôture algébrique de $\mathbb{C}(F)$ dans $\mathbb{C}(X,Y)$, (respectivement $\mathbb{C}[H]$ est la clôture entière de $\mathbb{C}[F]$ dans $\mathbb{C}[X,Y]$).*

Démonstration. $1 \Rightarrow 2$, d'après la Proposition 5.
$2 \Rightarrow 3$, comme F est une intégrale première nous avons $F \in \mathbb{C}(X,Y)^D = \mathbb{C}(H)$, donc $\mathbb{C}(F) \subset \mathbb{C}(H)$. Comme $\mathbb{C}(H)$ est algébriquement clos d'après la Proposition 6, nous obtenons le résultat désiré. La preuve fonctionne de même dans le cas des polynômes.
$3 \Rightarrow 1$, comme $\mathbb{C}(F) \subset \mathbb{C}(H)$, il vient $F = u(H)$. Reste à voir, H indécomposable. Supposons le contraire, $H = v(G)$ avec $\deg(v) \geq 2$. Donc $\mathbb{C}(H) \subsetneq \mathbb{C}(G)$. On a alors $F = u(v(G))$ et donc G est algébrique sur $\mathbb{C}(F)$ ce qui amène une contradiction. □

On voit donc qu'en deux variables le calcul de la clôture entière de $\mathbb{C}[F]$ se ramène au calcul de $\mathbb{C}[X,Y]^{D_F}$, où D_F est la dérivation jacobienne associée à F. En n variables, Moulin Ollagnier et ses coauteurs ont montré comment trouver une dérivation D telle que la clôture entière de $\mathbb{C}[F]$ soit du type $\mathbb{C}[X_1,\ldots,X_n]^D$, voir [142]. Dans [110], Moulin Ollagnier a montré que dans le cas de n variables la clôture algébrique de $\mathbb{C}(F)$ est aussi du type $\mathbb{C}(H)$.

2.5 Spectre d'une fraction rationnelle

A présent, rappelons nous que les lignes de niveaux d'une intégrale première donnent les orbites de l'équation différentielle considérée. Nous sommes donc amenés à étudier les polynômes de la forme $\lambda F_1 - \mu F_2$ où F_1/F_2 est une intégrale première rationnelle indécomposable et $(\lambda : \mu) \in \mathbb{P}^1(\mathbb{C})$.
Le théorème suivant caractérise les fractions indécomposables à l'aide des lignes de niveaux. Nous rappelons que le degré $\deg(F_1/F_2)$ est le maximum des degrés $\deg(F_1)$ et $\deg(F_2)$.

Théorème 9 (Bertini-Krull)**.** *Soit $F_1/F_2 \in \mathbb{C}(X,Y)$ une fraction rationnelle. Les propriétés suivantes sont équivalentes :*

1. *F_1/F_2 est indécomposable.*
2. *$\lambda F_1 - \mu F_2$ est irréductible dans $\mathbb{C}[X,Y]$ pour tous $(\lambda : \mu) \in \mathbb{P}^1(\mathbb{C})$ sauf un nombre fini.*
3. *$F_1 - TF_2$ est irréductible dans $\overline{\mathbb{C}(T)}[X,Y]$, où T est une nouvelle variable.*

Afin de donner l'intuition de ce résultat nous allons montrer que lorsque F_1/F_2 est décomposable alors $\lambda F_1 - \mu F_2$ est réductible pour tous les couples $(\lambda : \mu) \in \mathbb{P}^1(\mathbb{C})$. Le lemme obtenu sera une des clefs des algorithmes de décomposition présentés au Chapitre 5.

Lemme 2. *Soient $H = H_1/H_2 \in \mathbb{C}(X,Y)$, $u = u_1/u_2 \in \mathbb{C}(T)$ et on pose $F = u(H)$ où $F = F_1/F_2 \in \mathbb{C}(X,Y)$ est une fraction rationnelle réduite. Soient $\lambda, \mu \in \mathbb{C}$, on a :*

$$\lambda F_1 - \mu F_2 = (\lambda u_1 - \mu u_2)(H).H_2^{\deg u}.$$

En particulier lorsque λ, μ sont tels que $\deg(\lambda u_1 - \mu u_2) = \deg(u)$, nous obtenons

$$\lambda F_1 - \mu F_2 = e(H_1 - t_1 H_2)\cdots(H_1 - t_l H_2)$$

où $e \in \mathbb{C}$, $l = \deg u$ et les $t_i \in \mathbb{C}$ sont les racines du polynôme en une variable $\lambda u_1(T) - \mu u_2(T)$.

Démonstration. On a

$$\frac{\lambda F_1 - \mu F_2}{F_2} = \lambda \frac{u_1(H)}{u_2(H)} - \mu \frac{u_2(H)}{u_2(H)} = \frac{\lambda u_1(H) - \mu u_2(H)}{u_2(H)}.$$

Donc : $(\star)$ $(\lambda F_1 - \mu F_2).u_2(H) = (\lambda u_1 - \mu u_2)(H).F_2$.
De plus,

$$(\star\star)\ \frac{F_1}{F_2} = \frac{u_1(H)}{u_2(H)} = \frac{\left(\sum_{i=0}^{d_1} a_i H_1^i H_2^{d_1-i}\right).H_2^{d_2}}{\left(\sum_{i=0}^{d_2} b_i H_1^i H_2^{d_2-i}\right).H_2^{d_1}},$$

où $u_1(T) = \sum_{i=0}^{d_1} a_i T^i$, $u_2(T) = \sum_{i=0}^{d_2} b_i T^i$.
Ainsi $F_2 = \left(\sum_{i=0}^{d_2} b_i H_1^i H_2^{d_2-i}\right).H_2^{\max(d_1-d_2,0)}$ puisque F est réduite et parce que le degré du terme de droite de l'équation $(\star\star)$ est inférieur ou égal à $\deg(F)$.
Il en découle $F_2 = u_2(H).H_2^{\max(d_1-d_2,0)+d_2} = u_2(H).H_2^{\deg u}$, et grâce à l'équation $(\star)$ on déduit le résultat souhaité. □

Le Théorème 9 et le Lemme 2 se généralisent sans difficultés en n variables.

Le Théorème 9 est dû à Bertini et date de 1882. Pour une présentation complète et historique de ce résultat on peut consulter l'article de Kleiman [83]. Bertini étudiait ce problème d'un point de vue géométrique, il s'intéressait à la réductibilité dans un pinceau de courbes. Poincaré a redémontré ce résultat en 1891 dans [126]. Poincaré montre ce résultat dans le cadre des équations différentielles et ne fait pas référence à Bertini. Comme nous le verrons plus bas, de nombreux auteurs ont ensuite généralisé ce résultat. Pour un preuve complète et moderne on peut consulter le livre de Schinzel [135]. Il semble que le premier énoncé pour un corps algébriquement clos soit dû à Krull en 1937, voir [87]. Voila pourquoi ce théorème est parfois nommé Bertini-Krull. Dans ce mémoire nous appellerons ce résultat ainsi, cela permettra de distinguer ce résultat du théorème de Bertini vu dans le prélude.
Souvent l'histoire de la décomposabilité est présentée en commençant par l'étude de Ritt sur les polynômes en une variable datant de 1922, voir [130]. Nous notons donc au passage que nous pouvons remonter aux travaux de Bertini.

Le théorème de Bertini-Krull nous dit que le nombre de lignes de niveaux réductibles d'une fraction rationnelle indécomposable, ou dont le degré chute, est fini. Il est alors naturel de vouloir borner cette quantité. On introduit alors l'ensemble suivant :

Définition 11. *Soit $F_1/F_2(X,Y) \in \mathbb{C}(X,Y)$ une fraction rationnelle réduite. On appelle spectre de F_1/F_2 l'ensemble suivant :*

$$\sigma(F_1,F_2) := \{(\lambda:\mu) \in \mathbb{P}^1(\mathbb{C}) \quad | \quad \lambda F_1 - \mu F_2 \text{ est réductible dans } \mathbb{C}[X,Y] \\ \text{ou } \deg(\lambda F_1 - \mu F_2) < \deg(F_1/F_2)\}.$$

Le spectre se note $\sigma(F)$ lorsque l'on considère un polynôme $F(X,Y) \in \mathbb{C}[X,Y]$.

Cette définition met en avant l'aspect projectif des phénomènes étudiés. En effet, nous pouvons considérer des équations différentielles dans $\mathbb{P}^2(\mathbb{C})$ et dans ce cas nous travaillons avec des polynômes homogènes et la condition $\deg(\lambda F_1 - \mu F_2) < \deg(F_1/F_2)$ disparaît. En effet, dans le langage projectif ce cas correspond à la situation où la droite à l'infini est un facteur d'un des éléments du pinceau de courbes étudié. Nous avons choisi de présenter ce cours dans un cadre affine. Les résultats sont inchangés avec le cas projectif. Nous y gagnerons parfois un peu en légèreté pour présenter certains résultats. Il est par exemple plus simple de dessiner le polytope de Newton d'un polynôme de $\mathbb{C}[X,Y]$ que celui de son homogénéisé associé. Pour une présentation du lien affine-projectif on peut consulter l'article de Moulin Ollagnier [109].

Remarque 5. Avec la notation précédente, le théorème Bertini-Krull peut s'énoncer ainsi : F_1/F_2 est indécomposable si et seulement si $\sigma(F_1/F_2)$ est fini.

A l'aide des figures 2.1 et 2.2 pages 11-11, nous pouvons voir comment apparaît le spectre sur un dessin. Le champ de vecteurs présenté dans ces figures possède une intégrale première rationnelle. Les lignes de niveaux représentées sont celles d'une intégrale première indécomposable. Le spectre de cette fraction rationnelle est non vide. En effet, nous pouvons constater sur la figure 2.2 qu'une ligne de niveau est réductible car c'est l'union d'une parabole et d'une cubique. Les autres lignes de niveaux représentées sont irréductibles.

A présent, revenons aux polynômes de Darboux. Quel lien existe-t-il entre les polynômes de Darboux et le spectre ? La Proposition 3 et la Proposition 4 répondent à cette question et nous donnent :

Proposition 7. *Soit D une dérivation et F_1/F_2 une intégrale première rationnelle indécomposable.*
Les facteurs irréductibles des polynômes $\lambda F_1 - \mu F_2$ avec $(\lambda:\mu) \in \sigma(F_1,F_2)$ sont les polynômes de Darboux irréductibles de degré inférieur à $\deg(F_1/F_2)$.

Ainsi, lorsque nous étudions le spectre d'une fraction rationnelle F_1/F_2 nous étudions les polynômes de Darboux de degré inférieur à $\deg(F_1/F_2)$ de la dérivation jacobienne associée à F_1/F_2. Nous pouvons d'ailleurs montrer la finitude du spectre en étudiant la finitude des cofacteurs. Cette approche a été utilisée par Moulin Ollagnier dans [110].

Afin de faire apparaître différemment les relations liant le spectre et les intégrales premières rationnelles, nous allons à présent donner une seconde preuve de la Proposition 5. Nous donnons deux preuves car celles-ci utilisent différents aspects des notions étudiées

et mettent en évidence différents phénomènes. En particulier, la preuve donnée ci-dessous met en avant un aspect géométrique alors que la preuve précédente mettait en avant un aspect plus algébrique.

Deuxième preuve de la Proposition 5. Cette preuve repose sur l'utilisation du lemme suivant, voir [139, Lemma A.1]. Ce lemme signifie qu'en un point régulier d'un champ de vecteurs, il passe au plus une seule courbe algébrique.

Lemme 3. *Soient $f_1, f_2 \in \mathbb{C}[X,Y]$ deux polynômes de Darboux d'une dérivation D et soit (x_0, y_0) un point régulier tel que $f_1(x_0, y_0) = f_2(x_0, y_0) = 0$. Dans ce cas, si f_1 est irréductible alors f_1 divise f_2.*

A présent supposons que $\mathbb{C}(X,Y)^D \neq \mathbb{C}$. Il existe alors $F = F_1/F_2 \in \mathbb{C}(X,Y)$ tel que $D(F) = 0$. La Remarque 4 page 19, nous montre que l'on peut supposer F indécomposable. Comme F est indécomposable nous pouvons aussi supposer F_1 et F_2 irréductibles dans $\mathbb{C}[X,Y]$ et tel que $\deg(F_1) = \deg(F_2)$. En effet, une homographie évitant le spectre nous ramène à cette situation.
Dans ce qui suit nous noterons F_1/F_2 une fraction rationnelle de degré minimal parmi toutes les intégrales premières rationnelles $\mathcal{F}_1/\mathcal{F}_2$ telles que $\mathcal{F}_1$ et $\mathcal{F}_2$ sont irréductibles et $\deg(\mathcal{F}_1) = \deg(\mathcal{F}_2)$.
Maintenant, considérons $G = G_1/G_2 \in \mathbb{C}(X,Y)^D$. On pose $G = U(H)$, où $\deg(U) \geq 2$ et H est indécomposable. Comme précédemment, nous pouvons supposer H_1 et H_2 irréductibles et vérifiant $\deg(H_1) = \deg(H_2)$.
Soient $(x_i, y_i) \in \mathbb{C}^2$, où $i = 1, 2$, deux points réguliers tels que $H_i(x_i, y_i) = 0$. Nous appliquons alors le Lemme 3 à H_i et $F_2(x_i, y_i)F_1(X,Y) - F_1(x_i, y_i)F_2(X,Y)$. Il vient alors H_i divise $F_2(x_i, y_i)F_1(X,Y) - F_1(x_i, y_i)F_2(X,Y)$. Comme F_1/F_2 est de degré minimal, nous déduisons l'existence de constantes α_i, β_i telles que $H_i = \alpha_i F_1 - \beta_i F_2$. Donc, il existe $V \in \mathbb{C}(T)$ tel que $H_1/H_2 = V(F_1/F_2)$ et donc $G = U\big(V(F_1/F_2)\big)$. De ce fait $\mathbb{C}(X,Y)^D = \mathbb{C}(F_1/F_2)$. □

2.6 Bornes sur le spectre

A notre connaissance, le spectre a été étudié pour la première fois par Poincaré dans [126]. Poincaré y considère une dérivation D possédant une intégrale première F_1/F_2 et où les points singuliers du système $A(x,y) = B(x,y) = 0$ sont tous distincts. Il appelle les éléments $(\lambda : \mu) \in \sigma(F_1, F_2)$, valeurs remarquables. Dans son article, lui aussi remarquable, Poincaré étudie alors l'intersection des lignes de niveaux d'une intégrale première rationnelle, note que l'équation différentielle étudiée ne comporte que des nœuds rationnels ou des cols, classifie et dénombre les valeurs remarquables, et montre au passage le théorème de Bertini-Krull. La borne sur le cardinal du spectre obtenue par Poincaré est égale au nombre de cols plus 2. Si l'on note k le degré de la dérivation, alors une application directe du théorème de Bezout nous donne $|\sigma(F_1, F_2)| \leq k^2 + 2$.

Une autre borne sur le spectre a été donnée bien plus tard. Cette fois-ci la borne est donnée en fonction du degré de la fraction F_1/F_2. En effet, comme corollaire du théorème de Ruppert nous avons :

Corollaire 4 (Ruppert)**.** *Soit $F_1/F_2 \in \mathbb{C}(X,Y)$ une fraction rationnelle réduite indécomposable de degré d. On a alors :*

$$|\sigma(F_1,F_2)| \leq d^2-1.$$

Démonstration. Dans un premier temps nous remarquons qu'en appliquant une homographie $u(T) \in \mathbb{C}(T)$ à F_1/F_2, nous pouvons supposer que tous éléments du spectre sont du type $(1:\mu)$.
Ensuite, nous considérons le polynôme $F_1 - TF_2$ comme un polynôme de $\mathbb{C}[T][X,Y]$, où T est une nouvelle variable. F_1/F_2 étant indécomposable nous avons, d'après le théorème de Bertini-Krull, $F_1 - TF_2$ irréductible dans $\overline{\mathbb{C}(T)}[X,Y]$. Nous appliquons alors le théorème de Noether à $F_1 - TF_2 \in \mathbb{C}[T][X,Y]$ et nous obtenons des polynômes $\Phi_m(T) \in \mathbb{C}[T]$ non nuls. De plus, ces polynômes s'annulent en $\mu \in \mathbb{C}$ si et seulement si $F_1 - \mu F_2$ est réductible dans $\mathbb{C}[X,Y]$. D'après le théorème de Ruppert, nous pouvons considérer que les polynômes $\Phi_m(T) \in \mathbb{C}[T]$ sont de degré inférieur à d^2-1. Ainsi, $(1:\mu) \in \sigma(F_1,F_2)$ si et seulement si μ est une racine du pgcd des $\Phi_m(T)$. Ce polynôme étant de degré inférieur à d^2-1, nous obtenons le résultat désiré. □

Comme nous utilisons le théorème de Bertini-Krull et le théorème de Noether qui sont valables en n variables, ce résultat reste lui aussi valable en n variables.

L'optimalité de cette borne n'est pas connue à ce jour. On constate que l'optimalité de cette borne est directement liée à l'optimalité de la borne de Ruppert à propos des formes de Noether.

Le résultat de Ruppert a été repris, amélioré et généralisé dans différentes directions. Afin de présenter ces résultats, nous introduisons quelques notations :

Définition 12. *Si $(\lambda:\mu) \in \sigma(F_1,F_2)$ alors on note la factorisation de $\lambda F_1 - \mu F_2$ de la manière suivante :*

$$\lambda F_1 - \mu F_2 = \prod_{i=1}^{N(\lambda:\mu)} f_{(\lambda:\mu),i}^{e_{(\lambda:\mu),i}}.$$

Lorsque $F_1/F_2 \in \mathbb{C}(X,Y)$ est indécomposable, on appelle ordre total de réductibilité la constante suivante :

$$\rho(F_1,F_2) = \sum_{(\lambda:\mu)\in\mathbb{P}^1(\mathbb{C})} \big(N(\lambda:\mu)-1\big),$$

Lorsque nous considérons un polynôme nous adoptons les notations suivantes :

$$\text{Si } \mu \in \sigma(F) \text{ alors } F-\mu = \prod_{i=1}^{N(\mu)} f_{\mu,i}^{e_{\mu,i}}, \text{ et } \rho(F) = \sum_{\mu\in\mathbb{C}} \big(N(\mu)-1\big).$$

L'ordre total de réductibilité est bien défini. En effet, la fraction F_1/F_2 étant indécomposable la somme considérée est finie.

Dans notre contexte nous pouvons voir l'ordre total de réductibilité comme une mesure du nombre de polynômes de Darboux irréductibles de degré inférieur à $\deg(F_1/F_2)$.

A présent, voici les bornes connues à ce jour à propos du spectre et de l'ordre total de réductibilité.
Dans [140], Stein a montré :

$$\rho(F) \leq d-1,$$

où d est le degré du polynôme F.
Lorenzini a montré dans [101] que la borne de Stein était optimale en considérant l'exemple : $F(X,Y) = X + Y\prod_{i=1}^{d-1}(X+i)$. De plus, celui-ci a donné le résultat suivant pour un corps algébriquement clos de caractéristique quelconque :

$$\rho(F) \leq \min_{\mu}\big(\sum_{i}\deg(f_{\mu,i})\big) - 1 \leq d-1.$$

Dans ce même article, Lorenzini donne une borne sur l'ordre total de réductibilité d'une fraction rationnelle F_1/F_2 de degré d :

$$\rho(F_1,F_2) \leq d^2-1.$$

Ensuite, Vistoli donne une borne du même type que la précédente dans le cadre d'un pinceau de courbes sur une variété projective lisse, voir [143]. Dans cet article, le corps est supposé algébriquement clos et de caractéristique 0.
Bodin a montré dans [13] qu'en reprenant la stratégie de preuve de Stein nous obtenions la borne : $\rho(F_1,F_2) \leq d^2+d-1$.
Dans [1], Abhyankar, Heinzer et Sathaye se sont intéressés à l'ordre total de réductibilité sur un corps non nécessairement algébriquement clos.
Dans [17], Bodin, Dèbes et Najib étudient la réductibilité de polynômes du type $F_1+\lambda_2F_2+\cdots+\lambda_sF_s$. Dans [16], les mêmes auteurs étudient le comportement du spectre après spécialisation des coefficients.
Le problème du comportement du spectre après spécialisation sera repris dans le Chapitre 3.
Najib dans [114] utilise le théorème de Bertini pour montrer que les bornes de Stein et Lorenzini restent valables lorsque l'on considère des polynômes en n variables.

Les bornes données ci-dessus sont exprimées en fonction du degré de l'intégrale première. Toutefois, puisque nous considérons des intégrales premières rationnelles, il est naturel de vouloir borner l'ordre total de réductibilité en fonction du degré de la dérivation étudiée. Dans le Chapitre 3 nous verrons comment obtenir de manière naturelle une borne sur le spectre en fonction du degré de la dérivation.
De plus, nous allons voir qu'il existe une relation entre le degré de la dérivation et le degré de l'intégrale première rationnelle. Pour donner cette relation nous avons besoin d'introduire la notion de valeurs remarquables critiques. Cette notion a été introduite par Poincaré dans [126].

Définition 13. *Lorsque dans la factorisation de $\lambda F_1 - \mu F_2$ il y a un exposant $e_{(\lambda:\mu),i}$ strictement supérieur à 1, on dit que $(\lambda:\mu)$ est une valeur remarquable critique et $f_{(\lambda:\mu),i}$ est un facteur remarquable critique.*
Le polynôme

$$R(X,Y) = \prod_{(\lambda:\mu)\in\sigma(F_1,F_2)}\ \prod_{i=1}^{N(\lambda:\mu)} f_{(\lambda,\mu),i}^{e_{(\lambda:\mu),i}-1}$$

s'appelle le facteur remarquable.

Il faut remarquer qu'à l'instar des facteurs $f_{(\lambda:\mu),i}$ le facteur remarquable est défini à une constante multiplicative près.

Théorème 10. *Si F_1/F_2 est une intégrale première indécomposable du champ de vecteurs 2.1, alors R/F_2^2 est un facteur intégrant.*
En notant k le degré du champ de vecteurs nous avons l'égalité :

$$k + \deg(R) = \deg(F_1) + \deg(F_2) - 1.$$

De plus, $R = pgcd\big(\partial_Y(F_1)F_2 - F_1\partial_Y(F_2), \partial_X(F_1)F_2 - F_1\partial_X(F_2)\big)$.

Démonstration. Ce résultat était déjà connu de Poincaré, voir [126]. Une preuve de : R/F_2^2 est un facteur intégrant, se trouve dans [27]. Le résultat sur le degré se trouve dans [55]. Voici une preuve inspirée de [27].
Comme F_1/F_2 est une intégrale première indécomposable nous pouvons supposer F_1 et F_2 irréductibles et premiers entre eux. En effet, une homographie évitant les valeurs remarquables nous ramène à cette situation.
De plus, la Remarque 1 page 12 nous donne l'existence d'un facteur intégrant $\mathcal{R}$ vérifiant :

$$\mathcal{R}A = -\partial_Y(F_1/F_2) \text{ et } \mathcal{R}B = \partial_X(F_1/F_2).$$

Nous en déduisons que $\mathcal{R}$ est de la forme L/F_2^2, où $L(X,Y) \in \mathbb{C}[X,Y]$. Il nous reste donc à montrer que L est le facteur remarquable.
L'équation ci-dessus se réécrit :

$$(\star)\ AL = -\partial_Y(F_1/F_2).F_2^2 \text{ et } BL = \partial_X(F_1/F_2).F_2^2.$$

L'équation $(\star)$ signifie que L est le pgcd de $\partial_Y(F_1)F_2 - F_1\partial_Y(F_2)$ et de $\partial_X(F_1)F_2 - F_1\partial_X(F_2)$. Considérons un facteur irréductible F de ce pgcd et $\varphi(X) \in \overline{\mathbb{C}(X)}$ une racine de F. Nous avons donc $F\big(X,\varphi(X)\big) = 0$, autrement dit F est le polynôme minimal de $\varphi(X)$.
On en déduit que $\partial_Y(F_1)F_2 - F_1\partial_Y(F_2)$ et $\partial_X(F_1)F_2 - F_1\partial_X(F_2)$ s'annule aussi en $\big(X,\varphi(X)\big)$. Ainsi nous obtenons :

$$\partial_X\Big(\frac{F_1}{F_2}\big(X,\varphi(X)\big)\Big)F_2^2\big(X,\varphi(X)\big) = 0.$$

Cela signifie que soit $\varphi(X)$ est racine de F_2 soit $F_1/F_2\big(X,\varphi(X)\big)$ est une fonction constante.
Si $\varphi(X)$ est racine de F_2 alors, comme F est un polynôme minimal, F divise F_2. Puisque F divise aussi $\partial_Y(F_1)F_2 - F_1\partial_Y(F_2)$, on obtient : F divise F_1. Cela est absurde puisque F_1 et F_2 sont premiers entre eux.
Il nous reste donc à étudier le cas où $(F_1/F_2)\big(X,\varphi(X)\big)$ est une fonction constante.
Dans ce cas, il existe une constante c telle que $\big(F_1 - cF_2\big)\big(X,\varphi(X)\big) = 0$. Ainsi, F divise $F_1 - cF_2$.
A présent, nous remarquons que l'égalité suivante :

$$\partial_Y\Big(\frac{F_1}{F_2}\Big) = \partial_Y\Big(\frac{F_1 - cF_2}{F_2}\Big)$$

entraine l'égalité

$$\partial_Y(F_1)F_2 - F_1\partial_Y(F_2) = \partial_Y(F_1 - cF_2)F_2 - (F_1 - cF_2)\partial_Y(F_2).$$

Nous avons le même type d'égalité pour la dérivation par rapport à X.
Nous en déduisons que F est un facteur multiple de $F_1 - cF_2$. La valeur remarquable c est donc une valeur critique. De plus, si F^e divise $F_1 - cF_2$ alors F^{e-1} divise L. En effectuant ce raisonnement pour chaque facteur irréductible de L. Nous obtenons $L = R$.
L'égalité $k + \deg(R) = 2d - 1$ provient à présent de l'étude des degrés dans l'équation $(\star)$. □

Ce théorème montre que connaître le degré d'une intégrale première rationnelle, revient à connaître le degré du facteur remarquable. Donc, la difficulté du problème de la détermination du degré d'une intégrale première rationnelle découle de l'existence de valeurs remarquables critiques.
Le théorème précédent nous montre l'importance des facteurs multiples des éléments du pinceau $\lambda F_1 - \mu F_2$. Dans le Chapitre 3, nous verrons comment améliorer les bornes connues sur l'ordre total de réductibilité en prenant en compte les multiplicités des facteurs.

2.7 Intégrales premières élémentaires, intégrales premières Liouvilliennes

Dans la section précédente nous avons vu que si une dérivation admet une intégrale première rationnelle F_1/F_2 alors elle admet pour facteur intégrant R/F_2^2, où R est le facteur remarquable. Nous allons voir ici que si nous supposons l'existence d'une intégrale première d'un type particulier, par exemple élémentaire ou liouvillienne, alors nous pouvons là encore en déduire une structure particulière pour le facteur intégrant.
Avant d'énoncer ces théorèmes définissons précisément ce qu'est une solution élémentaire. Dans ce qui suit δ désignera indifféremment ∂_X ou ∂_Y.

Définition 14. *Une extension différentielle de corps $\mathbb{E} \supset \mathbb{C}(X,Y)$ est dite élémentaire si nous avons une tour finie d'extensions différentielles : $\mathbb{C}(X,Y) \subset \mathbb{E}_1 \subset \mathbb{E}_2 \subset \cdots \subset \mathbb{E}_n = \mathbb{E}$, telle que :*

1. *soit $\mathbb{E}_{i+1}$ est une extension algébrique de $\mathbb{E}_i$,*
2. *soit $\mathbb{E}_{i+1} = \mathbb{E}_i(f)$, où f vérifie $\delta(f) = \delta(g)/g$ où $g \in \mathbb{E}_i$,*
3. *soit $\mathbb{E}_{i+1} = \mathbb{E}_i(f)$, où f vérifie $\delta(f) = \delta(g)f$ où $g \in \mathbb{E}_i$.*

La deuxième condition signifie que l'on autorise l'utilisation des logarithmes et la troisième condition signifie que l'on autorise l'utilisation de l'exponentielle.
Nous dirons qu'une dérivation possède une intégrale première élémentaire lorsqu'il existe une intégrale première dans une extension élémentaire. Dans [127], Prelle et Singer ont montré le résultat suivant.

Théorème 11 (Prelle-Singer,1983)**.** *Soit D une dérivation. Supposons qu'elle possède une intégrale première élémentaire alors il existe un facteur intégrant de la forme :*

$$\mathcal{R} = \prod_{i=1}^{n} f_i^{q_i},$$

où $q_i \in \mathbb{Q}$ et les f_i sont des polynômes de Darboux pour D.

Cela donne l'algorithme suivant :

Méthode de Prelle-Singer
Entrée : Une dérivation $D = A\partial_X + B\partial_Y$ de degré k.
Sortie : Le facteur intégrant d'une intégrale première élémentaire si elle existe.

1. Trouver des polynômes de Darboux irréductibles f_i.
2. Résoudre le système $\sum_i q_i \text{cof}(f_i) = -div(A, B)$, avec $q_i \in \mathbb{Q}$.
3. Si le système possède une solution alors rendre $\mathcal{F}(X, Y) = \prod_i f_i^{q_i}$.

La difficulté de mise en œuvre de cet algorithme provient de la première étape. En effet, nous avons déjà remarqué que nous ne savons pas comment borner le degré des polynômes de Darboux irréductibles. Donc, nous ne savons pas comment calculer tous les polynômes de Darboux d'une dérivation. Ainsi, en pratique l'algorithme de Prelle-Singer demande à l'utilisateur une borne sur le degré des polynômes de Darboux irréductibles que l'on doit chercher. Cela donne une méthode qui peut rendre "Je ne sais pas". Ce cas peut se produire lorsque la borne donnée par l'utilisateur est trop petite pour l'exemple considéré. Cette méthode a été mise en œuvre en pratique par Man et McCallum, pour plus de détails voir [106, 107].

A présent définissons les solutions liouvilliennes :

Définition 15. *Une extension différentielle de corps $\mathbb{L} \supset \mathbb{C}(X, Y)$ est dite liouvillienne si nous avons une tour finie d'extensions différentielles : $\mathbb{C}(X, Y) \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_n = \mathbb{L}$, telle que :*

1. *soit $\mathbb{L}_{i+1}$ est une extension algébrique de $\mathbb{L}_i$,*
2. *soit $\mathbb{L}_{i+1} = \mathbb{L}_i(f)$, où f vérifie $\delta(f) \in \mathbb{L}_i$,*
3. *soit $\mathbb{L}_{i+1} = \mathbb{L}_i(f)$, où f vérifie $\delta(f)/f \in \mathbb{L}_i$.*

Cela signifie que dans une extension liouvillienne nous nous autorisons l'utilisation des logarithmes, des exponentiels mais aussi des primitives ce qui signifie l'utilisation du symbole $\int$.
Nous dirons qu'une dérivation possède une intégrale première liouvillienne lorsqu'il existe une intégrale première dans une extension liouvillienne. Singer a montré dans [139], le théorème suivant :

Théorème 12 (Singer, 1992)**.** *Soit D une dérivation. Supposons qu'elle possède une intégrale première liouvillienne alors il existe un facteur intégrant de la forme :*

$$\mathcal{R} = e^{\int U dX + V dY},$$

où $U, V \in \mathbb{C}(X, Y)$ et vérifient $\partial_Y U = \partial_X V$.

Démonstration. Nous allons donner ici simplement une idée de la preuve afin d'expliquer la forme du facteur intégrant. Pour une preuve plus complète voir l'article original de

Singer [139] ou le livre de Christopher et Li [39].

Comme D possède une intégrale première alors d'après la Remarque 1, il existe un facteur intégrant $\mathcal{R}$. En considérant son inverse $H = 1/\mathcal{R}$ nous obtenons un facteur intégrant inverse, c'est à dire H vérifie :

$$A\partial_X(H) + B\partial_Y(H) = div(A,B)H.$$

De plus l'intégrale première étant liouvillienne, nous avons une tour d'extension comme dans la Définition 15 et nous remarquons aisément que $H \in \mathbb{L}_n$. On note alors $U_n = \partial_X\big(\ln(H)\big)$, et $V_n = \partial_Y\big(\ln(H)\big)$. On remarque que U_n et V_n appartiennent à $\mathbb{L}_n$ et que nous avons

$$AU_n + BV_n = div(A,B), \quad \text{et } \partial_Y(U_n) = \partial_X(V_n).$$

L'astuce de la preuve est de montrer que nous obtenons les mêmes équations avec $U_{n-1}, V_{n-1} \in \mathbb{L}_{n-1}$. Ainsi de proche en proche nous obtenons l'existence de $U, V \in \mathbb{C}(X,Y)$ tels que :

$$(\star)\ AU + BV = div(A,B), \quad \text{et } \partial_Y(U) = \partial_X(V).$$

La forme $UdX + VdY$ est donc fermée. Sur un voisinage simplement connexe cette forme est exacte et nous avons donc une fonction $H = \int UdX + VdY$ telle que $\partial_X(H) = U$ et $\partial_Y(H) = V$. On pose alors $K = e^H$ et en utilisant $(\star)$ nous obtenons :

$$A\partial_X(K) + B\partial_Y(K) = div(A,B)K.$$

K est donc un facteur intégrant. De plus par construction celui-ci est de la forme $e^{\int UdX+VdY}$ où $U, V \in \mathbb{C}(X,Y)$ vérifient $\partial_Y(U) = \partial_X(V)$. Ce qui est le résultat désiré. □

2.8 Lien avec la factorisation des polynômes

Nous pouvons simplifier la structure du facteur intégrant dans le théorème de Singer. En effet, dans ce théorème nous avons l'intégrale d'une forme fermée et nous avons vu dans le Prélude, Proposition 1, que les formes fermées ont elles aussi une structure particulière. Ainsi, nous en déduisons le résultat suivant dû à Christopher [38].

Proposition 8. *Soit D une dérivation. Supposons qu'elle possède une intégrale première liouvillienne alors il existe une facteur intégrant de la forme :*

$$\mathcal{R} = e^{p/q}\prod_i f_i^{c_i},$$

où f_i, p, $q \in \mathbb{C}[X,Y]$, de plus les f_i et q sont des polynômes de Darboux, et $c_i \in \mathbb{C}$.

Démonstration. D'après le Théorème de Singer, $\mathcal{R} = e^{\int UdX+VdY}$, où $\omega = UdX + VdY$ est une forme fermée. D'après la Proposition 1, nous pouvons écrire cette forme de la manière suivante : $\omega = \sum_i c_i \dfrac{df_i}{f_i} + d\Big(\dfrac{p}{q}\Big)$.
Ainsi, $\int \omega = p/q + \sum_i c_i \ln(f_i)$, ce qui donne la forme souhaitée pour la formule.
Ensuite un calcul direct montre que les f_i et q sont des polynômes de Darboux, voir [38]. □

Remarque 6. À nouveau les polynômes de Darboux jouent un rôle dans l'existence des intégrales premières. Cependant, dans [70], Giné et Llibre montrent que la dérivation $D = \big(-1-X(2X+Y)\big)\partial_X + \big(2X(2X+Y)\big)\partial_Y$ possède une intégrale première liouvillienne et ne possède pas de polynômes de Darboux.
Il faut toutefois noter que si nous nous plaçons dans le cadre homogène alors la droite à l'infini donnera un polynôme de Darboux.
Les mêmes auteurs ont montré dans [71], toujours dans un cadre affine, que lorsque $A(X,Y) = 1$ l'existence d'une intégrale première liouvillienne implique l'existence d'un polynôme de Darboux.

Nous venons de voir que la Proposition 1 permet d'étudier la factorisation des polynômes et le facteur intégrant d'une intégrale première liouvillienne. Cela n'est pas étonnant car dans ces deux cas nous étudions des formes fermées. Dans ce qui suit nous allons voir que le problème de la factorisation et du calcul du facteur intégrant sont intimement liés. Pour cela nous allons définir le facteur intégrant inverse.

Définition 16. *Soit $D = A\partial_X + B\partial_Y$ une dérivation. On appelle facteur intégrant inverse une fonction $\mathcal{I}$ telle que $D(\mathcal{I}) = div(A,B)\mathcal{I}$.*

Un facteur intégrant inverse est simplement l'inverse d'un facteur intégrant.

A présent, supposons que nous cherchions un facteur intégrant inverse polynomial. C'est à dire $\mathcal{I} \in \mathbb{C}[X,Y]$. Dans ce cas nous avons :

$$\begin{aligned} D(\mathcal{I}) = div(A,B)\mathcal{I} \quad &\Longleftrightarrow \quad A\partial_X(\mathcal{I}) + B\partial_Y(\mathcal{I}) = (\partial_X A + \partial_Y B)\mathcal{I} \\ &\Longleftrightarrow \quad \partial_X\Big(\frac{A}{\mathcal{I}}\Big) = \partial_Y\Big(\frac{B}{\mathcal{I}}\Big) \\ &\Longleftrightarrow \quad (A,B) \in \ker \mathcal{R}up(\mathcal{I}) \end{aligned}$$

Ainsi, rechercher un facteur intégrant inverse polynomial $\mathcal{I}$ est le problème "inverse" de la factorisation de $\mathcal{I}$. En effet, dans le cadre de la factorisation, $\mathcal{I}$ est connu et nous cherchons $(A,B) \in \ker \mathcal{R}up(\mathcal{I})$. Lorsque nous cherchons un facteur intégrant inverse polynomial de $D = A\partial_X + B\partial_Y$, A et B sont connus et l'on cherche $\mathcal{I}$ tel que $(A,B) \in \ker \mathcal{R}up(\mathcal{I})$. Donc la relation reste la même, seul le rôle des inconnues changent.

L'utilisation d'un facteur intégrant inverse n'est pas un artifice de calcul permettant d'exhiber un lien avec la factorisation. Lorsqu'un facteur intégrant inverse existe cela permet d'obtenir des théorèmes, comme c'est le cas avec un facteur intégrant, voir par exemple l'article de Chavarriga, Giacomini, Giné et Llibre [27].
Autre propriété remarquable concernant le facteur intégrant inverse : Si un facteur intégrant inverse existe et que le champ de vecteurs possède des cycles limites algébriques alors ces cycles limites sont inclus dans l'ensemble des zéros du facteur intégrant inverse, voir [68].

Pour finir cette section sur les liens entre factorisation et équations différentielles, remarquons une chose. Beaucoup de méthodes "modernes" de factorisation [8, 19, 91, 36, 148] utilisent une méthode de recombinaison basée sur la dérivée logarithmique. Rappelons

cette méthode :
Dans un premier temps à l'aide de la méthode de Newton-Hensel nous obtenons une factorisation du type : $F(X,Y) = \prod_{j=1}^{t} \mathcal{F}_j(X,Y)$, où $\mathcal{F}_j(X,Y) \in \mathbb{K}[[X]][Y]$. Nous pouvons alors écrire les facteurs irréductibles $F_i(X,Y) \in \mathbb{K}[X,Y]$ de F de la manière suivante : $F_i = \prod_{j=1}^{t} \mathcal{F}_j^{e_{i,j}}$, où $e_{i,j} \in \{0,1\}$. Donc, nous avons juste à calculer dans un deuxième temps les exposants $e_{i,j}$ pour en déduire F_i. On calcule ces exposants grâce à la relation suivante :

$$\frac{\partial_Y F_i}{F_i} = \sum_{j=1}^{t} e_{i,j} \frac{\partial_Y \mathcal{F}_j}{\mathcal{F}_j}.$$

Avec cette relation les exposants $e_{i,j}$ deviennent des coefficients, et nous pouvons les calculer en faisant de l'algèbre linéaire. Les exposants $e_{i,j}$ permettent alors de *recombiner* les $\mathcal{F}_j$ pour obtenir F_i.
On remarque que cette approche est celle utilisée dans la méthode de Darboux. En effet, dans la méthode de Darboux on utilise des cofacteurs qui sont des dérivées logarithmiques. Les cofacteurs servent ensuite à construire une intégrale première qui est obtenue en *recombinant* des polynômes de Darboux.
Nous verrons au Chapitre 5 que la décomposition est un problème de factorisation qui peut se résoudre en utilisant la méthode de Darboux. Dans la section suivante nous verrons comment calculer des polynômes de Darboux à l'aide de la factorisation des polynômes.

2.9 La courbe extatique

Les polynômes de Darboux sont au cœur de ce chapitre. Cependant, la seule façon de les calculer est pour l'instant donnée par la définition. Nous allons voir ici une autre méthode basée sur la courbe extatique. Une présentation de la courbe extatique et des résultats donnés ici se trouvent dans les travaux de Pereira et de ses coauteurs [123, 40]. Cependant, il semblerait que la courbe extatique ait été étudiée auparavant par Lagutinskii, pour plus de détails sur ce mathématicien voir [89, 48].
Afin d'introduire la courbe extatique nous allons devoir rappeler certaines notions.

Définition 17. *Une courbe paramètrée* $\big(x(t), y(t)\big) \in \mathbb{C}[[t]]^2$ *et une courbe implicite* $f(X,Y) = 0$ *ont un ordre de contact* ν *en* $(x_0, y_0) = \big(x(0), y(0)\big)$ *lorsque* ν *est le plus grand entier tel que :*

$$f\big(x(t), y(t)\big) = 0 \mod t^{\nu-1}.$$

Lorsque nous considérons un champ de vecteurs du plan l'idée pour découvrir un polynôme de Darboux est de calculer une courbe algébrique possédant un ordre de contact "infini" avec une orbite. Cependant, nous allons voir que si l'ordre de contact est fini et suffisamment grand (une borne sera donnée par la suite) alors cet ordre de contact sera infini.

Ce genre d'idée apparait aussi en théorie du contrôle, voir les travaux de Risler [129] et Gabrielov [60]. Gabrielov a montré dans le cas de n variables que si $\big(x_1(t), \ldots, x_n(t)\big)$ est une orbite d'un système différentiel de degré d et f est un polynôme de degré k tel que $f\big(x_1(t), \ldots, x_n(t)\big) \neq 0$ alors l'ordre de contact entre $f = 0$ et l'orbite est inférieur à $2^{2n-1} \sum_{j=1}^{n} (k + (j-1)(d-1))^{2n}$.
Nous pouvons aussi remarquer que ce type d'idée a aussi été utilisé avec succès dans

le cadre de la factorisation. Dans [82], Kannan, Lenstra et Lovász utilise le paradigme suivant : Si nous connaissons une racine d'un polynôme avec une précision suffisamment grande alors nous pouvons en déduire une racine exacte, c'est à dire un facteur du polynôme.

Afin de calculer l'ordre de contact entre $f(X,Y)=0$ et une orbite $\big(x(t),y(t)\big)$ nous allons calculer le développement de Taylor de $f\big(x(t),y(t)\big)$.
Nous avons $\partial_t\Big(\big(f(x(t),y(t))\big)\Big) = D(f)\big(x(t),y(t)\big)$. Donc le développement de Taylor de $f\big(x(t),y(t)\big)$ en (x_0,y_0) c'est à dire en $t=0$ est :

$$f\big(x(t),y(t)\big)=\sum_{j=0}^{\infty} D^j(f)(x_0,y_0)\frac{t^j}{j!},$$

avec $D^0(f)=f$ et $D^k(f)=D\big(D^{k-1}(f)\big)$.

Cela nous amène à la définition suivante :

Définition 18. *Soit D une dérivation sur $\mathbb{C}[X,Y]$ et (x,y) deux nouvelles variables. On considère l'application linéaire suivante entre $\mathbb{C}(x,y)$ espace vectoriel :*

$$\begin{array}{rcl} E_N : \mathbb{C}(x,y)[X,Y]_{\leq N} & \longrightarrow & \mathbb{C}(x,y)^l \\ g(x,y;X,Y) & \longmapsto & \big(g(x,y;x,y), D(g)(x,y;x,y), D^2(g)(x,y;x,y),\ldots, D^{l-1}(g)(x,y;x,y)\big)\end{array}$$

avec $l=\dim_{\mathbb{C}}\mathbb{C}[X,Y]_{\leq N}$, $D^k(g)=D\big(D^{k-1}(g)\big)$ et D est par abus de notations l'extension de la dérivation D à $\mathbb{C}(x,y)[X,Y]$, c'est à dire

$$D\big(\sum_{i,j} c_{i,j}(x,y)X^iY^j\big)=\sum_{i,j} c_{i,j}(x,y)D(X^iY^j).$$

Le déterminant de cette application linéaire se note $\mathcal{E}_N(D)$ et s'appelle la N-ième courbe extatique.

Nous pouvons remarquer que par définition le noyau de E_N est constitué des polynômes de $\mathbb{C}(x,y)[X,Y]_{\leq N}$ ayant un contact d'ordre supérieur à $l=(N+1)(N+2)/2$ en (x,y) avec une orbite.
Nous remarquons aussi que la courbe extatique est indépendante de la base choisie pour $\mathbb{C}(x,y)[X,Y]_{\leq N}$. De plus ce polynôme est un polynôme en (x,y). Parfois afin d'éviter d'utiliser les nouvelles variables (x,y) et pour alléger les notations la N-ième courbe extatique est définie directement de la manière équivalente suivante. Toutefois le formalisme de la Définition 18 est nécessaire pour comprendre certaines propriétés.

Définition 19. *Soit D une dérivation de $\mathbb{C}[X,Y]$ dans $\mathbb{C}[X,Y]$, la Nième courbe extatique associée à D, $\mathcal{E}_N(D)$, est donnée par le polynôme*

$$\det\begin{pmatrix} v_1 & v_2 & \cdots & v_l \\ D(v_1) & D(v_2) & \cdots & D(v_l) \\ \vdots & \vdots & \cdots & \vdots \\ D^{l-1}(v_1) & D^{l-1}(v_2) & \cdots & D^{l-1}(v_l)\end{pmatrix},$$

où $\mathcal{B} = \{v_1, v_2, \ldots, v_l\}$ est une base de $\mathbb{C}[X,Y]_{\leq N}$, le $\mathbb{C}$-espace vectoriel des polynômes de $\mathbb{C}[X,Y]$ de degré au plus N, $l = (N+1)(N+2)/2$, et $D^k(v_i) = D\big(D^{k-1}(v_i)\big)$.

Une première propriété remarquable de cette courbe est la suivante :

Proposition 9. *Si P est un polynôme de Darboux de D de degré inférieur à N alors P est un facteur de $\mathcal{E}_N(D)$.*

Démonstration. Comme la courbe extatique est indépendante de la base choisie nous pouvons prendre une base $\mathcal{B}$ où $v_1 = P$.
Cela donne :

$$\begin{aligned} D(P) &= g_1 P, \\ D^2(P) &= D(g_1 P) = \big(g_1^2 + D(g_1)\big)P = g_2 P, \\ &\vdots \\ D^{l-1}(P) &= g_{l-1} P, \end{aligned}$$

où g_1, g_2, …, g_{l-1} sont des polynômes.
Donc P est un facteur de la première colonne de $\mathcal{E}_N(D)$. Ainsi, P est un facteur de $\mathcal{E}_N(D)$. □

Remarque 7. La réciproque est fausse. Afin de bien comprendre pourquoi nous devons utiliser le formalisme de la Définition 18.
Considérons la dérivation $D = \partial_X + 3X^2\partial_Y$. Cette dérivation possède une intégrale première polynomiale $P(X,Y) = Y - X^3$. Donc toutes les orbites ont une équation de la forme : $Y = X^3 + c$, avec $c \in \mathbb{C}$. De plus, nous avons :

$$\mathcal{E}_1(D)(x,y) = \begin{vmatrix} 1 & x & y \\ 0 & 1 & 3x^2 \\ 0 & 0 & 6x \end{vmatrix} = 6x.$$

Le polynôme $P(X,Y) = 6X$ n'est pas un polynôme de Darboux.
Que signifie alors $\mathcal{E}_1(D)(x,y) = 6x$?
Cela signifie qu'en tous points de coordonnées $(0,y)$ la première courbe extatique s'annule. Donc en ce point le noyau de E_1 est non trivial. Il existe donc une polynôme de degré 1, donc une droite, ayant un contact d'ordre supérieur à $(N+1)(N+2)/2 = 3$ (car ici N=1) avec l'orbite passant par $(0,y)$. Donc les orbites passant par $(0,y)$ ont un ordre de contact supérieur ou égal à 3 avec une droite. Cela signifie donc simplement que $Y = X^3 + c$ a un point d'inflexion lorsque $X = 0$.
Plus généralement, les facteurs de $\mathcal{E}_N(D)$ qui ne sont pas des polynômes de Darboux correspondent aux lieux des points où une orbite du système a un contact d'ordre supérieur à $(N+1)(N+2)/2$ avec une courbe algébrique de degré inférieur à N.

Un polynôme de Darboux irréductible de degré N est donc un facteur de $\mathcal{E}_N(D)$. Ce facteur peut avoir une multiplicité. Cette multiplicité peut être prise en compte pour améliorer les théorèmes de Darboux et de Jouanolou, voir le livre de Dumortier, Llibre et Artés [49] pour une synthèse de ces résultats. De plus, Christopher, Llibre et Pereira ont

donné différentes interprétations de cette multiplicité dans [40]. En particulier, cette multiplicité est liée à l'existence d'un facteur exponentiel. Nous avons vu que ce type de facteurs jouent un rôle dans la structure du facteur intégrant d'une intégrale première liouvillienne.

La définition de la courbe extatique fait apparaître un déterminant ayant une structure particulière, c'est un Wronskien. Afin de démontrer une propriété fondamentale de la courbe extatique nous rappelons le résultat classique suivant à propos des Wronskiens. Pour une preuve de ce résultat le lecteur peut consulter le livre de Bronstein, [21, Lemma 3.3.5] :

Lemme 4. *Soit* $\mathbb{K}$ *un corps et* D *une dérivation sur* $\mathbb{K}$*. Nous avons l'équivalence suivante :* $g_1, \ldots, g_k \in \mathbb{K}$ *sont linéairement dépendants sur* $\ker D$ *si et seulement si* $W(g_1, \ldots, g_k) = 0$*, où*

$$W(g_1, \ldots, g_k) = \begin{vmatrix} g_1 & g_2 & \cdots & g_k \\ D(g_1) & D(g_2) & \ldots & D(g_k) \\ \vdots & \vdots & \vdots & \vdots \\ D^{k-1}(g_1) & D^{k-1}(g_2) & \ldots & D^{k-1}(g_k) \end{vmatrix}$$

est le Wronskien de $g_1, \ldots, g_k$ *relativement à* D *et* $\ker D$ *est l'ensemble des éléments de* $\mathbb{K}$ *annulant* D*.*

Nous en déduisons la propriété suivante :

Proposition 10. *Les assertions suivantes sont équivalentes :*

1. *D possède un intégrale première rationnelle.*
2. *Il existe un entier N tel que $\mathcal{E}_N(D) = 0$.*

Démonstration. 1. $\Rightarrow$ 2. Soit F_1/F_2 une intégrale première rationnelle de degré N de D. Pour une infinité de $(\lambda : \mu) \in \mathbb{P}^1(\mathbb{C})$ nous avons $\lambda F_1 - \mu F_2$ qui est un polynôme de Darboux de degré N. Donc $\mathcal{E}_N(D)$ a une infinité de facteurs irréductibles distincts donc $\mathcal{E}_N(D) = 0$. Autre façon de voir les choses : $F_1(x,y)F_2(X,Y) - F_2(x,y)F_1(X,Y)$ est dans le noyau de E_N.

2. $\Rightarrow$ 1. On considère $g_1(X,Y), \ldots, g_l(X,Y)$ une base du $\mathbb{C}$ espace vectoriel $\mathbb{C}[X,Y]_{\leq N}$. Cette base est aussi une base du $\mathbb{C}(x,y)[X,Y]$ espace vectoriel $\mathbb{C}(x,y)[X,Y]_{\leq N}$.
Donc $\mathcal{E}_N(D)(x,y) = W(g_1(x,y), \ldots, g_l(x,y))$.
D'après le Lemme 4 appliqué à $\mathbb{K} = \mathbb{C}(x,y)$ et $\tilde{D} = A(x,y)\partial_x + B(x,y)\partial_y$, on déduit :

$$\mathcal{E}_N(D)(x,y) = 0 \iff g_1(x,y), \ldots, g_l(x,y) \text{ sont linéairement dépendants sur } \ker \tilde{D} = \mathbb{C}(x,y)^{\tilde{D}}.$$

Comme $g_1(x,y), \ldots, g_l(x,y)$ sont linéairement indépendants sur $\mathbb{C}$ cela implique $\mathbb{C}(x,y)^{\tilde{D}} \neq \mathbb{C}$. Donc $\tilde{D}$ et donc D ont une intégrale première rationnelle. □

Remarque 8. La preuve précédente nous montre que si D possède une intégrale première rationnelle de degré inférieur à N alors $\mathcal{E}_N(D) = 0$.

Afin d'obtenir un énoncé un peu plus précis que celui de la Proposition 10 nous allons étudier un peu plus en détails les éléments du noyau de E_N.

Proposition 11. *Soit $g_1(x,y;X,Y),\ldots,\ g_r(x,y;X,Y)$ une base de $\ker E_N$ sous forme échelonnée réduite. Nous pouvons alors écrire chaque g_i sous la forme suivante :*

$$g_i(x,y;X,Y)=\sum_{k+l\leq N} c_{k,l}(x,y)X^kY^l,$$

où $c_{k,l}(x,y)\in\mathbb{C}(x,y)^{\tilde{D}}$ et $\tilde{D}=A(x,y)\partial_x+B(x,y)\partial_y$.
De plus, il existe k_0 et l_0 tels que $c_{k_0,l_0}(x,y)\notin\mathbb{C}$.

Cette propriété montre que le calcul du noyau de E_N donne une intégrale première rationnelle de D.

Démonstration. Soit $\{g_1,\ldots,g_r\}$ une base de $\ker E_N$ sous forme échelonnée réduite. On note

$$g_i(x,y;X,Y)=\sum_{(k,l)\in S_i} p_{k,l}(x,y)X^kY^l,$$

où S_i est le support de $g_i(\underline{x},\underline{X})$ comme polynôme de $\mathbb{C}(x,y)[X,Y]$.

Comme $g_i\in\ker E_N$ on en déduit que $W(x^ky^l;(k,l)\in S_i)=0$ et d'après le Lemme 4 nous avons x^ky^l linéairement dépendants sur $\mathbb{C}(x,y)^{\tilde{D}}$, où $(k,l)\in S_i$.
Donc il existe $c_{k,l}(x,y)\in\mathbb{C}(x,y)^{\tilde{D}}$ tel que $\sum_{(k,l)\in S_i}c_{k,l}(x,y)x^ky^l=0$. On en déduit qu'il existe k_0, l_0 tels que $c_{k_0,l_0}(x,y)\notin\mathbb{C}$. De plus, nous avons :

$$\tilde{D}(\sum_{(k,l)\in S_i} c_{k,l}(x,y)x^ky^l)=\sum_{(k,l)\in S_i}\tilde{D}(c_{k,l})x^ky^l+\sum_{(k,l)\in S_i}c_{k,l}(x,y)\tilde{D}(x^ky^l)=\sum_{(k,l)\in S_i}c_{k,l}(x,y)\tilde{D}(x^ky^l)=0.$$

De même, on obtient $\sum_{(k,l)\in S_i}c_{k,l}(x,y)\tilde{D}^j(x^ky^l)=0$.
Il en découle : $\mathcal{G}_i(x,y;X,Y)=\sum_{(k,l)\in S_i}c_{k,l}(x,y)X^kY^l\in\ker E_N$.
Comme $\mathcal{G}_i$ et g_i ont le même support et que nous avons supposé la base $\{g_1,\ldots,g_r\}$ sous forme échelonnée réduite, nous en déduisons : $\mathcal{G}_i=c_{k_1,l_1}(x,y)g_i$, où $c_{k_1,l_1}(x,y)$ est le terme de tête de $\mathcal{G}_i$. Comme $c_{k_1,l_1}(x,y)\in\mathbb{C}(x,y)^{\tilde{D}}$ nous obtenons le résultat souhaité. □

A présent nous pouvons montrer que si l'ordre de contact en un point générique entre une courbe algébrique et une orbite est suffisamment grand alors cet ordre de contact est infini.

Proposition 12. *Soit $(x(t),y(t))$ une orbite passant par (x,y) en $t=0$.*
Soit $P(x,y;X,Y)$ un polynôme de degré total en X, Y inférieur ou égal à N, et $l=(N+1)(N+2)/2$.
Alors nous avons

$$P(x,y;x(t),y(t))=0 \mod t^l \ \Rightarrow\ P(x,y;x(t),y(t))=0.$$

Autrement dit, si en un point générique (x,y) l'ordre de contact entre $P(x,y;X,Y)$ et une orbite est supérieur à $l=(N+1)(N+2)/2$ alors cette orbite annule $P(x,y;X,Y)$.

C'est à dire : Si $\mathcal{E}_N(D)(x,y)=0$ alors toutes les orbites sont inclues dans des courbes algébriques de degré au plus N.

Démonstration. Soit $P(x,y;X,Y)$ tel que $P(x,y;x(t),y(t)) = 0 \mod t^l$.
Le développement de Taylor de $P(x,y;x(t),y(t))$ montre que $P(x,y;X,Y) \in \ker E_N$.
Nous pouvons donc écrire $P(x,y;X,Y)$ sous la forme suivante :

$$P(x,y;X,Y) = \sum_i \lambda_i(x,y) g_i(x,y;X,Y),$$

où $g_i(x,y;X,Y)$ vérifie la Proposition 11.

Nous avons

$$\begin{aligned} g_i(x(t),y(t);X,Y) &= \sum_{k+l\leq N} c_{k,l}(x(t),y(t)) X^k Y^l \\ &= \sum_{k+l\leq N} c_{k,l}(x,y) X^k Y^l, \text{ car } c_{k,l}(x,y) \in \mathbb{C}(x,y)^{\tilde{D}}, \\ &= g_i(x,y;X,Y) \end{aligned}$$

De plus, $g_i(x,y;x,y) = 0$ car $g_i(x,y;X,Y) \in \ker E_N$. Donc

$$0 = g_i(x(t),y(t);x(t),y(t)) = g_i(x,y;x(t),y(t)).$$

D'où $P(x,y;x(t),y(t)) = \sum_i \lambda_i(x,y) g_i(x,y;x(t),y(t)) = 0$.

Le dernier point de la proposition provient du fait que l'existence du polynôme P est équivalent à $\mathcal{E}_N(D)(x,y) = 0$. □

Nous pouvons alors préciser la Proposition 10.

Proposition 13. *Les assertions suivantes sont équivalentes :*

1. *D possède un intégrale première rationnelle indécomposable de degré d.*
2. *Nous avons $\mathcal{E}_d(D) = 0$ et $\mathcal{E}_{d-1}(D) \neq 0$.*

Démonstration. 1. $\Rightarrow$ 2. Nous avons déjà vu, voir Remarque 8, que $\mathcal{E}_d(D) = 0$. Il nous reste à prouver que $\mathcal{E}_{d-1}(D) \neq 0$.
Supposons $\mathcal{E}_{d-1}(D) = 0$ alors d'après la Proposition 12 toutes les orbites sont inclues dans des courbes algébriques de degré au plus $d-1$. Or nous avons une intégrale première indécomposable de degré d, ce qui entraine que nous avons une infinité d'orbites inclues dans des courbe algébriques irréductibles de degré d. Cette situation est impossible donc $\mathcal{E}_{d-1}(D) \neq 0$.

2. $\Rightarrow$ 1. La Proposition 10 nous donne l'existence d'une intégrale première rationnelle F_1/F_2. Il nous reste donc à voir que nous pouvons la supposer indécomposable de degré d. Comme nous pouvons toujours prendre une intégrale première indécomposable, la discussion va donc porter sur le degré de celle-ci.
Si F_1/F_2 est indécomposable et de degré $N < d$ alors d'après la Remarque 8 nous aurions $E_{d-1} = 0$, ce qui est impossible
Si F_1/F_2 est indécomposable et de degré $N > d$ alors toutes les lignes de niveaux $\lambda F_1 - \mu F_2 = 0$ sont réductibles. En effet, $\lambda F_1 - \mu F_2 = 0$ est de degré N mais contient une courbe de degré d d'après la Proposition 12. Cela contredit donc le fait que F_1/F_2 soit indécomposable.
Ainsi F_1/F_2 est indécomposable et de degré d. □

En appliquant à la dérivation jacobienne les propriétés précédentes et la Proposition 7 page 23, nous pouvons montrer à nouveau que le spectre d'une fraction indécomposable est fini. En effet, les polynômes divisant $\lambda F_1 - \mu F_2$ sont des facteurs de $\mathcal{E}_{d-1}(D_{F_1/F_2})$ qui est un polynôme non nul.

Les propriétés ci-dessus donnent une méthode de calcul des polynômes de Darboux et un test d'existence d'intégrales premières rationnelles. A propos de cette méthode nous pouvons lire dans [28] la chose suivante :
"This gives an algorithmic method which allows the computation of invariant algebraic curves and which characterizes the polynomial systems with a rational first integral. We must notice that this method is computationally inefficient."
Dans le Chapitre 6 nous étudierons la complexité de cette méthode et nous verrons que ces propos doivent être modérés.

2.10 Etudes des singularités

Lorsque nous étudions une équation différentielle, les singularités à distance finie, i.e. les points $(x, y) \in \mathbb{C}^2$ tels que $A(x, y) = B(x, y) = 0$, nous fournissent de nombreuses informations sur les solutions. Nous allons donner quelques exemples d'informations pouvant être obtenues. Cette section ne donnera que quelques aspects de l'étude des singularités. Cependant, les résultats présentés donnent un nouveau point de vue sur les objets étudiés dans ce cours et donc permettent de développer une certaine intuition. De plus, dans le Chapitre 6, nous utiliserons le test ci-dessous de non-existence d'intégrales premières rationnelles.

Commençons par un exemple simple :
On considère la dérivation $D_{a,b} = aX\partial_X + bY\partial_Y$, où $a, b \in \mathbb{C}$. Cela correspond au système : $\dot{X} = aX$, $\dot{Y} = bY$.
Les solutions de ce système sont : $X(t) = c_1 e^{at}$ et $Y(t) = c_2 e^{bt}$, où c_1 et c_2 sont des constantes. Ainsi, nous avons $Y(t) = cX(t)^{b/a}$ avec c une constante. Il vient alors que $YX^{-b/a}$ est une intégrale première. Pour avoir une intégrale première rationnelle il faut donc avoir $b/a \in \mathbb{Q}$, autrement dit : si $D_{a,b}$ possède une intégrale première alors a et b sont $\mathbb{Z}$-dépendants.

Dans un cas plus général nous avons un résultat équivalent. Ce résultat montre que si nous avons une intégrale première rationnelle alors les singularités ne peuvent être que des noeuds rationnels ou des cols. Ce résultat est assez intuitif puisque la présence d'un foyer impliquerait des solutions spiralant autour de cette singularité ce qui n'est pas compatible avec des solutions algébriques. Ce résultat était connu de Poincaré, voir [126].

Proposition 14. *Soit $D = A\partial_X + B\partial_Y$ une dérivation. On suppose que D possède une intégrale première rationnelle (respectivement polynomiale).*
Soit (x, y) une singularité. On suppose qu'au point (x, y) la jacobienne de l'application $(X, Y) \mapsto \big(A(X, Y), B(X, Y)\big)$ est diagonalisable de valeurs propres a et b.
Dans ce cas a et b sont $\mathbb{Z}$-dépendants (respectivement $\mathbb{N}$-dépendants).

Démonstration. Comme la matrice jacobienne est diagonalisable, après un changement linéaire de coordonnées nous avons $A(X,Y) = aX + \mathcal{O}\big((X,Y)^2\big)$ et $B(X,Y) = bY + \mathcal{O}\big((X,Y)^2\big)$. Ici, $\mathcal{O}\big((X,Y)^2\big)$ désigne un polynôme dont la valuation est supérieure à 2.
Soit F_1/F_2 une intégrale première de D. On note $F_i(X,Y) = \sum_{k,l} f_{i,k,l} X^k Y^l$ et v_i la valuation de F_i.
Comme F_1/F_2 est une intégrale première rationnelle nous avons :

$$D(F_1)F_2 - F_1 D(F_2) = 0.$$

En considérant la partie de plus bas degré de cette équation nous obtenons :

$$(\star) \qquad \sum_{k+l=v_1, k'+l'=v_2} \big(a(k-k') + b(l-l')\big) f_{1,k,l} f_{2,k',l'} X^{k+k'} Y^{l+l'} = 0.$$

A présent on considère les couples (k_0, l_0) et (k_0', l_0') tels que

$$k_0 = \min\{k \,|\, k+l = v_1, \text{ et } f_{1,k,l} \neq 0\}, \;\; k_0' = \min\{k' \,|\, k'+l' = v_2, \text{ et } f_{2,k',l'} \neq 0\},$$

$$k_0 + l_0 = v_1 \text{ et } k_0' + l_0' = v_2.$$

Le coefficient du monôme $X^{k_0+k_0'} Y^{l_0+l_0'}$ dans l'équation $(\star)$ est

$$\big(a(k_0 - k_0') + b(l_0 - l_0')\big) f_{1,k_0,l_0} f_{2,k_0',l_0'}.$$

Comme nous avons fait en sorte d'avoir f_{1,k_0,l_0} et $f_{2,k_0',l_0'}$ non nuls, il vient alors :

$$a(k_0 - k_0') + b(l_0 - l_0') = 0.$$

Cela signifie : a et b sont $\mathbb{Z}$-dépendants.
Pour le cas où il existe une intégrale première polynomiale, nous avons alors dans le raisonnement précédent $F_2 = 1$ et $k_0' = l_0' = 0$. Donc a et b sont $\mathbb{N}$-dépendants. □

Par la suite nous utiliserons ce résultat afin de fabriquer des exemples de dérivation sans intégrales premières rationnelles. Il existe de nombreux autres résultats et méthodes autour des singularités pour montrer la "non-intégrabilité" d'un champ de vecteurs. Par exemple, des résultats du même type existent pour montrer la non-existence d'intégrale première analytique, voir e.g. [58, Lemma 1]. Pour plus de détails autour de la non-intégrabilité nous renvoyons au livre de Goriely [72]. Le lecteur peut aussi consulter le travail de Moulin Ollagnier, Nowicki et Strelcyn [112], où la méthode de Lagutinski-Levelt est présentée. Cette méthode a été étudiée par les auteurs afin de montrer qu'une certaine dérivation ne possède pas de polynômes de Darboux. Nous reviendrons là dessus dans la section suivante.

Revenons à l'étude de la dérivation $D_{a,b} = aX\partial_X + bY\partial_Y$. Considérons à présent la situation où $a, b \in \mathbb{N}$. Nous avons vu ci-dessus que dans ce cas Y^a/X^b est une intégrale première rationnelle. On remarque alors que le pinceau $\lambda Y^a + \mu X^b$ possède deux facteurs critiques Y^a et X^b. De plus, les exposants de ces facteurs sont les valeurs propres de la matrice jacobienne au point $(0,0)$ associée à la dérivation $D_{a,b}$. Cette situation n'est pas due à la simplicité de notre exemple. Poincaré avait déjà remarqué le lien existant entre les valeurs propres de la jacobienne et les exposants des facteurs remarquables critiques. Nous avons le résultat suivant :

Proposition 15. *Soit D une dérivation possédant une intégrale première rationnelle. Soient f et g deux facteurs remarquables critiques distincts s'annulant en (x,y) et d'exposant respectifs e_f et e_g. Supposons qu'il n'existe pas d'autres facteurs remarquables s'annulant en (x,y).*
Soient a et b les valeurs propres de la jacobienne associée à cette dérivation en (x,y).

1. *Si les courbes $f=0$ et $g=0$ ne se coupent pas de manière transverse alors a et b sont nulles.*

2. *Si les deux courbes $f=0$ et $g=0$ se coupent de manière transverse en (x,y), alors,*
   (a) *soit f et g correspondent à la même valeur remarquable et $a/b=-e_f/e_g$, dans ce cas on dit que (x,y) est un col*
   (b) *soit f et g ne correspondent pas à la même valeur remarquable et $a/b=e_f/e_g$, dans ce cas on dit que (x,y) est un nœud.*

Le vocabulaire "nœud" et "col" correspond à celui connu dans le cas de l'étude d'un système différentiel linéaire. Ce type de résultat est donné par Poincaré dans [126] sans preuves. Une preuve se trouve dans l'article de Ferragut et Llibre [55]. Nous reprenons ici cette preuve :

Démonstration. A l'aide d'une homographie nous pouvons supposer que si les deux facteurs remarquables correspondent à la même valeur remarquable alors cette valeur remarquable est 0. De même, si les deux facteurs remarquables ne correspondent pas à la même valeur remarquable alors la première valeur remarquable est 0 et la seconde ∞. Ainsi, en notant F_1/F_2 l'intégrale première rationnelle de D, $F_1=\prod_{I_1} f_i^{e_i}$ et $F_2=\prod_{I_2} f_i^{e_i}$ où les f_i sont irréductibles, nous avons f et g qui sont des facteurs irréductibles des polynômes F_i. Nous pouvons supposer que nous avons $f=f_1$ et $g=f_2$.
Soit R le facteur remarquable associé, nous avons d'après le Théorème 10, R/F_2^2 qui est un facteur intégrant et comme nous l'avons vu dans la preuve de ce théorème

$$A=-\frac{\partial_Y(F_1/F_2)}{R/F_2^2} \text{ et } B=\frac{\partial_X(F_1/F_2)}{R/F_2^2}.$$

A présent, notons F_1/F_2 sous la forme $\prod_i f_i^{n_i}$ où $n_i\in\mathbb{Z}$, c'est à dire $e_i=|n_i|$. Cela donne

$$A=-\frac{\sum_i\left(n_i\big(\prod_{j\neq i}f_j^{n_j}\big)\partial_Y f_i.f_i^{n_i-1}\right).F_2^2}{R} \text{ et } B=\frac{\sum_i\left(n_i\big(\prod_{j\neq i}f_j^{n_j}\big)\partial_X f_i.f_i^{n_i-1}\right).F_2^2}{R}.$$

Donc

$$A=-\frac{\sum_i\left(n_i\big(\prod_{j\neq i}f_j\big)\partial_Y f_i\right)}{F} \text{ et } B=\frac{\sum_i\left(n_i\big(\prod_{j\neq i}f_j\big)\partial_X f_i\right)}{F},$$

où

$$F=\frac{R}{\prod_j f_j^{e_j-1}}.$$

A présent, notons $\hat{F}_i=\prod_{j\neq i}f_j$ et $\hat{F}_{i,k}=\prod_{j\neq i,k}f_j$. Nous avons alors,

$$A=-\frac{\sum_i\left(n_i\hat{F}_i\partial_Y f_i\right)}{F} \text{ et } B=\frac{\sum_i\left(n_i\hat{F}_i\partial_X f_i\right)}{F}.$$

Comme a et b sont les valeurs propres de la jacobienne associée à D, nous allons à partir des expression précédentes calculer la trace et le déterminant de la jacobienne en (x, y) afin d'en déduire une expression pour a et pour b. Nous avons

$$\partial_X\Big(\frac{-n_i\hat{F}_i\partial_Y f_i}{F}\Big)(x,y) = \frac{-n_i\partial_X\hat{F}_i(x,y)\partial_Y f_i(x,y)}{F(x,y)}$$

nous avons utilisé le fait que $f_1(x, y) = f_2(x, y) = 0$ et donc $\hat{F}_i(x, y) = 0$.
D'autre part, $\partial_X\hat{F}_i(x, y) = \sum_{k\neq i}\hat{F}_{k,i}(x, y)\partial_X f_k(x, y)$. Donc,

$$\partial_X\hat{F}_i(x,y) = \begin{cases} 0, \text{ si } i \neq 1, 2 \\ \hat{F}_{1,2}(x,y)\partial_X f_2(x,y) \text{ si } i = 1 \\ \hat{F}_{1,2}(x,y)\partial_X f_1(x,y) \text{ si } i = 2. \end{cases}$$

Cela donne

$$\partial_X A(x,y) = \frac{-n_1(\hat{F}_{1,2}\partial_X f_2\partial_Y f_1)(x,y) - n_2(\hat{F}_{1,2}\partial_X f_1\partial_Y f_2)(x,y)}{F(x,y)}$$

De même,

$$\partial_Y B(x,y) = \frac{n_1(\hat{F}_{1,2}\partial_Y f_2\partial_X f_1)(x,y) + n_2(\hat{F}_{1,2}\partial_Y f_1\partial_X f_2)(x,y)}{F(x,y)}$$

On en déduit

$$S = \Big(\partial_X A + \partial_Y B\Big)(x,y) = (n_1 - n_2)\frac{\hat{F}_{1,2}(x,y)}{F(x,y)}\Big(\partial_X f_1\partial_Y f_2 - \partial_X f_2\partial_Y f_1\Big)(x,y).$$

Des calculs similaires sur $\partial_Y A(x, y)$ et $\partial_X B(x, y)$ nous donne :

$$P = \Big(\partial_X A.\partial_Y B - \partial_Y A.\partial_X B\Big)(x,y) = -\frac{n_1 n_2\hat{F}^2_{1,2}(x,y)}{F^2(x,y)}(\partial_X f_1\partial_Y f_2 - \partial_Y f_1\partial_X f_2)(x,y).$$

Ainsi, les racines a et b de $\lambda^2 - S\lambda + P = 0$, sont :

$$\frac{(n_1 - n_2) \pm (n_1 + n_2)}{2}(\partial_X f_1\partial_Y f_2 - \partial_Y f_1\partial_X f_2)(x,y)\hat{F}^2_{1,2}(x,y).$$

La première partie du théorème s'en déduit directement puisque f_1 et f_2 ne se coupent pas de manière transverse en (x, y) signifie que $(\partial_X f_1\partial_Y f_2 - \partial_Y f_1\partial_X f_2)(x, y) = 0$.
Lorsque l'intersection est transverse, comme $\hat{F}^2_{1,2}(x, y) \neq 0$ nous en déduisons $P \neq 0$ et donc nous avons deux racines non nulles. Il vient alors

$$\frac{a}{b} = -\frac{n_1}{n_2}.$$

Pour finir nous remarquons que f_1 et f_2 sont des facteurs remarquables associés à la même valeur remarquable si et seulement si $n_1 n_2 > 0$. Cela nous donne donc le résultat souhaité. □

Poincaré utilise ce résultat pour borner le nombre de valeurs remarquables. De façon simplifiée sa démarche est la suivante : le résultat ci-dessus nous dit que pour chaque valeur remarquable donnant lieu à une factorisation avec deux facteurs distincts nous avons au moins un col. Ensuite, l'utilisation d'un résultat dû à Halphen permet de montrer que le nombre de valeurs remarquables donnant une puissance pure dans le pinceau est au plus 2. Il en résulte que le nombre de valeurs remarquables est borné par le nombre de cols plus 2.

Nous venons de voir que les valeurs propres de la jacobienne associée à la dérivation en une singularité sont liées à la multiplicité des facteurs remarquables critiques, et donc au degré de l'intégrale première rationnelle. Dans certains cas l'étude des singularités permet même de borner le degré des polynômes de Darboux en fonction du degré du champ de vecteurs. En effet, Carnicer a montré dans [24] que le degré des polynômes de Darboux ne pouvaient pas être plus grand que $k+2$ lorsque k est le degré du champ de vecteurs et lorsqu'il n'y a pas de singularité dicritique. Nous rappelons qu'une singularité est dicritique lorsqu'il y a une infinité de polynômes de Darboux qui passent par cette singularité. Il existe de nombreux autres résultats allant dans ce sens, nous renvoyons le lecteur intéressé aux travaux de Cerveau et Lins Neto [26], Walcher [144] et Lei et Yang [93].

2.11 Le problème de Poincaré

Nous venons de voir dans la section précédente une condition nécessaire sur les points critiques d'une dérivation possédant une intégrale première rationnelle. Nous allons utiliser ce résultat afin de montrer l'indécidabilité du problème de Poincaré dans le modèle de calcul BSS.

Le problème de Poincaré s'énonce généralement de la façon suivante, voir par exemple l'article de Prelle et Singer [127], ou celui de Schlomiuk [136] ou celui de Walcher [144] :

Soit $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$ une dérivation où $A(X,Y), B(X,Y) \in \mathbb{C}[X,Y]$, donner une méthode permettant de calculer une borne N sur le degré des polynômes de Darboux irréductibles de D.

Nous allons voir que sous cette forme ce problème est mal posé.

En effet, si nous supposons A et B à coefficients dans $\mathbb{C}$ et que nous recherchons un algorithme alors qu'entendons nous par algorithme ?
Nous voulons un modèle de calcul qui accepte de manipuler des nombres réels ou complexes et non pas des approximations à précision finie de ceux-ci.
Le modèle de calcul proposé par Blum, Shub et Smale (BSS) répond à cette attente, voir [12, 11].
De manière simplifiée mais suffisante pour la compréhension de ce qui suit, une machine BSS est une machine qui accepte en entrée des nombres réels, peut faire des opérations arithmétiques $(+, -, \times, \div)$ et des tests $(<, >, \leq, \geq, =)$ de manière exacte. Nous considérons ici une machine fonctionnant sur des nombres réels afin de pouvoir utiliser

les tests d'inégalités. Cela est naturel car nous souhaitons obtenir une borne donc une inégalité. Le corps $\mathbb{C}$ est donc représenté comme le $\mathbb{R}$ espace vectoriel $\mathbb{R} + i\mathbb{R}$.

Avec ce formalisme nous avons le résultat suivant :

Théorème 13. *Il n'existe pas de machine BSS permettant de décider si une dérivation a une intégrale première polynomiale.*

On en déduit :

Corollaire 5. *Il n'existe pas de machine BSS permettant de résoudre le problème de Poincaré.*

Avant de montrer le Théorème 13, montrons pourquoi celui-ci implique le Corollaire 5 : Supposons qu'il existe une machine BSS permettant de résoudre le problème de Poincaré. Dans ce cas, nous pouvons décider si une dérivation a une intégrale première polynomiale. En effet, dans un premier temps nous calculons une borne N sur le degré des polynômes de Darboux irréductibles. Ceci donne automatiquement une borne sur le degré d'une intégrale première polynomiale candidate. Ensuite, nous résolvons le système linéaire : $D(f) = 0$ où f est un polynôme de degré N avec ses coefficients indéterminés. Ce système possède une solution non-triviale si et seulement si D possède une intégrale première polynomiale non-triviale. La démarche proposée peut se modéliser comme une machine BSS. Donc, s'il existe un machine BSS pour résoudre le problème de Poincaré alors il existe une machine BSS pour décider de l'existence d'une intégrale première polynomiale. Il nous reste donc à voir que nous ne pouvons pas décider avec une machine BSS si une dérivation possède ou non une intégrale première polynomiale.

Le Théorème 13 est un théorème d'indécidabilité. Rappelons qu'un ensemble est décidable dans le modèle BSS lorsque sa fonction caractéristique peut être modélisée par une machine BSS. De plus, nous pouvons caractériser les ensembles décidables. Un ensemble $S \subset \mathbb{R}^n$ est décidable si et seulement si S et $\mathbb{R}^n \setminus S$ sont des unions dénombrables d'ensembles semi-algébriques, voir [11, Theorem 1 p. 52].
Cela signifie en particulier que l'ensemble des nombres rationnel $\mathbb{Q}$ est indécidable. Cela n'est pas surprenant car il n'existe pas de méthode générale pour décider si un nombre est irrationnel ou non.

Preuve du Théorème 13. Considérons la dérivation suivante :

$$D_\alpha = Xp(X)\partial_X - \big(\alpha p(X) + p'(X)X\big)Y\partial_Y,$$

où $\alpha \in \mathbb{C}$, $p(x) \in \mathbb{C}[X]$ est un polynôme sans facteurs carrés tel que $p(0) \neq 0$.
Le point $(0;0)$ est un point critique. De plus, la matrice jacobienne associée en ce point est diagonale avec pour valeurs propres $p(0)$ et $-\alpha p(0)$. L'application de la Proposition 14 en $(0;0)$, nous dit que si D_α possède une intégrale première polynomiale alors il existe $n_1, n_2 \in \mathbb{N}$ tels que $n_1 p(0) + n_2\big(-\alpha p(0)\big) = 0$. Comme $p(0) \neq 0$ il vient $\alpha = n_1/n_2$.
D'autre part si $\alpha = n_1/n_2$ avec $n_1, n_2 \in \mathbb{N}$ alors $f(X,Y) = X^{n_1}p(X)Y^{n_2}$ est une intégrale première polynomiale.
De ce qui précède il vient l'équivalence suivante : D_α possède une intégrale première

polynomiale si et seulement si $\alpha \in \mathbb{Q}^+$, où $\mathbb{Q}^+$ est l'ensemble des rationnels positifs.
Donc décider si D_α possède une intégral première polynomiale revient à décider si $\alpha \in \mathbb{Q}^+$.
Or cela est impossible par une machine BSS car $\mathbb{R} \setminus \mathbb{Q}^+$ n'est pas une union dénombrable d'ensembles semi-algébriques. □

Le Corollaire 5 met en avant le fait que dans l'énoncé du problème de Poincaré il faut préciser la manière dont sont représentés les coefficients et comment nous calculons avec eux.
Si nous considérons uniquement des dérivations à coefficients entiers alors le modèle de calcul théorique correspondant est celui des machines de Turing. Dans ce cas le problème de Poincaré est ouvert.

Pour finir, notons que d'autres résultats d'indécidabilité ont été donnés dans le cadre des équations différentielles. Il y a différentes approches pour obtenir ce type de résultat.
La première approche consiste à utiliser l'indécidabilité du dixième problème de Hilbert. La démarche est alors la suivante : on ramène un problème sur des équations différentielles à un problème sur des fonctions élémentaires, ensuite ce problème sur les fonctions élémentaires est ramené à un problème diophantien, voir par exemple le livre de Matiyasevich [108], l'article de Richardson [128] ou bien celui de da Costa et Doria [43]. Dans ce cadre, une fonction élémentaire désigne une fonction obtenue à partir de la composition de fonctions polynômes, logarithmes, exponentielles, et valeur absolue. Ce type d'approche permet par exemple de montrer que nous ne pouvons pas décider si la primitive d'une fonction élémentaire est élémentaire.
Une autre approche est basée sur le fait que nous pouvons simuler l'exécution d'une machine de Turing à l'aide d'une équation différentielle polynomiale, voir par exemple le travail de Graça, Campagnolo et Buescu [73]. Les résultats d'indécidabilité sont alors obtenus en se ramenant au problème de l'arrêt d'une machine de Turing. Par exemple, nous ne pouvons pas décider si une trajectoire va passer par un ensemble fixé.
D'autre type de résultats existent, voir par exemple de livre de Ko [85]. Tous ces résultats utilisent comme modèle de calcul la machine de Turing.

2.12 Situation générique et exemples

Jusqu'à présent nous avons étudié des situations où la dérivation possède une intégrale première rationnelle, élémentaire ou liouvillienne. Que se passe-t-il dans une situation générique ?

Nous identifions l'ensemble des dérivations de degré k avec l'espace $\mathbb{C}^{(k+1)(k+2)}$. Nous pouvons montrer que l'ensemble des dérivations de degré k possédant un polynôme de Darboux de degré l est un ensemble algébrique. Il suffit pour cela d'écrire la définition d'un polynôme de Darboux puis de faire de l'élimination. Pour une preuve détaillée de cela on peut consulter [104]. Ainsi, les dérivations possédant au moins un polynôme de Darboux sont incluses dans une union dénombrable d'ensembles algébriques.
De ce fait, l'ensemble des dérivations possédant un polynôme de Darboux correspond soit à l'espace $\mathbb{C}^{(k+1)(k+2)}$ tout entier soit à un ensemble de mesure nulle. Afin de savoir dans

quelle situation nous sommes il faut savoir s'il existe des dérivations sans polynômes de Darboux. Le théorème suivant de Jouanolou répond à cette question, voir [79].

Théorème 14 (Jouanolou, 1979)**.** *Lorsque $k \geq 2$ la dérivation*

$$D = (Y^k - X^{k+1})\partial_X + (1 - X^k Y)\partial_Y$$

ne possède pas de polynôme de Darboux.

La dérivation du théorème est en général donnée dans le cadre projectif de la manière suivante : $D = Y^k\partial_X + Z^k\partial_Y + X^k\partial_Z$. Cette dérivation et ce théorème ont été très étudiés par Moulin Ollagnier et ses coauteurs, voir par exemple [112, 104]. Pour d'autres exemples explicites on peut consulter [111]. Dans ce contexte, signalons aussi les articles [41, 42] où Coutinho et Menasché Schechter donnent une méthode permettant de reconnaitre si une dérivation possède un polynôme de Darboux. Cette méthode est du type "Las Vegas" c'est à dire peut rendre parfois "Je ne sais pas".

La généralisation à n variables du théorème de Jouanolou donné ci-dessus se trouve dans [153, 102, 103].

De ce théorème nous déduisons que génériquement une dérivation ne possède pas de polynômes de Darboux, donc ne possède pas d'intégrale première rationnelle, ni d'intégrale première élémentaire.

Qu'en est il des intégrales premières liouvilliennes ?
Nous avons vu à la Remarque 6 qu'il est possible d'avoir une intégrale première liouvillienne sans avoir de polynômes de Darboux autres que la droite à l'infini. La stratégie précédente ne permet donc pas de conclure.

Le raisonnement suivant va nous donner la réponse attendue.

Nous devons montrer que génériquement une dérivation n'admet pas de facteurs intégrant exponentiels du type e^p avec $p \in \mathbb{C}[X, Y]$, voir Proposition 8 page 30. Nous devons donc montrer que génériquement l'égalité $D(e^p) = -div(A, B)e^p$ n'est pas vérifiée. Cette égalité se réécrit $D(p) = -div(A, B)$.
Soit k le degré de la dérivation et soit s le degré de p. On note $\text{coef}(F, X^iY^j)$ le coefficient du monôme X^iY^j d'un polynôme F.
En regardant les coefficients des monômes de degré supérieur à $k-1$ nous obtenons :

$$(\star)\ \text{coef}(D(p), X^iY^j) = 0,\ \text{pour } k \leq i + j \leq s + k - 1.$$

Ces équations nous fournissent un système linéaire dont les inconnues sont les coefficients de p et dont les coefficients du système sont donnés en fonction des coefficients de A et de B.
Les équations $(\star)$ impose donc à ce système d'avoir des mineurs nuls.
Ainsi pour s donné, l'ensemble des dérivations possédant un facteur intégrant du type e^p avec p un polynôme de degré s est inclus dans un ensemble algébrique. De ce fait, l'ensemble des dérivations possédant un facteur intégrant du type e^p est inclus dans une union dénombrable d'ensembles algébriques.
Comme précédemment, afin de montrer que cette union d'ensembles algébriques n'est pas

égale à l'espace des dérivations de degré k, il faut trouver une dérivation ne possédant pas de facteur intégrant du type e^p. Les équations de Liénard nous permettent d'exhiber ce type d'exemples comme le montre le résultat suivant, voir l'article de Llibre et Valls [96] ou pour une preuve directe l'article de Chèze et Cluzeau [35].

L'équation de Liénard généralisée est l'équation différentielle suivante :

$$\begin{cases} \dot{X} = Y, \\ \dot{Y} = -g(X) - f(X)\,Y, \end{cases} \tag{2.4}$$

où $f(X), g(X) \in \mathbb{C}[X]$.

A ce système différentielle nous associons la dérivation $D_{\mathcal{L}} = Y\partial_X - \big(f(X)Y + g(X)\big)\partial_Y$.

Cette équation a été introduite par Liénard en 1928, voir [95], dans le cas où $g(X) = cX$ et c est une constant. Cette équation est utilisée pour modéliser des oscillations de systèmes électriques. Cette classe d'équation contient aussi l'équation de van der Pol. En 1942 Levinson et Smith dans [94], ont introduit une description plus générale des oscillation de relaxation ce qui a conduit à l'équation de Liénard généralisée donnée ci-dessus. Depuis, de nombreux travaux ont été effectués sur ce type d'équations (étude des cycles limites, solutions périodiques, ...), voir e.g. [69, 119, 152].

Récemment, dans [97] Llibre et Valls ont classifié les équations de Liénard (i.e. $g(X) = cX$) possédant une intégrale première liouvilienne. Dans [35] nous avons donné une classification des équations de Liénard généralisée possédant une intégrale première liouvilienne dans le cas où $\deg(g) \leq \deg(f)$. De plus, la preuve donnée dans [35] est plus directe que celle donnée dans [97]. Voici le résultat :

Proposition 16. *Soit $D_{\mathcal{L}} = Y\partial_X - \big(f(X)Y + g(X)\big)\partial_Y$ où $f(X)$ et $g(X)$ sont deux polynômes de $\mathbb{C}[X]$.*
On suppose $\deg(g) \leq \deg(f)$, $f(X) \neq 0$, $g(X) \neq 0$, et $g(X) \neq \alpha\, f(X)$ pour $\alpha \in \mathbb{C}$.
Dans ce cas, la dérivation $D_{\mathcal{L}}$ ne possède pas d'intégrale première liouvilienne.

Cela donne une classification des intégrale premières liouviliennes de l'équation de Liénard généralisée lorsque $\deg(g) \leq \deg(f)$ puisque nous avons :

(i) si $f(X) = 0$, alors (2.4) admet comme intégrale première

$$H(X, Y) = Y^2 + 2\int g(X)\,\mathrm{d}X,$$

(ii) si $g(X) = 0$, alors (2.4) admet comme intégrale première

$$H(X, Y) = Y + \int f(X)\,\mathrm{d}X$$

(iii) si $g(X) = \alpha\, f(X)$, où $\alpha \in \mathbb{C}$, alors (2.4) admet comme intégrale première (voir [120])

$$H(X, X) = Y + \int f(X)\,\mathrm{d}X - \alpha\,\log(Y + \alpha).$$

Pour montrer la Proposition 16 on s'appuie sur le résultat suivant d'Odani [119].

Theorem 15. *Soit* $D_{\mathcal{L}} = Y\partial_X - \big(f(X)Y + g(X)\big)\partial_Y$ *où* $f(X)$ *et* $g(X)$ *sont deux polynômes de* $\mathbb{C}[X]$.
On suppose $\deg(g) \leq \deg(f)$, $f(X) \neq 0$, $g(X) \neq 0$, *et* $g(X) \neq \alpha\, f(X)$ *pour* $\alpha \in \mathbb{C}$.
Dans ce cas, la dérivation $D_{\mathcal{L}}$ *ne possède pas de polynômes de Darboux.*

Démonstration de la Proposition 16. D'après le Théorème 15, nous savons que $D_{\mathcal{L}}$ ne possède pas de polynôme de Darboux. Par conséquent, le Théorème de Singer et la Proposition 8 impliquent que si $D_{\mathcal{L}}$ possède une intégrale première liouvilienne, alors il existe un polynôme $P \in \mathbb{C}[x,y]$ tel que $D_{\mathcal{L}}(e^P) = f(x)\, e^P$, ceci étant équivalent à $\mathcal{D}_L(P) = f(x)$. Cette dernière égalité donne :

$$(\star) \qquad Y\,\partial_X\big(P(X,Y)\big) - \big(g(X) + f(X)\,Y\big)\,\partial_Y\big(P(X,Y)\big) = f(X).$$

La stratégie utilisée dans ce qui suit est proche de celle développée par Odani pour démontrer le Théorème 15. On pose $P(X,Y) = \sum_{i=0}^{n} P_i(X)\,Y^i$, où $P_n(X) \neq 0$ et $P_i'(X) = \partial_X(P_i(X))$.
Si $n = 0$, alors $(\star)$ donne $Y\,P_0'(X) = f(X)$, cela est impossible puisque $f(X) \neq 0$.
Si $n \geq 1$, alors en identifiant les coefficients en Y^i, où $i = 0, \ldots, n$, dans le membre de gauche de $(\star)$, nous obtenons le système suivant d'équations pour les P_i.

$$(\star\star) \qquad \left\{ \begin{array}{rcl} P_n'(X) & = & 0, \\ P_{n-1}'(X) & = & n\,f(X)\,P_n(X), \\ P_{n-2}'(X) & = & (n-1)\,f(X)\,P_{n-1}(X) + n\,g(X)\,P_n(X), \\ \vdots & & \\ P_{n-j}'(X) & = & (n-j+1)\,f(X)\,P_{n-j+1}(X) + (n-j+2)\,g(X)\,P_{n-j+2}(X), \\ \vdots & & \\ P_1'(X) & = & 2\,f(X)\,P_2(X) + 3\,g(X)\,P_3(X), \\ P_0'(X) & = & f(X)\,P_1(X) + 2\,g(X)\,P_2(X), \\ 0 & = & f(X) + g(x)\,P_1(X). \end{array} \right.$$

Si $n = 1$, alors l'équation $P_1'(X) = 0$ implique $P_1(x) = \beta$, où β est une constante non-nulle. Or la dernière équation de $(\star\star)$ donne $f(X) = -\beta\,g(X)$ et cela contredit les hypothèses de la proposition.

A présent nous supposons $n \geq 2$ et nous allons calculer les degrés des polynômes P_i solutions du système $(\star\star)$.
La première équation de $(\star\star)$, $P_n'(x) = 0$, implique que $P_n(x)$ est une constante non-nulle. Donc l'équation $P_{n-1}'(X) = n\,f(X)\,P_n(X)$, entraine P_{n-1} est un polynôme de degré $\deg(f) + 1$. Comme $\deg(g) \leq \deg(f)$, l'équation suivante donnant P_{n-2}' en fonction de f, g, P_n et P_{n-1} implique que $\deg(P_{n-2}) = 2\,(\deg(f) + 1)$. Par récurrence, on obtient :

$$\deg(P_{n-j}) = j\,(\deg(f) + 1), \quad j = 0, \ldots, n.$$

En particulier, nous avons $\deg(P_1) = (n-1)\,(\deg(f) + 1)$.
Pour finir nous étudions la dernière équation $f(X) = -g(X)P_1(X)$ de $(\star\star)$. Nous comparons les degrés de chacun des deux membres, et nous obtenons

$$\deg(f) = \deg(g) + (n-1)\,(\deg(f) + 1)$$

ce qui est impossible puisque $n \geq 2$. En conclusion, nous avons montré que sous les hypothèses de la proposition l'équation $(\star)$ n'a pas de solution polynomiale. Cela signifie qu'il n'existe pas de polynômes $P \in \mathbb{C}[X, Y]$ tels que $D_{\mathcal{L}}(e^P) = f(x)e^P$, donc en conclusion $D_{\mathcal{L}}$ ne possède pas d'intégrale première liouvilienne. □

Deuxième partie

Précisons certains points

Chapitre 3

Étude du spectre

Dans le Chapitre 2 nous avons effectué une présentation générale de différents objets et des liens qui les unissent. Nous avons défini la décomposition, le spectre et l'ordre total de réductibilité d'une fraction rationnelle dans $\mathbb{C}(X, Y)$. Ces notions s'étendent sans difficulté aux fractions rationnelles de $\mathbb{K}(X_1, \ldots, X_n)$ où $\mathbb{K}$ est un corps commutatif.
Dans tout ce qui suit les fractions rationnelles seront toujours considérées comme réduites, c'est à dire le numérateur et le dénominateur sont premiers entre eux.

Dans un cadre général la décomposition se définit ainsi :

Définition 20. *Soit $F_1/F_2 \in \mathbb{K}(X_1, \ldots, X_n)$ une fraction rationnelle.*
S'il existe $u(T) \in \mathbb{K}(T)$ et $H(X_1, \ldots, X_n) \in \mathbb{K}(X_1, \ldots, X_n)$ tels que $F_1/F_2 = u(H)$ et $\deg(u) \geq 2$ *alors on dit que F_1/F_2 est* décomposable*, sinon F_1/F_2 est dite* indécomposable*.*

Le spectre étant une notion géométrique nous considérons la réductibilité dans $\overline{\mathbb{K}}[X_1, \ldots, X_n]$ où $\overline{\mathbb{K}}$ est une clôture algébrique de $\mathbb{K}$.

Définition 21. *Soit $F_1/F_2(X_1, \ldots, X_n) \in \mathbb{K}(X_1, \ldots, X_n)$ une fraction rationnelle. On appelle spectre de F_1/F_2 l'ensemble suivant :*

$$\sigma(F_1, F_2) := \{(\lambda : \mu) \in \mathbb{P}^1(\overline{\mathbb{K}}) \quad | \quad \lambda F_1 - \mu F_2 \text{ est réductible dans } \overline{\mathbb{K}}[X_1, \ldots, X_n] \text{ ou } \deg(\lambda F_1 - \mu F_2) < \deg(F_1/F_2)\}.$$

Le spectre se note $\sigma(F)$ lorsque l'on considère un polynôme $F(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n]$.

Nous pouvons remarquer que si nous considérons les polynômes homogènes $F_i^\sharp \in \overline{\mathbb{K}}[X_0, X_1, \ldots, X_n]$ associés aux polynômes F_i alors le spectre est l'ensemble des $(\lambda : \mu)$ tels que $\lambda F_1^\sharp - \mu F_2^\sharp$ est réductible dans $\overline{\mathbb{K}}[X_0, X_1, \ldots, X_n]$.

L'ordre total de réductibilité se généralise aussi sans peine :

Définition 22. *Si $(\lambda : \mu) \in \sigma(F_1, F_2)$ alors on note la factorisation de $\lambda F_1 - \mu F_2$ dans $\overline{\mathbb{K}}[X_1, \ldots, X_n]$ de la manière suivante :*

$$\lambda F_1 - \mu F_2 = \prod_{i=1}^{N(\lambda:\mu)} f_{(\lambda:\mu),i}^{e_{(\lambda:\mu),i}}.$$

Lorsque $F_1/F_2 \in \mathbb{K}(X_1, \ldots, X_n)$ est indécomposable, on appelle ordre total de réductibilité la constante suivante :

$$\rho(F_1, F_2) = \sum_{(\lambda:\mu)\in\mathbb{P}^1(\overline{\mathbb{K}})} \big(N(\lambda : \mu) - 1\big),$$

Dans ce chapitre, nous allons étudier le spectre et l'ordre total de réductibilité dans ce cadre général. Ce chapitre est une synthèse des articles [23], [22] et [34]. Nous verrons comment le spectre se comporte après l'application d'un morphisme sur les coefficients des F_i. Ensuite, nous améliorerons les bornes connues sur l'ordre total de réductibilité en prenant en compte la multiplicité des facteurs. Enfin nous montrerons comment le théorème de Jouanolou, voir Théorème 7 page 16, permet d'obtenir sans difficultés une nouvelle borne sur le spectre.
Dans ce chapitre nous étudierons le spectre d'une fraction rationnelle en deux variables car comme nous le rappellerons le cas général avec plusieurs variables peut toujours s'y ramener.

3.1 Une méthode simple et effective

Afin d'étudier le spectre nous introduisons le polynôme suivant :

Définition 23. *Soient $F_1, F_2 \in \mathbb{K}[X, Y]$ deux polynômes premiers entre eux tels que $\max\big(\deg(F_1), \deg(F_2)\big) = d$.*
Soient U et V deux nouvelles variables.
On considère le polynôme $UF_1(X, Y) - VF_2(X, Y) \in \mathbb{K}[U, V][X, Y]$, comme un polynôme en les variables X et Y, et on note $\Phi_1(U, V), \ldots, \Phi_M(U, V)$ les formes de Noether associées à ce polynôme.
Le polynôme $Spect_{F_1,F_2}(U, V)$ est le pgcd des polynômes $\Phi_i(U, V)$.

Le polynôme $Spect_{F_1,F_2}$ possède la propriété fondamentale suivante :

Proposition 17. *Le polynôme $Spect_{F_1,F_2}(U, V) \in \mathbb{K}[U, V]$ est homogène et vérifie :*

$$(\lambda : \mu) \in \sigma(F_1, F_2) \iff Spect_{F_1,F_2}(\lambda, \mu) = 0.$$

Cette propriété découle de la définition des formes de Noether et de celle du spectre.

Ainsi, l'étude du spectre peut se ramener à l'étude de ce polynôme.

En étudiant une matrice du type Sylvester et ses mineurs, nous obtenons la propriété suivante qui va nous permettre d'étudier le comportement du spectre après spécialisation. Dans ce qui suit lorsque nous avons un morphisme d'anneaux $\sigma : A \to \mathbb{L}$, on notera aussi σ l'extension de ce morphisme à $A[U, V]$.

Proposition 18. *Soient A un anneau factoriel, et $f_1, \ldots, f_n$, $n \geq 2$ polynômes homogènes non nuls dans $A[U, V]$. Soit $\sigma : A \to \mathbb{L}$ un morphisme d'anneaux où $\mathbb{L}$ est un corps. On pose $g := \gcd(f_1, \ldots, f_n) \in A[U, V]$ et $\alpha \in A$ est le terme de tête de g. Dans ce cas nous avons :*

Il existe un ensemble fini d'éléments $(c_i)_{i\in I}$ de A tels que : s'il existe $i \in I$ tel que $\sigma(c_i) \neq 0$ alors

$$\sigma(\gcd(f_1, \ldots, f_n)) = \sigma(\alpha)\gcd(\sigma(f_1), \ldots, \sigma(f_n)) \in \mathbb{L}[U, V].$$

Appliqué aux formes de Noether, cela donne le résultat suivant montrant comment se comporte le spectre après une spécialisation :

Proposition 19. *Soient $(F_1/F_2)(X, Y) \in A(X, Y)$, où A est un sous-anneau du corps $\mathbb{K}$ et $\sigma : A \to \mathbb{L}$ un morphisme d'anneaux.*
Alors, il existe un élément non nul c de A tel que si $\sigma(c) \neq 0$ alors

$$\sigma(Spect_{F_1,F_2}) = Spect_{\sigma(F_1),\sigma(F_2)}.$$

La matrice de Ruppert nous fournit une version effective du théorème de Noether, voir Chapitre 1. Comme nous souhaitons donner des bornes effectives, nous allons à partir de maintenant ne plus considérer que les formes de Noether données par la matrice de Ruppert.

Dans la suite nous noterons $Spect_{F_1,F_2}$ le polynôme obtenu en considérant les formes de Noether données par la matrice de Ruppert.

Nous avons une borne sur la hauteur et le degré des formes de Noether, voir Théorème 2 au Chapitre 1. De plus, les éléments c_i sont explicites car ce sont les mineurs d'une matrice de type Sylvester. Ainsi, lorsque nous considérons le morphisme, $\sigma : \mathbb{Z} \to \mathbb{F}_p$ la réduction modulo un nombre premier p, ou $\sigma : \mathbb{K}[Z_1, \ldots, Z_s] \to \mathbb{K}$ un morphisme d'évaluation nous pouvons alors donner des bornes certifiant que $\sigma(c) \neq 0$, voir [23].

Théorème 16. *Soient F_1, F_2 deux polynômes de $\mathbb{Z}[X_1, \ldots, X_n]$ premiers entre eux. Soient $d = \deg(F_1/F_2) = \max(\deg(F_1), \deg(F_2))$. Pour tout premier $p > \mathcal{B}$ où*

$$\mathcal{B} = 2^{2(d^2-1)^2} d^{2d^2-2}(d^2-1)^{d^2-1}\mathcal{H}^{2d}$$

et

$$\mathcal{H} = d^{3d^2-3}\left(\binom{n+d}{n}2^d\right)^{d^2-1}\binom{d^2-1}{\lfloor (d^2-1)/2 \rfloor}\max\left(\|f\|_\infty), \|g\|_\infty)\right)^{d^2-1}.$$

nous avons

$$Spect_{\overline{f}^p,\overline{g}^p} = \kappa.\overline{Spect_{f,g}}^p$$

dans l'anneau $\mathbb{F}_p[U, V]$ et $0 \neq \kappa \in \mathbb{F}_p$.

Nous pouvons voir ce résultat comme une sorte de théorème d'Ostrowski pour le spectre, voir Théorème 1 du Chapitre 1. A présent voyons une autre application lorsque $A = \mathbb{K}[Z_1, \ldots, Z_s]$ et σ et un morphisme d'évaluation.

Théorème 17. *Soient F_1, F_2 deux polynômes de $\mathbb{K}[Z_1, \ldots, Z_s][X_1, \ldots, X_n]$ tel que $\deg_{\underline{Z}}(F_1) \leq k$, $\deg_{\underline{Z}}(F_2) \leq k$, $\deg_{\underline{X}}(F_1) \leq d$ et $\deg_{\underline{X}}(F_2) \leq d$. Soit $\underline{z} := (z_1, \ldots, z_s) \in \mathbb{K}^s$, on note $ev_{\underline{z}}$ le morphisme $\mathbb{K}[Z_1, \ldots, Z_s] \to \mathbb{K}$ qui envoie Z_i sur z_i pour $i = 1, \ldots, s$. Il existe un nombre fini de polynômes dans $\mathbb{K}[\underline{Z}]$, que nous notons $(q_i)_{i\in I}$, de degré inférieur à $2(d^2-1)^2k$ et vérifiant la propriété : si les $ev_{\underline{z}}(q_i) \in \mathbb{K}$ ne sont pas tous nuls alors*

$$ev_{\underline{z}}(Spect_{f,g}) = \kappa.Spect_{ev_{\underline{z}}(f),ev_{\underline{z}}(g)}$$

où $0 \neq \kappa \in \mathbb{K}$.

Dans ce qui précède nous avons étudié les coefficients du polynôme $Spect_{F_1,F_2}$. A présent regardons les racines de $Spect_{F_1,F_2}$. Plus précisément, étudions la multiplicité de ses racines. Pour cela, nous allons devoir étudier en détails le noyau de la matrice de Ruppert puisque nous avons le résultat suivant :

Proposition 20. *Soit F_1 et F_2 deux polynômes de même degré. La matrice de Ruppert vérifie les propriétés suivantes :*

1. *Soient U et V deux variables nous avons :*
$$\mathcal{R}up(UF_1 - VF_2) = U\mathcal{R}up(F_1) - V\mathcal{R}up(F_2).$$
2. *Soit $(\lambda : \mu) \in \sigma(F_1, F_2)$, nous avons :*
$$\dim_{\mathbb{K}} \ker\big(\lambda\mathcal{R}up(F_1) - \mu\mathcal{R}up(F_2)\big) \leq mult_{(\lambda:\mu)}Spect_{F_1,F_2}.$$

La première propriété est immédiate à partir de la définition de la matrice de Ruppert. De plus, cette propriété montre que le polynôme $Spect_{F_1,F_2}(U, V)$ et le dernier facteur invariant de $U\mathcal{R}up(F_1) - V\mathcal{R}up(F_2)$ sont directement liés.
La seconde propriété peut être vue comme la propriété bien connue sur le polynôme caractéristique et la dimension des sous-espaces propres.

Nous sommes donc amenés à étudier la dimension du noyau de la matrice de Ruppert.

3.2 Dimension du noyau de la matrice de Ruppert

Dans cette section, le corps $\mathbb{K}$ est supposé algébriquement clos et de caractéristique nulle.
Dans cette section nous allons expliciter la dimension du noyau de la matrice de Ruppert d'un polynôme $f(X, Y) \in \mathbb{K}[X, Y]$ de degré d. Dans la section suivante nous appliquerons le résultat obtenu à l'étude du spectre. Cette section et la suivante est une synthèse de l'article [22].

Comme nous l'avons vu dans le prélude la dimension du noyau de la matrice de Ruppert d'un polynôme $f(X, Y) \in \mathbb{K}[X, Y]$ est liée à la dimension de $\mathcal{H}^1\big(\overline{\mathbb{K}}^2 \setminus \mathcal{V}(f)\big)$. Grace à ce lien nous allons pouvoir donner une formule explicite pour la dimension de ce noyau.

Par définition $\mathcal{H}^1\big(\overline{\mathbb{K}}^2 \setminus \mathcal{V}(f)\big)$ est le quotient des formes fermées de $\Omega_{\mathbb{K}[X,Y]_f/\mathbb{K}}$ par les formes exactes. Nous avons rappelé dans le prélude qu'une base de cet espace vectoriel est donné par $df_1/f_1, \ldots, df_r/f_r$ où les f_i sont les facteurs absolument irréductibles de f. Comme
$$\frac{df_i}{f_i} = \frac{\partial_X f_i}{f_i}dX + \frac{\partial_Y f_i}{f_i}dY = \frac{\partial_X(f_i).f}{f_i.f}dX + \frac{\partial_Y(f_i).f}{f_i.f}dY,$$
nous remarquons que lorsque nous considérons des formes fermées nous pouvons prendre des représentants du type : $G/fdX + H/fdY$, où G et H sont des polynômes de degré strictement inférieur à d. On note alors :
$$\mathcal{Z}_f = \{(G, H) \in \mathbb{K}[X, Y]^2_{\leq d-1} \mid \partial_Y\Big(\frac{G}{f}\Big) = \partial_X\Big(\frac{H}{f}\Big)\}.$$

Cet espace vectoriel est le noyau de l'application suivante :

$$\begin{aligned} \mathcal{G}(f) : \mathbb{K}[X,Y]^2_{\leq d-1} &\longrightarrow \mathbb{K}[X,Y]_{2d-2} \\ (g,h) &\longmapsto f^2.\Big[\partial_X\Big(\frac{H}{f}\Big) - \partial_Y\Big(\frac{G}{f}\Big)\Big] \end{aligned}$$

Cette application a été introduite par Gao dans [61]. Celui-ci a repris l'approche de Ruppert afin d'obtenir un algorithme de factorisation absolue. Dans son article, Gao suppose le polynôme f sans facteurs carrés et montre que $\dim_{\mathbb{K}} Z_f = \dim_{\mathbb{K}} \ker \mathcal{G}(f) = r$, où r est le nombre de facteurs absolument irréductibles de f.

Dans [22], il a été remarqué que les dimensions des noyaux des matrices de Gao et de Ruppert sont liées de la manière suivante :

$$\dim_{\mathbb{K}} \ker \mathcal{G}(f) - 1 = dim_{\mathbb{K}} \ker \mathcal{R}up(f).$$

Le fait qu'il est possible de borner le degré d'un représentant d'une forme exacte est aussi utilisé. C'est à dire, toutes formes exactes de $\mathcal{Z}_f$ est du type $d(P/f)$ où P est de degré inférieur à d. On note alors

$$\begin{aligned} \mathcal{B}_f = \{(G,H) \in \mathbb{K}[X,Y]^2_{\leq d-1} \quad | \quad & \omega = \frac{G}{f}dX + \frac{H}{f}dY \in \mathcal{Z}, \\ & \text{et } \exists P \in \mathbb{K}[X,Y]_{\leq d} \text{ vérifiant } d\Big(\frac{P}{f}\Big) = \omega\} \end{aligned}$$

Nous obtenons alors

$$\mathcal{H}^1\big(\overline{\mathbb{K}}^2 \setminus \mathcal{V}(f)\big) \simeq \frac{\mathcal{Z}_f}{\mathcal{B}_f}.$$

Comme $\dim_{\mathbb{K}} \mathcal{H}^1\big(\overline{\mathbb{K}}^2 \setminus \mathcal{V}(f)\big) = r$, nous en déduisons que pour connaitre la dimension de $\mathcal{Z}_f$, donc la dimension du noyau de la matrice de Gao et de la matrice de Ruppert, nous devons calculer la dimension de $\mathcal{B}_f$. Nous pouvons effectuer ce calcul et montrer

$$\dim_{\mathbb{K}} \mathcal{B}_f = \dim_{\mathbb{K}} \mathbb{K}[X,Y]_\nu, \text{ où } \nu = \deg\big(\gcd(f, \partial_X f, \partial_Y f)\big) - 1.$$

Cela entraine le résultat suivant :

Proposition 21. *Soit $f \in \mathbb{K}[X,Y]$, et $f = f_1^{e_1} \cdots f_r^{e_r}$ sa factorisation absolue, où les f_i sont des polynômes de degré d_i. Nous avons :*

$$\dim_{\mathbb{K}} \ker \mathcal{R}up(f) = r - 2 + \binom{2 + \sum_{i=1}^r d_i(e_i - 1)}{2}.$$

Comme nous l'avons dit plus haut, une formule explicite pour la dimension de la matrice de Ruppert et de la matrice de Gao n'était connue que dans le cas où f est sans facteurs carrés. Avec ce résultat général nous allons pouvoir donner une borne sur le spectre en prenant en compte les multiplicités.

3.3 Spectre et multiplicités via la matrice de Ruppert

3.3.1 Le cas dense

Les propriétés sur la matrice de Ruppert et son noyau vont nous permettre d'améliorer la borne sur l'ordre total de réductibilité. En effet, la borne de Lorenzini nous donne $\rho(F_1, F_2) \leq d^2 - 1$, où d est le degré de F_1/F_2, et nous allons voir que nous pouvons conserver la borne $d^2 - 1$ tout en prenant en compte les multiplicités des facteurs. Pour cela nous allons définir quelques quantitiés :

Définition 24. *Si $(\lambda : \mu) \in \sigma(F_1, F_2)$ alors on note la factorisation de $\lambda F_1 - \mu F_2$ dans $\overline{\mathbb{K}}[X, Y]$ de la manière suivante :*

$$\lambda F_1 - \mu F_2 = \prod_{i=1}^{N(\lambda:\mu)} f_{(\lambda:\mu),i}^{e_{(\lambda:\mu),i}}.$$

On pose :

$$m(\lambda : \mu) = \sum_{i=1}^{N(\lambda:\mu)} e_{(\lambda:\mu),i},$$

$$m(F_1, F_2) = \sum_{(\lambda:\mu)\in\mathbb{P}^1(\mathbb{K})} \big(m(\lambda : \mu) - 1\big),$$

$$\omega(\lambda : \mu) = \sum_{i=1}^{N(\lambda:\mu)} \deg(f_{(\lambda:\mu),i}) \left(e_{(\lambda:\mu),i} - 1\right),$$

$$\omega(F_1, F_2) = \sum_{(\lambda:\mu)\in\mathbb{P}^1(\mathbb{K})} \omega(\lambda : \mu),$$

$$\theta(\lambda : \mu) = \binom{\omega(\lambda : \mu) + 1}{2} - \sum_{i=1}^{N(\lambda:\mu)} (e_{(\lambda:\mu),i} - 1),$$

$$\theta(F_1, F_2) = \sum_{(\lambda:\mu)\in\mathbb{P}^1(\mathbb{K})} \theta(\lambda : \mu).$$

La quantité $m(F_1, F_2)$ généralise l'ordre total de réductibilité en prenant en compte la multiplicité des facteurs.
La quantité $\omega(F_1, F_2)$ est le degré du facteur remarquable associé à F_1/F_2, voir Définition 13 page 26.
Nous connaissons la dimension du noyau de $\mathcal{R}up(\lambda F_1 - \mu F_2)$ d'après la Proposition 21.
La quantité $\theta(\lambda : \mu)$ a alors été définie de telle sorte à avoir :

$$(\star)\ m(\lambda : \mu) - 1 + \omega(\lambda : \mu) + \theta(\lambda : \mu) = \dim_{\mathbb{K}} \ker \mathcal{R}up(\lambda F_1 - \mu F_2).$$

Nous pouvons alors énoncer le résultat principal obtenu dans [22] :

Théorème 18. *Soit $\mathbb{K}$ un corps algébriquement clos de caractéristique zéro.*
Soit F_1/F_2 une fraction rationnelle indécomposable de $\mathbb{K}(X, Y)$ de degré d. Nous avons :

$$0 \leq \rho(F_1, F_2) \leq m(F_1, F_2) + \omega(F_1, F_2) + \theta(F_1, F_2) \leq d^2 - 1.$$

Ce résultat signifie que nous pouvons conserver la borne $d^2 - 1$ tout en prenant en compte les multiplicités des facteurs mais aussi en rajoutant d'autres quantités liées aux multiplicités. Par exemple, nous pouvons ajouter $\omega(F_1, F_2)$ qui est le degré du facteur remarquable. Cela donne aussi un autre moyen de montrer la borne de Lorenzini. Nous allons voir que cette stratégie de preuve est simple, constructive et ramène l'étude d'un pinceau de courbes à celle d'un pinceau de matrices.

La preuve de ce théorème fonctionne de la manière suivante :
La Proposition 20 nous donne :

$$\dim_{\mathbb{K}} \ker \big(\lambda \mathcal{R}up(F_1) - \mu \mathcal{R}up(F_2)\big) \leq mult_{(\lambda:\mu)} Spect_{F_1,F_2}.$$

D'après l'égalité $(\star)$, nous avons :

$$m(\lambda : \mu) - 1 + \omega(\lambda : \mu) + \theta(\lambda : \mu) \leq mult_{(\lambda:\mu)} Spect_{F_1,F_2}.$$

En sommant ces inégalités pour toutes les valeurs de $(\lambda : \mu) \in \mathbb{P}^1(\mathbb{K})$, ce qui revient à faire une somme pour $(\lambda : \mu) \in \sigma(F_1, F_2)$, nous obtenons :

$$\sum_{(\lambda:\mu)\in\mathbb{P}^1(\mathbb{K})} \big(m(\lambda : \mu) - 1 + \omega(\lambda : \mu) + \theta(\lambda : \mu)\big) \leq \deg Spect_{F_1,F_2}.$$

Par définition, le membre de gauche est égal à $m(F_1, F_2) + \omega(F_1, F_2) + \theta(F_1, F_2)$. Pour conclure, il nous reste donc juste à remarquer que $Spect_{F_1,F_2}$ est le pgcd de polynômes $\Phi_i(U, V)$ qui sont de degré $d^2 - 1$. En effet, les $\Phi_i(U, V)$ sont les mineurs maximaux de la matrice $\mathcal{R}up(UF_1 - VF_2)$. Le degré de ces mineurs est donc borné par la taille de la matrice. Comme l'espace de départ de l'application linéaire $\mathcal{R}up(UF_1 - VF_2)$ est l'espace vectoriel $\mathcal{E}$, voir Définition 2 page 4, et que celui-ci est de dimension $d^2 - 1$, nous obtenons le résultat désiré.

On obtient un résultat similaire en n variables. C'est à dire, les quantités $m(F_1, F_2)$, $\omega(F_1, F_2)$, et $\theta(F_1, F_2)$ se généralisent aisément en n variables. Ensuite, nous appliquons les théorèmes de Bertini, voir Théorème 4, qui ramène l'étude du problème à un problème en 2 variables. C'est pourquoi, même si nous considérons le spectre d'une fraction rationnelle en n variables la borne reste $d^2 - 1$ et est indépendante du nombre de variables.

3.3.2 Le cas creux

Dans [22] une borne sur $m(F_1, F_2)$ en fonction du polytope de Newton de F_1 et F_2 est aussi donnée. L'approche utilisée permet d'obtenir un énoncé pour des corps de caractéristique non nulle mais ne permet pas de borner la quantité $m(F_1, F_2) + \omega(F_1, F_2) + \theta(F_1, F_2)$.

L'idée est la suivante : Lorsque nous avons un polynôme f qui se factorise absolument en $f = f_1^{e_1} \cdots f_r^{e_r}$ alors nous pouvons exhiber une famille libre de $\ker \mathcal{R}up(f)$ possédant $e_1 + \cdots + e_r$ éléments.
En effet, on peut montrer que les éléments

$$G_i^{(k)} = \frac{f\partial_X(f_i)}{f_i^k},\ H_i^{(k)} = \frac{f\partial_Y(f_i)}{f_i^k}$$

appartiennent au noyau $\ker \mathcal{R}up(f)$ et sont linéairement indépendants.

Comme nous avons une formule explicite pour ces éléments du noyau nous pouvons contrôler leurs polytopes de Newton à partir de celui de f. Cela est possible en utilisant la propriété classique suivante due à Ostrowski [121] : Soient f, f_1, ..., f_r des polynômes de $\mathbb{K}[X,Y]$ tels que $f = f_1 \cdots f_r$ alors $\mathcal{N}(f) = \mathcal{N}(f_1) + \cdots + \mathcal{N}(f_r)$, où la somme est une somme de Minkowski.

Ainsi nous pouvons connaitre a priori un polytope contenant $\mathcal{N}(G_i^{(k)})$ et $\mathcal{N}(H_i^{(k)})$, donc il est possible de restreindre l'étude de $\mathcal{R}up(f)$ à un sous-espace vectoriel dont la dimension dépend de la taille de $\mathcal{N}(f)$. L'application de la Proposition 20 permet alors de conclure comme précédemment. Il vient alors, voir [22] :

Théorème 19. *Soit $\mathcal{N}$ un ensemble convexe de $\mathbb{R}^2$. On désigne par N le nombre de points à coordonnées entières à l'intérieur de celui-ci, et par N_X (respectivement N_Y) le nombre de points à coordonnées entières de $\mathcal{N}$ se trouvant sur l'axe des X (respectivement sur l'axe des Y). Si $\mathcal{N}$ possède une arête $\mathcal{A}$ verticale, horizontale ou de pente négative, alors on note $N_{\mathcal{A}}$ le nombre de points à coordonnées entières sur cette arête.*
Soit F_1/F_2 une fraction rationnelle indécomposable dans $\mathbb{K}(X,Y)$ de degré d. On suppose que $\mathcal{N} \subseteq N\left((1+X+Y)^d\right)$ et que le corps $\mathbb{K}$ est de caractéristique $p = 0$ ou $p > d(d-1)$.

- *Si $N(F_1) \subset \mathcal{N}$ et $N(F_2) \subset \mathcal{N}$ alors*

$$\rho(F_1, F_2) \leq 2N - N_X - N_Y - N_{\mathcal{A}} + \kappa.$$

- *Si $N(F_1) \subset \mathcal{N}$, $N(f_2) \subset \mathcal{N}$ et $(-F_2(0,0) : F_1(0,0)) \notin \sigma(F_1, F_2)$ alors*

$$m(F_1, F_2) \leq 2N - N_X - N_Y - N_{\mathcal{A}} + \kappa.$$

où $\kappa = \max(e_\infty - 1, 0)$ et e_∞ est la multiplicité (qui peut être nulle) de la droite à l'infini $\{Z = 0\}$ dans le pinceau de courbes $\lambda F_1 - \mu F_2$.

Il faut comprendre ce résultat ainsi :
Dans le cas dense G et H sont de degré $d-1$ et le -1 provient d'une dérivée en X pour G et d'un dérivée en Y pour H. Le passage au cas creux donne G et H de taille bornée par $N - N_X$ et $N - N_Y$.
Dans le cas dense, nous utilisons la relation d'Euler pour restreindre le noyau aux éléments satisfaisant $\deg(XG + YH) \leq d-1$. Ici, nous faisons de même avec un degré pondéré sur l'arête $\mathcal{A}$. Cela donne le $-N_{\mathcal{A}}$.
Ensuite, κ est là pour gérer une chute de degré possible.

L'hypothèse $(-F_2(0,0) : F_1(0,0)) \notin \sigma(F_1, F_2)$ nous permet d'étudier des polynômes avec des termes constants non nuls ce qui est un besoin technique de la preuve.

Une autre variante de ce résultat est donnée dans [22]. De plus, on montre grâce à l'exemple de Lorenzini : $F_1(X,Y) = Y\prod_{i=1}^{d-1}(X-i) + X$, $F_2(X,Y) = 1$ que celle-ci est quasi optimale (à une unité près). Autrement dit, dans ce cas $m(F_1, F_2) = 2d-2$ et la borne donne $2d-1$.

Après avoir étudié les bornes sur le spectre et joué sur la représentation des polynômes en prenant en compte le polytope de Newton, une question naturelle se pose : lorsque

nous considérons un polynôme lacunaire ou bien donné par un programme d'évaluation peut on borner le spectre en fonction de la taille des polynômes dans ces représentations ?

Le polynôme $F(X,Y) = Y(X^d - 1) + X$ nous montre que la réponse est non.
Ce polynôme possède 3 termes et les entiers utilisés pour représenter ce polynôme sont de taille $\log(d)$. Le spectre de F est l'ensemble des racines d-ième de l'unité. Le cardinal du spectre est donc égal à d. Nous voyons ainsi que nous ne pouvons pas borner le cardinal du spectre en fonction du nombre de coefficients non nuls de F, ni de manière polynomial en la taille de l'entrée.

3.4 Utilisation de la borne de Jouanolou

Précédemment nous avons amélioré la borne $\rho(F_1, F_2) \leq d^2 - 1$ en prenant en compte les multiplicités. Autrement dit, nous avons conservé le membre de droite de l'inégalité et fait grossir le membre de gauche. Une autre façon d'améliorer la borne $\rho(F_1, F_2) \leq d^2 - 1$ est de conserver le membre de gauche et de diminuer le membre de droite en prenant en compte les multiplicités. Nous allons voir ici que la borne de Jouanolou nous permet de faire cela. Cette remarque se trouve dans [34].

Théorème 20. *Soit D une dérivation de degré k et $F_1/F_2 \in \mathbb{C}(X,Y)$ une intégrale première rationnelle indécomposable de D. Nous avons alors :*

$$\rho(F_1, F_2) < k(k+1)/2 + 2.$$

L'hypothèse "F_1/F_2 intégrale première d'une dérivation" n'est pas restrictive puisque nous pouvons toujours considérer la dérivation jacobienne associée à F_1/F_2.

Si nous exprimons la borne obtenue en fonction du degré de F_1/F_2 alors cette borne prend bien en compte les multiplicités car nous rappelons la relation, voir Théorème 10 page 27 :

$$k + \omega(F_1, F_2) = \deg(F_1) + \deg(F_2) - 1,$$

où $\omega(F_1, F_2)$ est le degré du facteur remarquable associé à F_1/F_2.

La stratégie que nous allons utiliser s'inspire de celle développée par Stein dans [140]. Tout d'abord nous construisons une intégrale première rationnelle à partir de facteurs du type $f_{(\lambda,\mu),i}$ et ensuite nous obtenons une contradiction.

Démonstration. On désigne par s le cardinal du spectre, alors :

$$f_{(\lambda_1,\mu_1),1}, \ldots, f_{(\lambda_1,\mu_1),N(\lambda_1:\mu_1)-1}, \ldots, f_{(\lambda_s,\mu_s),1}, \ldots, f_{(\lambda_s,\mu_s),N(\lambda_s:\mu_s)-1}$$

sont des polynômes de Darboux de D distincts.
A présent supposons que nous ayons

$$(\star)\ \rho(F_1, F_2) \geq \frac{k(k+1)}{2} + 2.$$

Cela signifie que la dérivation D de degré k possède au moins $k(k+1)/2+2$ polynômes de Darboux distincts. Le théorème de Jouanolou, voir Théorème 7, implique donc qu'il existe des entiers $c_{(\lambda_1:\mu_1),1}, \dots c_{(\lambda_s:\mu_s)-1}$ tels que

$$\prod_{j=1}^{s} \prod_{i=1}^{N(\lambda_j,\mu_j)-1} f_{(\lambda_j,\mu_j),i}^{c_{(\lambda_j:\mu_j),i}} \in \mathbb{C}(X,Y)^D.$$

D'après la Proposition 5 page 19, on obtient :

$$\prod_{j=1}^{s} \prod_{i=1}^{N(\lambda_j,\mu_j)-1} f_{(\lambda_j,\mu_j),i}^{c_{(\lambda_j:\mu_j),i}} = u\Big(\frac{F_1}{F_2}\Big),$$

où $u \in \mathbb{C}(T)$. De plus, $u(F_1/F_2)$ est de la forme :

$$u\Big(\frac{F_1}{F_2}\Big) = \frac{\prod_l(\alpha_l F_1 - \beta_l F_2)}{\prod_m(\gamma_m F_1 - \delta_m F_2)}.F_2^e,$$

où $\alpha_l, \beta_l, \gamma_m, \delta_m \in \mathbb{C}$ et $e \in \mathbb{Z}$. Donc, nous avons l'égalité :

$$\prod_{j=1}^{s} \prod_{i=1}^{N(\lambda_j,\mu_j)-1} f_{(\lambda_j,\mu_j),i}^{c_{(\lambda_j:\mu_j),i}} = \frac{\prod_l(\alpha_l F_1 - \beta_l F_2)}{\prod_m(\gamma_m F_1 - \delta_m F_2)}.F_2^e,$$

qui est impossible. En effet, comme la factorisation en irréductibles dans $\mathbb{C}[X,Y]$ est unique, on en déduit que $(\alpha_l : \beta_l)$ et $(\gamma_m : \delta_m)$ appartiennent à $\sigma(F_1,F_2)$. On peut supposer alors que $(\lambda_1 : \mu_1) = (\alpha_1 : \beta_1)$. Dans ce cas nous constatons que le facteur irréductible $f_{(\lambda_1:\mu_1),N(\lambda_1:\mu_1)}$ apparaît dans le membre de droite mais pas dans le membre de gauche. Cela signifie que la supposition $(\star)$ est absurde et prouve notre résultat. □

Lorsque $\omega(F_1,f_2) = 0$, la borne proposée dans le Théorème 20 donne $\rho(F_1,F_2) \leq 2d^2-d+2$. Cela se compare défavorablement à la borne d^2-1. Cependant, nous verrons au Chapitre 6 comment obtenir un théorème du type Jouanolou en fonction d'un polytope de Newton lié à la dérivation. Cela signifie que le Théorème 20 a lui aussi un homologue creux. Dans le cas creux nous verrons que cette approche permet d'obtenir une borne optimale en fonction de la taille du polytope de Newton considéré, voir le Théorème 34 page 84.

3.5 Prolongements

Avant de clore ce chapitre mentionnons deux problèmes liés au spectre :

– La borne d^2-1 sur l'ordre total de réductibilité est-elle optimale ?
Autrement dit, peut-on trouver des exemples où $\rho(F_1,F_2) = d^2-1$?
Il existe de tels exemples pour $d \leq 3$, voir l'article de Lorenzini [101].
Remarquons que ce problème est lié à la question de l'optimalité de la borne d^2-1 pour les formes de Noether.

– La borne $k(k+1)/2+2$ du théorème de Jouanolou est-elle optimale ?

Chapitre 4

Étude des polynômes et des fractions rationnelles indécomposables

4.1 Indécomposabilité et extension de corps

Nous savons que la factorisation rationnelle (c'est à dire la factorisation dans le corps des coefficients) et la factorisation absolue (c'est à dire la factorisation dans une clôture algébrique du corps des coefficients) sont deux choses distinctes. Dans cette section nous étudions le comportement de l'indécomposabilité lorsque nous considérons une extension de corps. Nous allons voir que contrairement à la factorisation, il n'y a pas de distinction entre décomposition rationnelle et décomposition absolue. Lorsque l'on étudie la décomposition ces deux notions coïncident.

Dans le cas des polynômes indécomposables, la situation a été bien étudiée. On peut toujours ramener facilement le problème à un problème en une variable en utilisant une substitution à la Kronecker. Dans le cas d'une seule variable l'indécomposabilité se définit comme suit :

Définition 25. *Soit $f(T) \in \mathbb{K}(T)$ (resp. $\in \mathbb{K}[T]$). On dit que f est décomposable lorsqu'il existe $g, h \in \mathbb{K}(T)$ (resp. $\in \mathbb{K}[T]$) de degré strictement supérieur à 1 tels que $f = g(h)$, sinon on dit que f est indécomposable.*

Il faut noter la différence avec la définition de la décomposabilité dans $\mathbb{K}(X, Y)$. Dans le cas d'une seule variable h doit aussi être de degré strictement supérieur à 1. Cette condition provient du fait qu'une fraction rationnelle en une variable et de degré 1 est inversible pour la composition.

Pour les polynômes en une seule variable nous avons le résultat suivant, voir [135, Theorem 6] :

Proposition 22. *Soient $\mathbb{K}$ un corps de caractéristique $p \geq 0$, et $f \in \mathbb{K}[T]$ un polynôme indécomposable de degré d. Si p ne divise pas d alors f reste indécomposable sur toutes extensions de corps de $\mathbb{K}$.*

Dans le cas de plusieurs variables : une réduction à la Kronecker nous ramène au cas d'une seule variable puis l'application de la proposition précédente nous permet alors de conclure que la situation est la même en n variables. Pour plus de détails voir l'article d'Ayad [5, Théorème 7]. Une caractérisation des cas où l'indécomposabilité sur $\mathbb{K}$ n'est pas équivalente à l'indécomposabilité sur $\overline{\mathbb{K}}$ est donnée dans l'article de Bodin, Dèbes et Najib [16, Theorem 4.2].

Dans le cas des fractions rationnelles, nous ne pouvons pas avoir la même stratégie de preuve que dans le cas polynomial. En effet, nous avons le contre-exemple suivant donné par Gutierrez et Sevilla [75, Example 5] :

$$f(X) = \frac{\omega^3 X^4 - \omega^3 X^3 - 8X - 1}{2\omega^3 X^4 + \omega^3 X^3 - 16X + 1}$$

où $\omega \notin \mathbb{Q}$ et $\omega^3 \in \mathbb{Q} \setminus \{1\}$. Dans ce cas, on a f indécomposable dans $\mathbb{Q}(X)$, mais $f = g(h)$ avec

$$g(X) = \frac{X^2 + (4-\omega)X - \omega}{2X^2 + (8+\omega)X + \omega},\ h(X) = \frac{X\omega(X\omega - 2)}{X\omega + 1}.$$

Donc f est indécomposable dans $\mathbb{Q}(X)$ mais décomposable dans $\mathbb{Q}(\omega)(X)$. Toutefois, dans le cas où f possède plusieurs variables, nous pouvons montrer que nous conservons l'indécomposabilité dans une extension de corps, voir [23] :

Théorème 21. *Soit $F(X_1, \ldots, X_n) \in \mathbb{K}(X_1, \ldots, X_n)$ une fraction rationnelle de degré d à coefficients dans un corps parfait $\mathbb{K}$ de caractéristique 0 ou supérieure à d^2. On a alors l'équivalence entre :*

1. *F est indécomposable dans $\mathbb{K}(X_1, \ldots, X_n)$,*
2. *F est indécomposable dans $\overline{\mathbb{K}}(X_, \ldots, X_n)$, où $\overline{\mathbb{K}}$ désigne une clôture algébrique de $\mathbb{K}$.*

L'idée de la preuve est la suivante :
L'implication (2.) $\Rightarrow$ (1.) est évidente. Il faut donc montrer l'implication (1.) $\Rightarrow$ (2.). Pour cela, nous allons supposer $F = F_1/F_2$ décomposable dans $\overline{\mathbb{K}}(X_1, \ldots, X_n)$ et montrer que F est décomposable dans $\mathbb{K}(X_1, \ldots, X_n)$.
Dire que F est décomposable dans $\overline{\mathbb{K}}(X_1, \ldots, X_n)$ signifie que $F = u(H)$ avec $u \in \overline{\mathbb{K}}(T)$ et $H = H_1/H_2 \in \overline{\mathbb{K}}(X_1, \ldots, X_n)$, où H est indécomposable et $\deg u \geq 2$. Comme le spectre est fini, nous pouvons trouver un élément $\lambda \in \overline{\mathbb{K}}$ tel que

$$(\star)\ F_1 - \lambda F_2 = \prod_i (H_1 - t_i H_2),$$

avec $t_i \in \overline{\mathbb{K}}$ et $H_1 - t_i H_2$ irréductible dans $\overline{\mathbb{K}}[X_1, \ldots, X_n]$.
La preuve repose alors sur l'étude du comportement d'un $\mathbb{K}$-automorphisme τ dans cette factorisation. Cela permet alors de montrer que $\tau(H_i) = H_i$, et de conclure que $H_i \in \mathbb{K}[X_1, \ldots, X_n]$. Le fait que $u \in \mathbb{K}(T)$ est alors immédiat.

Dans le cadre de l'étude des intégrales premières rationnelles du plan, ce théorème entraine le résultat suivant donné dans [18] :

Théorème 22. *Soit $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$ une dérivation avec $A, B \in \mathbb{Q}[X,Y]$. Si D admet une intégrale première rationnelle indécomposable dans $\mathbb{C}(X,Y)$ alors D possède une intégrale première rationnelle indécomposable dans $\mathbb{Q}(X,Y)$ et de même degré.*

Démonstration. Soit $f \in \mathbb{C}(X,Y)$ une intégrale première rationnelle indécomposable. La norme $N(f)$ de f est le produit suivant :

$$N(f) = \prod_{\sigma_i \in G} \sigma_i(f),$$

où G est le groupe de Galois sur $\mathbb{Q}$ du corps engendré par tous les coefficients de f. Il vient alors $N(f) \in \mathbb{Q}(X,Y)$ et $N(f)$ est aussi une intégrale première. Il existe donc une intégrale première $F \in \mathbb{Q}(X,Y)$ indécomposable. Donc d'après la Proposition 5, nous obtenons $F = u(f)$. Or, F est indécomposable dans $\mathbb{Q}(X,Y)$ donc indécomposable dans $\mathbb{C}(X,Y)$ d'après le Théorème 21. Ainsi, il vient $\deg u = 1$ et alors $\deg(F) = \deg(f)$. □

Ce théorème explique pourquoi lorsque nous avons une dérivation à coefficients rationnels, nous pouvons chercher une intégrale première à coefficients rationnels. Dans [107], Man et MacCallum ont montré dans ce contexte que si une intégrale première existe dans $\mathbb{C}(X,Y)$ alors il en existe une dans $\mathbb{Q}(X,Y)$. Ici, nous améliorons ce résultat en montrant qu'en cherchant une intégrale première dans $\mathbb{Q}(X,Y)$ nous n'augmentons pas le degré de l'expression recherchée.

4.2 Indécomposabilité et théorèmes de Bertini, Noether et Ostrowski

Dans cette section, nous allons voir que les théorèmes classiques de factorisation ont des équivalents dans le cadre de la décomposition des polynômes et des fractions rationnelles. Autrement dit, nous allons voir qu'en modifiant les bornes des énoncés effectifs, nous pouvons remplacer le mot "irréductible" par "indécomposable" dans les théorèmes de Bertini, Noether et Ostrowski.

4.2.1 Le cas des fractions rationnelles

Le théorème de Bertini-Krull, voir Théorème 9 page 21, nous donne l'équivalence entre les assertions suivantes :

1. $F_1/F_2(X_1,\ldots,X_n) \in \mathbb{K}[X_1,\ldots,X_n]$ est indécomposable,
2. $F(X_1,\ldots,X_n) - TF_2(X_1,\ldots,X_n)$ est irréductible dans $\overline{\mathbb{K}(T)}[X_1,\ldots,X_n]$, où T est une variable.

Ainsi, pour obtenir des énoncés à la Bertini, Ostrowski, et Noether dans le cadre de la décomposition nous pouvons simplement appliquer ces théorèmes classiques au polynôme $F_1(\underline{X}) - TF_2(\underline{X}) \in \mathbb{K}(T)[\underline{X}]$. Le théorème de Bertini devient alors :

Théorème 23. *Soient $F_1/F_2 \in \mathbb{K}(X_1,\ldots,X_n)$, $A_1,\ldots,A_{n-1}$, $B_1,\ldots,B_{n-1}$, des variables indépendantes sur $\mathbb{K}$, $\mathbb{L} = \mathbb{K}(A_1,B_1,\ldots,A_{n-1},B_{n-1})$ et*

$$R(X,Y) = F_1/F_2(A_1 + B_1Y,\ldots,A_{n-1} + B_{n-1}Y, X, Y) \in \mathbb{L}(X,Y).$$

On a alors : $R(X,Y)$ est indécomposable dans $\mathbb{L}(X,Y)$ si et seulement si F_1/F_2 est indécomposable dans $\mathbb{K}(X_1,\ldots,X_n)$.

Nous avons choisi dans cet énoncé d'utiliser une substitution à la Matsusaka-Zariski, voir Chapitre 1.

A titre d'exemple, voici ce que donne la version effective du théorème d'Ostrowski pour les fractions rationnelles indécomposables.

Théorème 24. *Soit F_1 et $F_2 \in \mathbb{Z}[X_1,\ldots,X_n]$ deux polynômes premiers entre eux tels que F_1/F_2 soit indécomposable. On pose $d = \deg(F_1/F_2)$ et*

$$\mathcal{B} = d^{3d^2-3}\left(\binom{n+d}{n}2^d\right)^{d^2-1}\binom{d^2-1}{\lfloor (d^2-1)/2\rfloor}\max\left(\|F_1\|_\infty, \|F_2\|_\infty\right)^{d^2-1}.$$

Si p est un nombre premier supérieur à $\mathcal{B}$ alors :

1. *$\overline{F_1}$, et $\overline{F_2} \in \mathbb{F}_p[X_1,\ldots,X_n]$ sont premiers entre eux,*
2. *$\overline{F_1}/\overline{F_2} \in \mathbb{F}_p(X_1,\ldots,X_n)$ est indécomposable.*

4.2.2 Le cas des polynômes

Le problème de la décomposition est un problème de factorisation spécifique. En effet, si $F(X,Y) \in \mathbb{K}[X,Y]$ se décompose en $u(H)$ alors en notant $u(T) = u_r\prod_{i=1}^r(t-\lambda_i)$, avec $u_r \in \mathbb{K}$ et $\lambda_i \in \overline{\mathbb{K}}$ nous avons $F(X,Y) = u_r.\prod_{i=1}^r(H(X,Y)-\lambda_i)$. La décomposition peut donc se voir comme une factorisation absolue particulière.
Il faut donc s'attendre, lorsque l'on étudie la décomposition, à pouvoir obtenir des résultats plus fins que lorsque l'on étudie la factorisation d'un polynôme quelconque. Nous allons voir ici comment obtenir des résultats fins en développant une stratégie adaptée à la décomposition des polynômes.

La démarche présentée dans cette section est semblable à celle utilisée dans le Chapitre 1. C'est à dire, nous construisons dans un premier temps une application linéaire caractérisant la décomposabilité. Cette matrice sera la matrice associée à une dérivation jacobienne, et elle aura le même rôle que la matrice de Ruppert pour la factorisation. Ensuite, en regardant les mineurs maximaux de cette matrice nous obtenons les formes de Noether pour la décomposition. (Nous appelons par abus de langage "formes de Noether pour la décomposition", les équations de la variété algébrique des polynômes décomposables.) Puis, en majorant la taille de ces mineurs maximaux nous obtenons une borne pour un énoncé à la Ostrowski.

Avant de définir la matrice qui remplacera celle de Ruppert, nous devons introduire quelques notations :

Définition 26. *On note $E_{d_{min}}$ l'ensemble suivant :*

$$E_{d_{min}} = \left\{H(X,Y) \in \mathbb{K}[X,Y] \mid \deg H \leq \frac{d}{d_{min}} \text{ et } H(0,0) = 0\right\},$$

où d_{min} est le plus petit nombre premier divisant $\deg(F) = d$.

Définition 27. *Soit* $F(X,Y) \in \mathbb{K}[X,Y]$ *un polynôme tel que* $\deg_X(F) > 0$ *et* $\deg_Y(F) > 0$. *L'application linéaire suivante :*

$$\begin{array}{rcl} \mathcal{J}ac(F) : E_{d_{min}} & \longrightarrow & \mathbb{K}[X,Y] \\ H(X,Y) & \longmapsto & \partial_X F.\partial_Y H - \partial_Y F.\partial_X H \end{array}$$

est la restriction à $E_{d_{min}}$ *de la dérivation jacobienne associée à* F.

L'application de la Proposition 5 page 19 à la dérivation jacobienne donne directement le résultat suivant. Dans [37], le cas de la caractéristique positive a aussi été traité et on obtient :

Proposition 23. *Soit* $F \in \mathbb{K}[X,Y]$ *un polynôme de degré* d *où* $\mathbb{K}$ *un corps de caractéristique* $p = 0$ *ou* $p > \dfrac{d^2}{d_{min}}$. *Nous avons :*

$$\dim_{\mathbb{K}} \ker \mathcal{J}ac(F) = \{0\} \iff F \text{ est indécomposable.}$$

Nous pouvons remarquer que l'hypothèse sur la caractéristique est nécessaire car $F(X,Y) = X^{p+1}Y \in \mathbb{F}_p[X,Y]$ est indécomposable puisque $\deg_Y(F) = 1$, mais $0 \neq XY \in \ker \mathcal{J}ac(F)$.

Dans le cadre de la décomposition, cette proposition est l'équivalent du Théorème 3 page 5. C'est à dire, $\mathcal{J}ac(F)$ est à la décomposition ce que $\mathcal{R}up(F)$ est à la factorisation. En reprenant, l'approche présentée dans le Chapitre 1, nous pouvons donc obtenir des énoncés effectifs à la Noether, Bertini et Ostrowski pour la décomposition.

Nous pouvons comprendre facilement l'intérêt de passer par la matrice $\mathcal{J}ac(F)$ pour étudier la décomposition. En effet, lorsque nous étudions la factorisation via la matrice de Ruppert, la borne $d^2 - 1$ sur le degré des formes de Noether provient de la dimension de l'espace source de $\mathcal{R}up(F)$. Pour la matrice $\mathcal{J}ac(F)$ la dimension de l'espace source est deux fois plus petite que celle de $\mathcal{R}up(F)$. Cela provient du simple fait que nous considérons ici qu'un seul polynôme H à la place de deux (G,H) pour la matrice de Ruppert.

En considérant les mineurs maximaux de $\mathcal{J}ac(F)$ nous obtenons :

Théorème 25. *Soient* $d \geq 2$ *et* $n \geq 2$ *deux entiers, et soit* $F = \sum_{|\underline{e}| \leq d} c_{\underline{e}} X_1^{e_1} \dots X_n^{e_n}$ *un polynôme à coefficients dans* $\mathbb{K}$. *On suppose que* $\mathbb{K}$ *est de caractéristique* $p = 0$ *ou* $p > d^2/d_{min}$.
Dans ce cas, il existe une famille finie de polynômes

$$\Psi_1, \dots, \Psi_N \in \mathbb{Z}[C_{\underline{e}}] := \mathbb{E},$$

où $C_{\underline{e}}$ *sont des variables, et* $e_1 + \dots + e_n \leq d$, *vérifiant la propriété suivante :*

$$\Psi_t(c_{\underline{e}}) = 0 \text{ pour tout } t = 1, \dots, N \iff F \text{ est décomposable ou } \deg(F) < d.$$

De plus, pour tout $t = 1, \dots, N$,

$$\deg(\Psi_t) \leq \frac{1}{2}\Big(\frac{d}{d_{min}} + 1\Big)\Big(\frac{d}{d_{min}} + 2\Big) + 1$$

La borne obtenue est inférieure à d^2-1. Par exemple, si nous considérons un polynôme de degré 10 alors le degré des formes obtenues est bornée par 22 tandis que le degré des formes de Noether pour la factorisation absolue est dans ce cas borné par 99.

En considérant la taille des mineurs maximaux de $\mathcal{J}ac(F)$, nous pouvons donner un théorème effectif à la Ostrowski pour l'indécomposabilité, voir Theorem 15 dans [37]. Dans ce cas, pour borner la taille des mineurs maximaux nous utilisons la borne d'Hadamard. Ainsi, la borne obtenue est du type : hauteur des coefficients de F à la puissance la dimension de l'espace source de $\mathcal{J}ac(F)$. La borne obtenue est donc plus fine que celle obtenue dans l'étude de l'irréductibilité absolue où la borne est du type : hauteur des coefficients de F à la puissance d^2-1.

4.3 Indécomposabilité et spécialisation

Les sections précédentes ont montré comment obtenir via la dérivation jacobienne l'équivalent des théorèmes classiques portant sur l'irréductibilité absolue, à savoir les théorèmes de Bertini, Noether et Ostrowski. Il existe un autre théorème classique portant sur l'irréductibilité d'un polynôme : le théorème d'irréductibilité de Hilbert. Ce théorème dit que si nous considérons un polynôme $f(X,Y) \in \mathbb{Q}[X,Y]$ irréductible et tel que $\deg_Y(f) > 0$ alors pour une infinité de $x_0 \in \mathbb{Q}$, $f(x_0,Y)$ est irréductible dans $\mathbb{Q}[Y]$.
Une question naturelle se pose alors : l'indécomposabilité d'un polynôme en plusieurs variables est elle préservée par spécialisation d'une de ses variables ?
La réponse est non. Le polynôme $F(X,Y) = XY^4$ est indécomposable dans $\mathbb{K}[X,Y]$ mais pour tout $x_0 \in \mathbb{K}$ nous avons $f(x_0,Y) = x_0(Y^2)^2$. Donc $F(x_0,Y)$ est décomposable, sous la forme $g(h)$, avec $g(Y) = x_0Y^2$ et $h(Y) = Y^2$.
Dans cette section nous allons voir que si nous considérons des spécialisations "génériques" du type : $X_i \mapsto x_i + \alpha_i Y$ où $x_i, \alpha_i \in \mathbb{K}$ alors l'indécomposabilité est préservée. Rappelons que générique signifie que l'on considère des couples $(x_1,\ldots,x_n,\alpha_1,\ldots,\alpha_n)$ en dehors d'une variété algébrique. Nous verrons comment décrire cette variété et comment en déduire un énoncé probabiliste.

Tout d'abord remarquons que le Théorème 23 nous permet de ramener notre étude de n à deux variables. Pour démontrer la réduction de deux à une variable nous allons procéder comme suit. Tout d'abord nous allons démontrer le théorème suivant :

Théorème 26. *Soient $F(X,Y) \in \mathbb{K}[X,Y]$ un polynôme indécomposable de degré d, où $\mathbb{K}$ est un corps de caractéristique $p = 0$ ou $p > d$. Alors le polynôme $F(X+AY,Y)$ est indécomposable dans $\mathbb{K}(A,X)[Y]$, où A est une nouvelle variable.*

L'hypothèse sur la caractéristique du corps est nécessaire. En effet, le polynôme $F(X,Y) = Y^{p^2} + Y^p + X$ est indécomposable dans $\mathbb{F}_p[X,Y]$ mais $F(X+AY,Y) \in \overline{\mathbb{F}_p(A,X)}[Y]$ est décomposable. Nous avons $F(X+AY,Y) = U(H)$, où $U(X,Y) = Y^p + aY + X$ et $H(X,Y) = Y^p + bY$, lorsque $ab = \alpha$ et $a + b^p = 1$.
Dans ce qui suit, cette hypothèse sur la caractéristique nous servira aussi à avoir l'équivalence entre : indécomposable dans $\mathbb{K}(A,X)[Y]$ et indécomposable dans $\overline{\mathbb{K}(A,X)}[Y]$, voir la Proposition 22.

A partir de ce théorème nous obtenons le corollaire :

Corollaire 6. *Soit $F(X,Y) \in \mathbb{K}[X,Y]$ un polynôme indécomposable de degré d, où $\mathbb{K}$ est un corps de caractéristique $p = 0$ ou $p > d$. Il existe des polynômes $\Psi_{m,i}(A,X) \in \mathbb{K}[A,X]$ de degré inférieur à $md^2 + 2d$, où m divise d et $i = 1, \ldots, d - d/m$, vérifiant :*
Pour tout $(\alpha, x) \in \mathbb{K}^2$, si pour chaque diviseur m de d il existe un indice i_0 tel que $\Psi_{m,i_0}(\alpha, x) \neq 0$, alors $F(x + \alpha Y, Y)$ est de degré d et indécomposable dans $\mathbb{K}[Y]$.

Donnons à présent les grandes lignes des preuves de ces résultats en caractéristique zéro. La caractéristique zéro nous permettra de mettre en avant les idées et évitera des difficultés techniques. La preuve complète effectuée en toute généralité se trouve dans [15].

Commençons par étudier le théorème. Pour le démontrer, nous allons montrer la contraposée. Notons $G(A,X,Y) = F(X + AY, Y)$ et supposons que G soit décomposable dans $\mathbb{K}(A,X)[Y]$. A l'aide de quelques manipulations algébriques nous pouvons supposer que G est unitaire dans $\mathbb{K}(A,X)[Y]$ et que dans la décomposition $G = U(H)$, U et $H \in \mathbb{K}(A,X)[Y]$ sont des polynômes unitaires et de degré supérieur à deux. Un résultat de Turnwald [141], nous permet alors de supposer que $U, H \in \mathbb{K}(A)[X][Y]$. A présent, en considérant les racines et la décomposition de G nous obtenons :

$$(\star)\ G(A,X,Y) = \prod_i \big(Y - \varphi_i(A,X)\big) = \prod_j \big(H(A,X,Y) - t_j(A,X)\big),$$

où les $\varphi_i(A,X) \in \overline{\mathbb{K}(A,X)}$ sont les racines de G vu comme un polynôme en Y et les $t_j(A,X) \in \overline{\mathbb{K}(A,X)}$ sont les racines de U vu comme un polynôme en Y.

L'objectif à présent est de montrer : $t_j(A,X) \in \overline{\mathbb{K}(A)}$.
Cela donnera $U \in \mathbb{K}(A)[Y]$, c'est à dire nous aurons fait disparaitre la variable X du polynôme U. En posant $A = 0$ dans la décomposition $G = U(H)$, nous obtiendrons dans $\mathbb{K}[X,Y]$: $F = \tilde{U}(\tilde{H})$ où $\tilde{U} = U(0,Y) \in \mathbb{K}[Y]$ et $\tilde{H} = H(0,X,Y)$, donc F décomposable. Cela donne le résultat annoncé dans le théorème.

Pour montrer que $t_j(A,X) \in \overline{\mathbb{K}(A)}$ nous procédons comme suit :
De l'équation $(\star)$ nous déduisons l'existence d'ensembles d'indices I_j tels que :

$$\prod_{I_j} \big(Y - \varphi_i(A,X)\big) = H(A,X,Y) - t_j(A,X).$$

On pose $\deg_Y(H) = r$. En identifiant les coefficients en Y^k du membre de gauche et du membre de droite, nous remarquons alors que pour $k = 1, \ldots, r-1$, les fonctions élémentaires σ_k en les φ_i sont des coefficients de $H(A,X,Y)$. Ces fonctions élémentaires sont donc indépendantes des ensembles d'indices I_j et appartiennent à $\mathbb{K}(A)[X]$. En considérant les sommes de Newton cela donne :

$$(\star\star)\ \sum_{i \in I_i} \varphi_i(A,X)^k = \sum_{j \in I_j} \varphi_j(A,X)^k \text{ dans } \mathbb{K}(A)[X],\ \text{pour } k = 1, \ldots, r-1.$$

Nous allons à présent voir comment passer cette information au rang $k = r$. Pour cela, nous pouvons utiliser une idée présentée par G. Lecerf et A. Galligo lorsque ceux-ci étudiaient un algorithme de factorisation :

Lemme 5. *Soient $\mathbb{K}$ un corps de caractéristique 0 ou $p > d$ et $f \in \mathbb{K}[X, Y]$ un polynôme de degré d.*
Soient $G(A, X, Y) = f(X + AY, Y)$ dans $\mathbb{K}[A, X, Y]$ et φ une racine dans $\overline{\mathbb{K}(A, X)}$ de $G(A, X, Y)$ vu comme un polynôme en Y. On a :

$$\frac{\partial \varphi}{\partial A} = \varphi \frac{\partial \varphi}{\partial X} (\textit{Équation de Burger}).$$

Lecerf et Galligo ont utilisé cette relation afin d'étudier une technique de recombinaison pour la factorisation des polynômes. Ici, cette relation va nous permettre de conclure. En effet, dérivons par rapport à A la relation $(\star\star)$ lorsque $k = r - 1$, cela donne :

$$\sum_{i \in I_i} (r-1) \partial_A(\varphi_i) \varphi_i^{r-2} = \sum_{j \in I_j} (r-1) \partial_A(\varphi_j) \varphi_j^{r-2} \text{ dans } \mathbb{K}(A)[X].$$

Nous appliquons à présent le Lemme 5, on obtient :

$$\sum_{i \in I_i} (r-1) \varphi_i \partial_X(\varphi_i) \varphi_i^{r-2} = \sum_{j \in I_j} (r-1) \varphi_i \partial_X(\varphi_j) \varphi_j^{r-2} \text{ dans } \mathbb{K}(A)[X].$$

Donc

$$\sum_{i \in I_i} \partial_X(\varphi_i^r) = \sum_{j \in I_j} \partial_X(\varphi_j^r) \text{ dans } \mathbb{K}(A)[X].$$

Comme nous avons supposé $\mathbb{K}$ de caractéristique zéro, il vient

$$\sum_{i \in I_i} \varphi_i^r = \sum_{j \in I_j} \varphi_j^r + c_{I_i, I_j} \text{ dans } \overline{\mathbb{K}(A)}[X]$$

avec c_{I_i,I_j} dans $\overline{\mathbb{K}(A)}$. En utilisant à nouveau les relations de Newton, nous obtenons

$$\prod_{i \in I_i} \varphi_i = \prod_{j \in I_j} \varphi_j + C_{I_i, I_j} \text{ dans } \overline{\mathbb{K}(A)}[X],$$

où $C_{I_i,I_j} \in \overline{\mathbb{K}(A)}$. Les produits $\prod_{i \in I_j} \varphi_i$ correspondant au terme constant de $H(A, X, Y) - t_j(A, X)$, on montre alors que quitte à translater H nous avons : $t_j(A, X) \in \overline{\mathbb{K}(A)}$. Cela démontre alors le théorème.

Pour démontrer le Corollaire 6, on s'appuie sur une caractérisation de la décomposition développée par Bodin dans [14]. En effet, sous certaines hypothèses si un polynôme en une variable $f(Y) \in \mathbb{K}[Y]$ s'écrit $f = u(h) + r$ avec $u, h, r \in \mathbb{K}[Y]$ alors u, h et r sont uniques et nous avons f décomposable si et seulement si $r = 0$. Ce résultat peut se voir comme une "décomposition euclidienne" où r est un reste. Nous pouvons borner le degré des polynômes r et dans notre cas ces polynômes nous permettent d'obtenir les polynômes $\Psi_{m,i}$ du Corollaire 6. Grâce à ces polynômes $\Psi_{m,i}$ et au lemme de Zippel-Schwartz, voir Lemme 1, nous pouvons obtenir un énoncé probabiliste sur les spécialisations conservant l'indécomposabilité, voir [15].

Chapitre 5

Algorithmes de décomposition

Ce chapitre traite de la décomposition telle qu'elle a été présentée au Chapitre 2. Dans le Chapitre 2 toutes les notions ont été présentées en prenant $\mathbb{C}$ comme corps de base. Cependant les résultats restent valables pour des corps plus généraux.
Dans tout ce chapitre, lorsque nous parlerons d'un corps, cela signifiera un corps pour lequel les résultats du Chapitre 2 sont vrais. Cela permettra d'alléger la présentation des résultats. Toutefois, les énoncés des théorèmes seront tous donnés avec les hypothèses adéquates sur le corps.
Nous rappelons que $F \in \mathbb{K}(X_1, \ldots, X_n)$ est décomposable lorsqu'il existe $u \in \mathbb{K}(T)$ de degré supérieur ou égal à 2 et $H \in \mathbb{K}(X_1, \ldots, X_n)$ tels que $F = u(H)$. L'entier n est toujours supposé supérieur ou égal à 2, sauf mention explicite du contraire.

D'autres notions de décomposition existent : par exemple pour $F(X, Y) \in \mathbb{K}[X, Y]$ nous pouvons chercher à écrire F sous la forme $F = G(H_1, H_2)$ où $G, H_1, H_2 \in \mathbb{K}[X, Y]$. Ce type de décomposition n'est pas étudié dans ce mémoire. Le lecteur intéressé par ce type de décomposition pourra consulter par exemple les travaux de Faugère, Perret et von zur Gathen [51, 52, 53], pour d'autres types de décomposition voir [66, 67, 84, 145, 146].

5.1 Modèle de complexité

Dans ce chapitre les résultats de complexité seront donnés, sauf mention du contraire pour la complexité arithmétique. Cela signifie que nous comptons le nombre d'opérations $+, -, \div, \times$ dans le corps de base et que chacune de ces opérations a le même coût.

On suppose de plus que le degré d tend vers l'infini mais que le nombre de variables n est fixé.

On dira qu'un algorithme est *quasi-optimal* lorsque nous pouvons l'effectuer avec $\tilde{\mathcal{O}}(N)$ opérations arithmétiques dans le corps de base, où N est la taille de l'entrée. Pour une définition de $\tilde{\mathcal{O}}$ on peut consulter le livre de von sur Gathen et Gerhard [65]. Cette notation a pour but de supprimer les facteurs logarithmiques dans les $\mathcal{O}$.

Nous supposerons que nous pouvons multiplier deux polynômes d'une variable de

degré d représentés de manière dense avec $\tilde{\mathcal{O}}(d)$ opérations arithmétiques, voir [65].

Nous supposerons aussi que nous pouvons multiplier deux matrices de taille $n \times n$ avec $\tilde{\mathcal{O}}(n^\theta)$ opérations, où θ désigne l'exposant de l'algèbre linéaire. Nous rappelons que nous pouvons supposer $2 \leq \theta \leq 2,36$. Nous utiliserons aussi le fait que nous pouvons calculer la base du noyau d'une matrice $m \times d$ où $d \leq m$ avec $\tilde{\mathcal{O}}(md^{\theta-1})$ opérations, voir le livre de Bini et Pan [10].

Dans [92], Lecerf a donné un algorithme probabiliste (resp. déterministe) pour la factorisation rationnelle d'un polynôme de degré d en $n \geq 3$ variables. Cet algorithme s'effectue en $\tilde{\mathcal{O}}(d^n)$ opérations (reps. $\tilde{\mathcal{O}}(d^{n+\theta-1})$). Nous remarquons donc que cet algorithme est quasi-optimal dans le cas probabiliste. Lorsque $n = 2$, nous pouvons calculer la factorisation rationnelle d'un polynôme de degré d de manière probabiliste avec $\tilde{\mathcal{O}}(d^3)$ opérations et de manière déterministe en $\tilde{\mathcal{O}}(d^{\theta+1})$, voir [19, 91, 92].

5.2 État de l'art

Dans ce chapitre nous allons présenter différents algorithmes développés pour décomposer des fractions rationnelles en plusieurs variables. La recherche et la mise au point d'algorithmes pour décomposer des polynômes ou des fractions rationnelles ne sont pas nouvelle.

Les algorithmes de décomposition fonctionnent toujours ainsi :

Méthode générale de décomposition
Entrée : $F \in \mathbb{K}(X_1, \ldots, X_n)$,
Sorties : $u \in \mathbb{K}(T)$, $H \in \mathbb{K}(X_1, \ldots, X_n)$, s'ils existent, tels que $F = u(H)$ et $\deg(u) \geq 2$.

1. Calculer H.
2. Calculer u.

Dans ce cours nous souhaitons obtenir H indécomposable. En effet, une fois H indécomposable obtenu, calculer une décomposition totale de F signifierait alors calculer aussi la décomposition de u. Comme dans ce cours nous nous concentrons sur les fractions rationnelles en plusieurs variables, et que u n'en possède qu'une seule, pour nous "décomposer" signifie donc trouver $H \in \mathbb{K}(X_1, \ldots, X_n)$ indécomposable et $u \in \mathbb{K}(T)$. Toutefois, nous verrons plus bas qu'il existe des algorithmes de décomposition pour les fractions rationnelles d'une seule variable.

Dans la méthode générale la difficulté réside dans la première étape : le calcul de H. En effet, une fois H connu, en écrivant $F = u(H)$ nous obtenons un système *linéaire* où les inconnues sont les coefficients de u. Cette méthode a une complexité en $\tilde{\mathcal{O}}(d^{n+\theta-1})$, où d est le degré de F. En adaptant une méthode proposée par Zippel, voir [150], nous obtenons une méthode plus efficace. Cette méthode utilise un approximant de Padé. Voici cette approche :

Calcul de u connaissant F et H
Entrées : $F, H \in \mathbb{K}(X_1, \ldots, X_n)$, où $\deg F = \deg_{X_n}(F)$,
Sortie : $u \in \mathbb{K}(T)$, s'il existe tel que $F = u(H)$.

1. $d_u := \deg(F)/\deg(H)$.
2. Calculer $\overline{F}(X) = F(0, \ldots, 0, X)$ et $\overline{H}(X) = H(0, \ldots, 0, X)$.
3. Calculer $h \in \mathbb{K}[[X]]$ tel que $\overline{H}(h) = X \mod X^{2d_u+1}$.
4. Calculer $U = \overline{F}(h) \mod X^{2d_u+1}$.
5. Calculer u un $(d_u + 1; d_u)$ approximant de Padé de U.
6. Rendre u.

L'idée de cette méthode est de calculer un inverse h pour la composition de $\overline{H}$. Comme $\overline{F} = u(\overline{H})$ on obtient $\overline{F}(h) = u\big(\overline{H}(h)\big) = u$.

Une étude simple de complexité, voir [30], montre que cette méthode donne u, lorsqu'il existe, en $\tilde{\mathcal{O}}(d^n)$ opérations. Voilà pourquoi cette méthode est plus efficace.

Pour les polynômes, le problème pratique de la décomposition a été très étudié et différents algorithmes existent, voir [2, 7, 46, 86, 63, 64]. Nous pouvons dire que la situation est bien comprise, car du point de vue de la complexité il existe un algorithme quasi-optimal dû à von zur Gathen [63].

Pour les fractions rationnelles, il existe aussi diverses méthodes. Zippel a donné un algorithme de décomposition pour les fractions rationnelles en une variable dans [150]. Cet algorithme a une complexité polynomiale. Avec les algorithmes de factorisation actuels cet algorithme peut s'effectuer en $\tilde{\mathcal{O}}(d^{2\theta+2})$. En effet, l'étape la plus coûteuse de cette approche est le calcul de la factorisation d'un polynôme en deux variables de degré d^2.
Dans les années 90, les algorithmes de factorisation étaient bien moins performants. Ainsi, la décomposition des fractions rationnelles avait une complexité polynomiale mais était réputée infaisable en pratique. Cela a conduit à l'étude d'algorithmes de complexité exponentielle mais rapides en pratique. Dans [3], Alonsso, Gutierrez et Recio proposent deux méthodes dans le cas d'une variable. Ces méthodes sont généralisées au cas de plusieurs variables par Gutierrez, Rubio, Sevilla dans [74]. Voici comment fonctionnent ces méthodes :

La première méthode est basée sur le Lemme 2 du Chapitre 2. En effet, ce lemme implique que si F_1/F_2 se décompose en $u(H_1/H_2)$ alors on peut considérer H_1 et H_2 comme étant des facteurs respectifs de F_1 et F_2. L'algorithme consiste alors à factoriser F_1 et F_2 et tester tous les facteurs possibles. C'est à dire pour chaque facteur f_i de F_i on cherche s'il existe u tel que $F_1/F_2 = u(f_1/f_2)$. Cet algorithme a une complexité exponentielle car nous testons a priori tous les facteurs des F_i, même les facteurs réductibles.

La deuxième méthode est basée sur le résultat suivant, voir e.g. [3, 134] :

Théorème 27. *Soit $F_1/F_2 \in \mathbb{K}(X_1, \ldots, X_n)$. On a l'équivalence entre :*

1. *Il existe* $H_1/H_2 \in \mathbb{K}(X_1, \ldots, X_n)$ *tel que* $F_1/F_2 = u(H_1/H_2)$.
2. $\hat{H}(\underline{X}, \underline{Y}) = H_2(\underline{Y})H_1(\underline{X}) - H_1(\underline{Y})H_2(\underline{X})$ *divise* $\hat{F}(\underline{X}, \underline{Y}) = F_2(\underline{Y})F_1(\underline{X}) - F_1(\underline{Y})F_2(\underline{X})$, *où* $\underline{X} = X_1, \ldots, X_n$, *et* $\underline{Y} = Y_1, \ldots, Y_n$.

Les polynômes du type $F_2(\underline{Y})F_1(\underline{X}) - F_1(\underline{Y})F_2(\underline{X})$ sont parfois appelés polynômes à variables presque séparées. L'étude de ce type de polynômes est classique, voir [57, 122, 135, 56].

Nous pouvons considérer ce théorème comme l'étude de la factorisation du polynôme $\lambda F_1 - \mu F_2$ où $\lambda = F_2(\underline{Y})$ et $\mu = F_1(\underline{Y})$. Nous avions déjà vu au Chapitre 2 que le polynôme $\lambda F_1 - \mu F_2$ est lié à la décomposition de F_1/F_2.

On en déduit l'algorithme suivant :

Décomposition via les polynômes à variables presque séparées
Entrée : $F = F_1/F_2 \in \mathbb{K}(X_1, \ldots, X_n)$.
Sorties : $u \in \mathbb{K}(T)$, $H = H_1/H_2 \in \mathbb{K}(X_1, \ldots, X_n)$ s'ils existent tels que $F = u(H)$.

1. Factoriser $\hat{F}(\underline{X}, \underline{Y})$.
2. Pour chaque facteur f_i de $\hat{F}$, tester s'il existe H tel que $f_i = \hat{H}$.
3. Calculer u.

L'étape 2 peut se faire en résolvant un système linéaire, voir l'article [74] de Gutierrez, Rubio, Sevilla. Dans le cas d'une seule variable nous pouvons utiliser une astuce développée spécialement pour cela par Ayad et Fleischmann [6]. Cette étape n'est pas la plus coûteuse. Là encore, le fait que nous testions tous les facteurs de $\hat{F}$ donne une complexité exponentielle.

Dans le cas où nous nous avons deux variables ou plus, nous pouvons obtenir un algorithme de complexité polynomiale en effectuant une modification mineure de cet algorithme. En effet, nous avons le résultat suivant, voir [30] :

Théorème 28. *Soit* $F_1/F_2 \in \mathbb{K}(X_1, \ldots, X_n)$. *S'il existe* $u \in \mathbb{K}(T)$ *de degré supérieur ou égal à 2 et* $H_1/H_2 \in \mathbb{K}(X_1, \ldots, X_n)$ *une fraction rationnelle indécomposable telle que* $F_1/F_2 = u(H_1/H_2)$ *alors les facteurs irréductibles de* $\hat{F}$ *de degré minimum en* $\underline{X}$ *sont du type*

$$\mathcal{H}(\underline{X}, \underline{Y}) = H_1(\underline{X})G_2(\underline{Y}) - H_2(\underline{X})G_1(\underline{Y}),$$

où $G_1/G_2 \in \mathbb{K}(Y_1, \ldots, Y_n)$ *est une fraction rationnelle indécomposable telle que* $H_1/H_2 = w(G_1/G_2)$, *où* $w \in \mathbb{K}(T)$ *et* $\deg(w) = 1$.

Ce théorème signifie donc qu'il suffit de chercher les facteurs irréductibles de plus petit degré en $\underline{X}$ dans l'algorithme Décomposition via les polynômes à variables presque séparées pour obtenir une décomposition. La complexité de l'algorithme devient alors polynomiale, plus précisément la complexité est en $\tilde{\mathcal{O}}(d^{2n+\theta-1})$, voir [30].

Cet algorithme n'est cependant pas le premier algorithme de complexité polynomiale pour décomposer des fractions rationnelles en plusieurs variables. Le premier a été donné

par Moulin Ollagnier dans [110].
Cet algorithme est une application du Théorème 8 page 21 du Chapitre 2 et n'est valable que lorsque le corps $\mathbb{K}$ est de caractéristique 0. En effet, certaines propriétés des dérivations sont perdues en caractéristique p.
L'idée est de considérer la dérivation jacobienne associée à F_1/F_2 et de considérer son noyau. En effet, avec les notations du Chapitre 2, si $F_1/F_2 = u(H_1/H_2)$ avec H_1/H_2 indécomposable alors $\mathbb{K}(X,Y)^{D_{F_1/F_2}} = \mathbb{K}(H_1/H_2)$. Calculer la décomposition de F_1/F_2 revient donc à calculer le noyau de la dérivation jacobienne D_{F_1/F_2}.
Nous présentons ici l'algorithme de Moulin Ollagnier dans le cas de deux variables afin de nous raccrocher à ce qui a été fait dans le Chapitre 2 et de simplifier certaines notations.

L'idée est donc de calculer $\mathbb{K}(X,Y)^{D_{F_1/F_2}}$. Or, si l'on calcule le noyau en écrivant simplement la définition, c'est à dire $D_{F_1/F_2}(H_1/H_2) = 0$ alors nous avons un système quadratique à résoudre. Plus précisément, nous savons que $\deg(H_i) \leq \deg(F_i) \leq d$, et la définition se réécrit : $D_{F_1/F_2}(H_1)H_2 - H_1 D_{F_1/F_2}(H_2) = 0$. Ainsi, si l'on souhaite calculer H_1/H_2 en utilisant directement la définition nous écrivons les polynômes H_i avec des coefficients indéterminés et nous résolvons un système quadratique en ces coefficients. Moulin Ollagnier propose l'approche suivante qui repose uniquement sur de l'algèbre linéaire :

Algorithme de Moulin Ollagnier
Entrée : $F = F_1/F_2 \in \mathbb{K}(X,Y)$ de degré d,
Sorties : $u \in \mathbb{K}(T)$, $H = H_1/H_2 \in \mathbb{K}(X,Y)$ s'ils existent tels que $F = u(H)$ et H indécomposable.

1. Calculer $\mathrm{cof}(F_1) = D_{F_1/F_2}(F_1)/F_1$.
2. Résoudre le système linéaire $D_{F_1/F_2}(H) = \mathrm{cof}(F_1)H$, où $H \in \mathbb{K}[X,Y]_{\leq d}$ et en déduire le degré de u.
3. Résoudre le système linéaire $D_{F_1/F_2}(H) = \dfrac{\mathrm{cof}(F_1)}{\deg(u)}H$, où $H \in \mathbb{K}[X,Y]_{\leq d}$ et en déduire H_1 et H_2.
4. Calculer u.

Expliquons à présent la correction de cet algorithme :
Comme H_1/H_2 est une intégrale première de D_{F_1/F_2}, H_1 et H_2 sont des polynômes de Darboux et $\mathrm{cof}(H_1) = \mathrm{cof}(H_2)$, voir Corollaire 2 page 16 du Chapitre 2. L'idée est alors de calculer dans un premier temps le cofacteur $\mathrm{cof}(H_i)$ pour ensuite calculer les polynômes H_i en résolvant le système linéaire $D_{F_1/F_2}(H) = \mathrm{cof}(H_i)H$, où $H \in \mathbb{K}[X,Y]_{\leq d}$.
Pour calculer le cofacteur $\mathrm{cof}(H_i)$ on procède de la manière suivante : On constate que nous avons la relation $\mathrm{cof}(F_i) = \deg(u)\mathrm{cof}(H_i)$ grâce au Lemme 2 et à la propriété d'additivité des cofacteurs. Ensuite, le cofacteur $\mathrm{cof}(F_i)$ s'obtient facilement en calculant $D_{F_1/F_2}(F_i)/F_i$. Puis le degré $\deg(u)$ s'obtient en considérant la dimension du noyau du système linéaire $D_{F_1/F_2}(H) = \mathrm{cof}(F_i)H$, où $H \in \mathbb{K}[X,Y]_{\leq d}$. En conclusion, nous pouvons calculer H_1/H_2 en effectuant uniquement de l'algèbre linéaire et la complexité de cette méthode est alors en $\tilde{\mathcal{O}}(d^{\theta n})$.

5.3 Décomposition et spectre

Lorsqu'une fraction rationnelle F_1/F_2 se décompose sous la forme $F_1/F_2 = u(H_1/H_2)$, la fraction H_1/H_2 est définie à une homographie près. Donc, dans ce qui suit nous allons chercher à calculer H_1/H_2 à une homographie près.

Nous avons vu au Lemme 2 que si F_1/F_2 se décompose sous la forme $F_1/F_2 = u\big(H_1/H_2\big)$ où $u = u_1/u_2$ alors pour $\lambda, \mu \in \mathbb{K}$ tels que $\deg(\lambda u_1 - \mu u_2) = \deg(u)$, nous obtenons :

$$\lambda F_1 - \mu F_2 = e \prod_{i=1}^{\deg(u)} (H_1 - t_i H_2),$$

où $e \in \mathbb{K}$ et les $t_i \in \overline{\mathbb{K}}$ sont les racines de $\lambda u_1 - \mu u_2$.
Nous remarquons donc qu'avec deux facteurs $H_1 - t_i H_2$, nous pouvons en déduire H_1/H_2 à une homographie près. Notre objectif est donc de faire en sorte d'avoir t_i dans $\mathbb{K} \setminus \sigma(H_1, H_2)$. Le fait d'avoir $t_i \in \mathbb{K}$ nous assure d'avoir une fraction à coefficients dans $\mathbb{K}$ et non pas dans $\overline{\mathbb{K}}$. Le fait d'avoir $t_i \notin \sigma(H_1, H_2)$ nous permet de reconnaitre facilement le facteur $H_1 - t_i H_2$: c'est un facteur irréductible de $\lambda F_1 - \mu F_2$.

Voici la méthode proposée dans [30] :

Décomposition probabiliste via le spectre
Entrées : $F = F_1/F_2 \in \mathbb{K}(X_1, \ldots, X_n)$, $(\underline{a}, \underline{b}) \in \mathbb{K}^{2n}$
Sorties : $u \in \mathbb{K}(T)$, $H = H_1/H_2 \in \mathbb{K}(X_1, \ldots, X_n)$ s'ils existent tels que $F = u(H)$ et H indécomposable.

1. Factoriser $\hat{F}(\underline{X}, \underline{a})$, et $\hat{F}(\underline{X}, \underline{b})$.
2. Soient $\mathcal{F}_a$ $\big($resp. $\mathcal{F}_b\big)$ un facteur irréductible de $\hat{F}(\underline{X}, \underline{a})$ $\big($resp. $\hat{F}(\underline{X}, \underline{b})\big)$ dans $\mathbb{K}[\underline{X}]$ de degré minimum. On pose $H = \mathcal{F}_a/\mathcal{F}_b$.
3. Calculer u.

Détaillons cet algorithme :
Remarquons avant tout chose que $\hat{F}(\underline{X}, \underline{a}) = F_2(\underline{a})F_1(\underline{X}) - F_1(\underline{a})F_2(\underline{X})$, c'est à dire nous considérons un polynôme du type $\lambda F_1 - \mu F_2$ avec $\lambda = F_2(\underline{a})$ et $\mu = F_1(\underline{a})$.
Voyons à présent pourquoi, lorsque F_1/F_2 est décomposable, cela implique qu'il existe une racine t_i dans $\mathbb{K}$.
Si $F_1/F_2 = (u_1/u_2)(H)$ avec $H = H_1/H_2 \in \mathbb{K}(\underline{X})$ alors nous avons

$$\frac{F_1(\underline{a})}{F_2(\underline{a})} = \frac{u_1\big(H(\underline{a})\big)}{u_2\big(H(\underline{a})\big)} \Rightarrow F_2(\underline{a})u_1\big(H(\underline{a})\big) - F_1(\underline{a})u_2\big(H(\underline{a})\big) = 0.$$

Comme $\underline{a} \in \mathbb{K}^n$ et $H \in \mathbb{K}(\underline{X})$, nous en déduisons que $H(\underline{a}) \in \mathbb{K}$ est une racine de $F_2(\underline{a})u_1(T) - F_1(\underline{a})u_2(T)$. Un facteur de $\hat{F}(\underline{X}, \underline{a})$ est donc $H_1 - H(\underline{a})H_2 \in \mathbb{K}[\underline{X}]$. Cela remplit donc le premier point de notre objectif.

Pour le deuxième point, il suffit de remarquer que l'ensemble des $\underline{a} \in \mathbb{K}^n$ tels que $H(\underline{a}) \in \sigma(H_1, H_2)$ est un fermé de Zariski. Nous obtenons alors le résultat suivant :

Théorème 29. *Soit $F = F_1/F_2 \in \mathbb{K}(X_1, \ldots, X_n)$ avec $\deg F = d$, et $(\underline{a}, \underline{b}) \in \mathbb{K}^{2n}$.*

Pour $\underline{a}, \underline{b}$ dans un ouvert de Zariski, l'algorithme Décomposition probabiliste via le spectre est correct. De plus :

1. *L'algorithme effectue deux factorisations de polynômes de degré d dans $\mathbb{K}[X_1, \ldots, X_n]$ et un calcul de u.*
2. *Lorsque nous pouvons utiliser l'algorithme de factorisation de Lecerf, l'algorithme effectue la factorisation d'un polynôme dans $\mathbb{K}[T]$ de degré d, plus un nombre d'opérations arithmétiques dans $\mathbb{K}$ de l'ordre de $\tilde{\mathcal{O}}(d^n)$ si $n \geq 3$, ou de l'ordre de $\tilde{\mathcal{O}}(d^3)$ si $n = 2$.*

Faisons quelques commentaires sur ce résultat :
Lorsque $n \geq 3$ cet algorithme est quasi-optimal.
L'algorithme obtenu est un algorithme probabiliste. Remarquons cependant qu'avec cette démarche, nous ne pouvons pas rendre de résultats faux. En effet, si la fraction H candidate n'est pas la bonne alors cela signifie que nous sommes dans une situation où par exemple $H(\underline{a}) \in \sigma(H_1, H_2)$. Le facteur $\mathcal{F}_a$ est donc de degré inférieur à celui de H. Donc, comme H est indécomposable, dans la dernière étape de l'algorithme il est impossible d'obtenir une fraction rationnelle u telle que $F = u(H)$.

Pour être sûr d'obtenir une solution avec cette approche il faut faire en sorte d'éviter le spectre de H. Comme celui-ci est fini en recommençant plusieurs fois l'approche probabiliste on obtient un algorithme déterministe. Le spectre de H ayant un cardinal inférieur à d^2 nous avons pu modifier l'algorithme probabiliste et démontrer :

Théorème 30. *Soit $F \in \mathbb{K}(X_1, \ldots, X_n)$ une fraction rationnelle de degré d. Si $\mathbb{K}$ est un corps ayant au moins $\max(d^2, \frac{3}{2}d^2 - 2d + 1)$ éléments, alors la décomposition $F = u(H)$, avec H indécomposable, peut se calculer de manière déterministe avec au plus $\mathcal{O}(d^2)$ factorisations absolues de polynômes de degré d, et au plus $\mathcal{O}(d^2)$ utilisation de l'algorithme calculant la fraction rationnelle u connaissant F et H.*
Lorsque nous pouvons utiliser l'algorithme de factorisation de Lecerf, cette méthode effectue la factorisation d'un polynôme dans $\mathbb{K}[T]$ de degré d, plus un nombre d'opérations arithmétiques dans $\mathbb{K}$ de l'ordre de $\tilde{\mathcal{O}}(d^{n+\theta+2})$ si $n \geq 3$ ou $\tilde{\mathcal{O}}(d^6)$ si $n = 2$.

Nous remarquons que cette méthode se compare favorablement à la méthode de Moulin Ollagnier et à la méthode utilisant les polynômes à variables presque séparées.

5.4 Décomposition via la méthode de Darboux

Le problème auquel nous devons faire face dans l'algorithme Décomposition probabiliste via le spectre vient du fait que les facteurs $H_1 - H(\underline{a})H_2$ et $H_1 - H(\underline{b})H_2$ de $\hat{F}(\underline{X}, \underline{a})$ et $\hat{F}(\underline{X}, \underline{b})$ ne sont pas nécessairement irréductibles. Ces facteurs peuvent donc se factoriser. Nous allons voir comment recombiner les facteurs irréductibles de $\hat{F}(\underline{X}, \underline{a})$ et de $\hat{F}(\underline{X}, \underline{b})$ afin de retrouver les polynômes $H_1 - H(\underline{a})H_2$ et $H_1 - H(\underline{b})H_2$.
Comme dans l'algorithme de Moulin Ollagnier, nous allons considérer la dérivation jacobienne D_{F_1/F_2} et chercher une intégrale première pour cette dérivation. En effet, les facteurs irréductibles des F_i sont des polynômes de Darboux pour D_{F_1/F_2} et à partir de

ces polynômes de Darboux nous allons pouvoir calculer une intégrale première rationnelle indécomposable. Contrairement à ce qui est fait dans l'algorithme de Moulin Ollagnier nous allons utiliser la méthode de Darboux pour trouver une intégrale première.

Nous donnons l'algorithme suivant dans le cas de deux variables afin de simplifier sa présentation. Cette approche se généralise en $n \geq 2$ variables, voir [31].

Décomposition déterministe via les polynômes de Darboux
Entrée : $F = F_1/F_2 \in \mathbb{K}(X, Y)$,
Sorties : $u \in \mathbb{K}(T)$, $H = H_1/H_2 \in \mathbb{K}(X, Y)$ s'ils existent tels que $F = u(H)$ et H indécomposable.

1. Prendre $(\underline{a}, \underline{b}) \in \mathbb{K}^{2n}$, et calculer $\hat{F}(\underline{X}, \underline{a})$ et $\hat{F}(\underline{X}, \underline{b})$.
2. Calculer les factorisations $\hat{F}(\underline{X}, \underline{a}) = \prod_{i=1}^{r_{\underline{a}}} F_{\underline{a},i}$ et $\hat{F}(\underline{X}, \underline{b}) = \prod_{j=1}^{r_{\underline{b}}} F_{\underline{b},i}$.
3. Calculer les cofacteurs $\Lambda_{\underline{a},i} = D_{F_1/F_2}(F_{\underline{a},i})/F_{\underline{a},i}$ et $\Lambda_{\underline{b},j} = D_{F_1/F_2}(F_{\underline{b},j})/F_{\underline{b},j}$.
4. Calculer une base échelonnée réduite de l'espace des solutions du système linéaire $\sum_{i=1}^{r_{\underline{a}}} e_i \Lambda_{\underline{a},i} - \sum_{j=1}^{r_{\underline{b}}} e_j \Lambda_{\underline{b},j} = 0$.
5. Parmi les vecteurs de la base obtenue prendre celui donnant une fraction rationnelle $\dfrac{\prod_{i=1}^{r_{\underline{a}}} F_{\underline{a},i}^{e_i}}{\prod_{j=1}^{r_{\underline{b}}} F_{\underline{b},i}^{e_j}}$ de degré minimum. On note H cette fraction rationnelle.
6. Calculer u.

Cet algorithme est donc une application de la méthode de Darboux dans un cas particulier. Cette particularité nous a permis de calculer facilement des polynômes de Darboux. En effet, lorsque nous considérons une dérivation quelconque, il est difficile de trouver des polynômes de Darboux. Par exemple, nous avons déjà vu au Chapitre 2 que nous ne savons pas comment borner a priori le degré de ces polynômes. Ici nous avons une dérivation jacobienne. Le calcul de polynômes de Darboux est donc aisé. Les polynômes F_1 et F_2 et leurs facteurs sont des polynômes de Darboux. Donc, dans ce cas, le calcul de polynômes de Darboux revient à factoriser les polynômes F_1 et F_2. On remarque d'ailleurs que si l'un des F_i est irréductible alors nous pouvons conclure automatiquement que F_1/F_2 est indécomposable.

Voyons maintenant pourquoi cette approche est avantageuse du point de vue de la complexité. Le système linéaire que nous avons à considérer possède $r_{\underline{a}} + r_{\underline{b}} \leq 2d$ inconnues. En effet, le nombre de facteurs de $\hat{F}(\underline{X}, \underline{a})$ est inférieur à d, de même pour $\hat{F}(\underline{X}, \underline{b})$. Lorsque nous utilisons l'algorithme de Moulin Ollagnier nous calculons H en résolvant un système linéaire qui possède $\mathcal{O}(d^n)$ inconnues. L'utilisation de la méthode de Darboux permet donc d'obtenir un système linéaire de taille plus petite que celui utilisé dans la méthode de Moulin Ollagnier.

Pour finir, comme nous l'avons vu à la Section 2.8 du Chapitre 2, la factorisation des polynômes peut s'effectuer à l'aide d'une méthode de recombinaison des facteurs via la dérivée logarithmique. Ici, nous considérons un problème de décomposition. C'est un problème de factorisation particulier car nous cherchons des facteurs du type $H_1 - t_i H_2$.

Donc nous avons utilisé une méthode de factorisation en utilisant une dérivation adaptée pour la recombinaison des facteurs.

L'algorithme Décomposition déterministe via les polynômes de Darboux a été présenté dans le cas de $n \geq 2$ variables dans [32]. Dans ce cas nous ne considérons plus une dérivation, mais une famille de dérivation provenant du critère jacobien. La difficulté de la preuve de cet algorithme réside alors dans l'étude de la structure de la base échelonnée réduite du système linéaire. En effet, un vecteur solution de ce système va nous donner une intégrale première mais il faut pouvoir garantir le fait que l'intégrale première calculée est bien indécomposable.

La complexité de cet algorithme est donnée par le théorème suivant :

Théorème 31. *Soit $F_1/F_2 \in \mathbb{Q}[\alpha](X_1, \ldots, X_n)$ une fraction rationnelle de degré d, où α est un nombre algébrique de degré r sur $\mathbb{Q}$.*
L'algorithme Décomposition déterministe via les polynômes de Darboux calcule de manière déterministe la décomposition de F_1/F_2.

1. *Cet algorithme effectue deux factorisations de polynômes de degré d, la résolution d'un système linéaire à coefficients dans $\mathbb{Q}$ de taille $\mathcal{O}(nrd^n) \times \mathcal{O}(d)$ et un calcul de u.*
2. *Si nous utilisons l'algorithme de factorisation de Lecerf alors cet algorithme nécessite 2 factorisations de polynômes d'une variable de degré d à coefficients dans $\mathbb{Q}[\alpha]$, plus un nombre d'opérations arithmétiques dans $\mathbb{Q}$ de l'ordre de $\tilde{\mathcal{O}}(rd^{n+\theta-1})$.*

Ce résultat signifie que cette méthode est plus performante que les autres méthodes déterministes présentées précédemment.

Dans [32], on trouve également un résultat de complexité de cette méthode en fonction du polytope de Newton de F_1 et de F_2. Cette méthode repose sur l'algorithme de factorisation de Berthomieu-Lercerf [9].

Un résultat de *complexité binaire* a aussi été donné. En effet, l'algorithme précédent est donné uniquement dans le cas d'un corps de nombres. Nous savons que dans ce genre de situations la taille des résultats intermédiaires peut augmenter de telle sorte que la complexité arithmétique ne mesure plus la vitesse de l'algorithme. Dans [32] est donc aussi considéré la situation où F_1 et F_2 sont des polynômes dans $\mathbb{Z}[X_1, \ldots, X_n]$ dont les coefficients sont de hauteur $\mathcal{H}$. Dans ce cas l'algorithme Décomposition déterministe via les polynômes de Darboux peut s'effectuer en $\tilde{\mathcal{O}}\big(nd^{n+\theta-1}\log(\mathcal{H})\big)$ opérations binaires. Ce résultat se compare toujours avantageusement à la méthode de Moulin Ollagnier qui utilise $\tilde{\mathcal{O}}(d^{n\theta})$ opérations arithmétiques.

5.5 Application au théorème de Lüroth

Le théorème de Lüroth étendu (l'énoncé est rappellé en appendice page 98) a déjà été rencontré lors de la preuve de la Proposition 5 page 19. Nous avons donc utilisé de

manière théorique ce résultat. Ici, nous allons voir comment calculer pratiquement un générateur donné par le théorème de Lüroth étendu.
Le calcul d'un générateur "à la Lüroth" permet entre autre de calculer les corps intermédiaires de degré de transcendance 1 d'une extension du type $\mathbb{K}(\mathsf{f}_1,\ldots,\mathsf{f}_m) \subset \mathbb{K}(X_1,\ldots,X_n)$, où $trdeg_{\mathbb{K}}\mathbb{K}(\mathsf{f}_1,\ldots,\mathsf{f}_m) = 1$. En effet, dans un premier temps nous calculons un générateur à la Lüroth de $\mathbb{K}(\mathsf{f}_1,\ldots,\mathsf{f}_m)$, et cela donne $\mathbb{K}(\mathsf{f}_1,\ldots,\mathsf{f}_m) = \mathbb{K}(\mathsf{h})$. Puis, dans un deuxième temps la décomposition de h donne les extensions intermédiaires entre $\mathbb{K}(\mathsf{h})$ et $\mathbb{K}(X_1,\ldots,X_n)$. En effet, si $\mathsf{h} = u(g)$ avec $\deg(u) \geq 2$ et $g \in \mathbb{K}(X_1,\ldots,X_n)$ est non nécessairement indécomposable, alors $\mathbb{K}(\mathsf{h}) \subsetneq \mathbb{K}(g) \subsetneq \mathbb{K}(X_1,\ldots,X_n)$. Il y a une bijection entre les extensions intermédiaires de $\mathbb{K}(\mathsf{h})$ et les décompositions de h. Pour plus de détails à ce propos, le lecteur peut consulter l'article [74] de Gutierrez, Rubio et Sevilla.

Sederberg [138] a donné une méthode pour calculer un générateur à la Lüroth dans le cas d'une variable, cette approche peut se généraliser en plusieurs variables, voir [30] :

Algorithme de Sederberg généralisé
Entrées : $F = F_1/F_2, G = G_1/G_2 \in \mathbb{K}(X_1,\ldots,X_n)$,$(\underline{a},\underline{b}) \in \mathbb{K}^{2n}$,
Sortie : $H = H_1/H_2 \in \mathbb{K}(X_1,\ldots,X_n)$ s'il existe tel que $\mathbb{K}(F,G) = \mathbb{K}(H)$.

1. Prendre $\underline{a} \in \mathbb{K}^n$, et calculer $H_{\underline{a}} = pgcd\big(\hat{F}(\underline{X},\underline{a}),\, \hat{G}(\underline{X},\underline{a})\big)$.
2. Si $H_{\underline{a}}$ est constant alors rendre "Pas de générateurs à la Lüroth".
3. Prendre $\underline{b} \in \mathbb{K}^n$, et calculer $H_{\underline{b}} = pgcd\big(\hat{F}(\underline{X},\underline{b}),\, \hat{G}(\underline{X},\underline{b})\big)$.
4. Si $H_{\underline{b}}$ est constant alors rendre "Pas de générateurs à la Lüroth".
5. Rendre $H = H_{\underline{a}}/H_{\underline{b}}$.

Nous avons présenté ici l'algorithme lorsque nous avons deux générateurs. Lorsque nous considérons un corps engendré avec m générateurs alors nous appliquons $m-1$ fois cet algorithme. C'est à dire pour calculer un générateur de $\mathbb{K}(\mathsf{f}_1,\ldots,\mathsf{f}_m)$ nous calculons un générateur h de $\mathbb{K}(\mathsf{f}_1,\mathsf{f}_2)$. Ensuite nous recommençons ce procédé avec $\mathbb{K}(\mathsf{f}_1,\ldots,\mathsf{f}_m) = \mathbb{K}(h,\mathsf{f}_3,\ldots,\mathsf{f}_m)$. Nous appelons aussi cette méthode Algorithme de Sederberg généralisé par abus de langage.

L'idée derrière l'Algorithme de Sederberg généralisé est la suivante : Comme la décomposition est un problème de factorisation particulier, le calcul d'un générateur à la Lüroth est un calcul de pgcd.
En effet, si $\mathbb{K}(F,G) = \mathbb{K}(H)$ alors $F = u(H)$ et $G = v(H)$. Donc en appliquant le Théorème 27 page 71, nous voyons que $\hat{F}(\underline{X},\underline{a})$ et $\hat{G}(\underline{X},\underline{a})$ ont comme facteur commun $\hat{H}(\underline{X},\underline{a})$. On montre alors que sous des hypothèses de généricité $\hat{H}(\underline{X},\underline{a})$ est le pgcd de $\hat{F}(\underline{X},\underline{a})$ et de $\hat{G}(\underline{X},\underline{a})$.

Nous avons obtenu le résultat de complexité suivant :

Théorème 32. *Soient $\mathsf{f}_1,\ldots,\mathsf{f}_m \in \mathbb{K}(X_1,\ldots,X_n)$, m fractions rationnelles de degré au plus d et $(\underline{z}) \in \mathbb{K}^{2mn}$.*

Pour $\underline{z}$ dans un ouvert de Zariski, l'Algorithme de Sederberg généralisé est correct. De plus :

1. *L'algorithme effectue* $2m$ *calculs de pgcd de polynômes dans* $\mathbb{K}[X_1, \ldots, X_n]$ *de degré au plus* d.
2. *Si* $\mathbb{K}$ *contient au moins* $(4d+2)d$ *éléments alors l'exécution de cet algorithme peut s'effectuer avec* $\tilde{\mathcal{O}}(md^n)$ *opérations arithmétiques.*

Ce résultat montre que l'algorithme proposé est quasi-optimal.

Il existe aussi une autre approche :
L'idée est la suivante, si $\mathbb{K}(F,G) = \mathbb{K}(H)$ alors $F = u(H)$ et $G = v(H)$. Nous décomposons alors F de la manière suivante : $F = u_0(H_0)$ où H_0 est indécomposable. Puis nous cherchons s'il existe $v_0 \in \mathbb{K}(T)$ tel que $G = v_0(H_0)$. Si c'est le cas alors notre problème est ramené à un problème en une variable. En effet, nous considérons $w_0 \in \mathbb{K}(T)$ tel que $\mathbb{K}(u_0, v_0) = \mathbb{K}(w_0)$, et nous avons $\mathbb{K}(F,G) = \mathbb{K}\big(w_0(H_0)\big)$.
Il est à noter que cette approche permet de rendre aussi u et v tel que $F = u(H)$ et $G = v(H)$, pour plus de détails voir [30].

5.6 Un test d'indécomposabilité

Parfois, un test d'indécomposabilité permet d'éviter l'utilisation d'un algorithme de décomposition. Nous allons présenter ici un test d'indécomposabilité basé uniquement sur le polytope de Newton.
Nous rappelons la relation $\deg\big(u(H)\big) = \deg(u)\deg(H)$. Donc si $F \in \mathbb{K}(X_1, \ldots, X_n)$ est tel que $\deg(F)$ est premier alors F est indécomposable. Nous allons généraliser cette remarque.
Supposons F_1/F_2 décomposable sous la forme $u(H_1/H_2)$. Dans ce cas le Lemme 2 nous fournit une factorisation du type :

$$F_1 - \Lambda F_2 = \prod_{i=1}^{\deg(u)} (H_1 - t_i H_2),$$

où Λ désigne une nouvelle variable, et $t_i \in \overline{\mathbb{K}(\Lambda)}$. En considérant le polytope de Newton pour chacun des membres de cette égalité et en appliquant le lemme d'Ostrowski au membre de droite et il vient :

$$\mathcal{N}(F_1 - \Lambda F_2) = \deg(u)\mathcal{N}(H_1 - \Lambda H_2).$$

Cela signifie que si F_1/F_2 est décomposable alors les coordonnées des sommets du polytope de Newton de $F_1 - \Lambda F_2$ ont un facteur commun. On en déduit :

Lemme 6. *Soit* $F_1/F_2 \in \mathbb{K}(X_1, \ldots, X_n)$ *une fraction rationnelle de degré* d, *où* $\mathbb{K}$ *est un corps de caractéristique* $p = 0$ *ou* $p > d$. *Soient* $(i_1^{(1)}, \ldots, i_n^{(1)}), \ldots, (i_1^{(k)}, \ldots, i_n^{(k)})$ *les coordonnées des sommets du polytope de Newton de* $F_1 - \Lambda F_2$, *où* Λ *est une nouvelle variable.*
Si $pgcd(i_1^{(1)}, \ldots, i_n^{(1)}, \ldots, i_1^{(k)}, \ldots, i_n^{(k)}) = 1$ *alors* F_1/F_2 *est indécomposable.*

La relation obtenue entre le polytope de Newton de F et le polytope de Newton de H a été utilisée dans [37] pour affiner la version effective du théorème d'Ostrowski pour la décomposition.

5.7 Prolongement

Nous pouvons noter la chose suivante : notre stratégie et notre cadre d'étude de la décomposition sont liés au théorème de Lüroth. On peut donc souhaiter étudier des généralisations du théorème de Lüroth.
La première étape vers une généralisation du théorème de Lüroth est donnée par le théorème de Castelnuovo. Ce théorème affirme que lorsque $trdeg_{\mathbb{C}}\mathbb{K} = 2$ alors $\mathbb{K} = \mathbb{C}(H_1, H_2)$. Ce résultat n'est plus valable lorsque le corps de base est $\mathbb{R}$ ou $\mathbb{Q}$. De plus, une preuve constructive du théorème de Castelnuovo ne semble pas connue. Pour plus de détails bibliographiques nous pouvons consulter le livre de Schinzel [135]. Il est donc naturel de se demander : existe-t-il un algorithme permettant de calculer les générateurs donnés par le théorème de Castelnuovo ?

Chapitre 6

Calcul d'intégrales premières et des polynômes de Darboux

Dans ce chapitre nous allons présenter des méthodes "efficaces" pour le calcul d'intégrales premières rationnelles et des polynômes de Darboux de degrés bornés. Ce chapitre est une synthèse des articles : [31], [33], [18].

6.1 Les théorèmes de Darboux et Jouanolou dans le cas creux

Nous avons vu au Chapitre 2 les théorèmes de Darboux et de Jouanolou. Ceux-ci nous permettent d'assurer l'existence d'une intégrale première Darbouxienne ou rationnelle lorsque nous avons suffisamment de polynômes de Darboux. Nous avons démontré ces deux théorèmes dans le cas de deux variables. La stratégie de preuve était la suivante : nous avons montré que les cofacteurs d'une dérivation de degré k ont nécessairement un degré au plus égal à $k-1$. Donc tous les cofacteurs appartiennent à $\mathbb{C}[X,Y]_{\leq k-1}$ qui est un espace vectoriel de dimension $k(k+1)/2$. Ainsi, $k(k+1)/2+1$ cofacteurs sont nécessairement liés et donnent naissance à une intégrale première Darbouxienne ce qui montre le théorème de Darboux. Pour le théorème de Jouanolou nous avons vu que $k(k+1)/2+2$ cofacteurs donnent deux relations de dépendance linéaire entre les cofacteurs et que cela suffit à construire une intégrale première rationnelle.
Ainsi, les bornes obtenues proviennent toutes deux de la dimension de l'espace vectoriel dans lequel vivent les cofacteurs.

Les théorèmes de Darboux et Jouanolou ont été donnés en fonction du degré k de la dérivation étudiée. Ces théorèmes possèdent un énoncé équivalent dans le cas creux, voir [33]. Cela signifie que nous pouvons exprimer la borne sur le nombre de polynômes de Darboux suffisant pour construire une intégrale première en fonction de la taille d'un polytope de Newton associé à la dérivation.
L'idée de la preuve est la même que celle utilisée dans le cas dense. Tout d'abord, nous identifions un espace vectoriel contenant tous les cofacteurs, puis nous calculons la dimension de cet espace vectoriel. Ensuite, les arguments de dimension utilisés dans le cas dense restent les mêmes.

La stratégie développée est alors la suivante : au lieu de considérer uniquement le degré total, nous considérons des degrés avec poids. Ces degrés permettent alors de contrôler les différentes faces d'un polytope. Nous montrons alors que tous les polytopes de Newton des cofacteurs sont inclus dans un même polytope. Plus précisément on montre :

Théorème 33. *Soit* $D = \sum_{i=1}^{n} A_i(X_1, \ldots, X_n)\partial_{X_i}$ *une dérivation. Soit* $(x_1, \ldots, x_n)$ *un point générique de* $\mathbb{C}^n$ *et* N_D *le polytope suivant* $N_D = \mathcal{N}\Big(\sum_{i=1}^{n} x_i \frac{A_i}{X_i}\Big)$.
Soit B *le nombre de points à coordonnées entières dans* $N_D \cap \mathbb{N}^n$, *alors*

1. *Soit* G *un cofacteur d'un polynôme de Darboux pour la dérivation* D, *alors* $\mathcal{N}(G) \subset N_D$.
2. *Si* D *possède* $B+1$ *polynômes de Darboux irréductibles et distincts alors* D *possède une intégrale première Darbouxienne non triviale. De plus, cette borne est optimale.*
3. *Si* D *possède* $B+n$ *polynômes de Darboux irréductibles et distincts alors* D *possède une intégrale première rationnelle non triviale. De plus, cette borne est optimale.*

Dans ce théorème la division par X_i dans A_i/X_i correspond à la chute du degré lorsque nous dérivons. Plus précisément, cela correspond au -1 lorsque nous écrivons $\deg(G) \leq k-1$, pour un cofacteur G. La somme $\sum_{i=1}^{n} x_i \frac{A_i}{X_i}$ avec $(x_1, \ldots, x_n)$ générique est là pour prendre en compte tous les polytopes de Newton des A_i.

Nous pouvons remarquer que dans le cas dense nous retrouvons l'énoncé classique. Remarquons aussi qu'un changement linéaire de coordonnées casse la structure du polytope N_D.

Lorsque nous considérons une dérivation du type $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$ où A et B sont du type $c_{e,e}X^eY^e + c_{e-1,e}X^{e-1}Y^e + c_{e,e-1}X^eY^{e-1} + c_{0,0}$, alors $B = 3e+2$ et le degré de la dérivation est $k = 2e$. Dans cette situation, l'utilisation de la borne dense donnerait une borne quadratique en le degré de la dérivation , i.e. $2e(2e+1)/2$. En utilisant la borne donnée par le théorème précédent nous obtenons une borne linéaire, i.e. $3e+4$. Ci-dessous, voir Figure 6.1, nous avons représenté le polytope de Newton N de A et de B ainsi que N_D lorsque $e = 3$.

A présent, nous allons expliquer pourquoi les bornes sont optimales.

L'optimalité de la borne dans le cas des intégrales premières Darbouxiennes découle de l'exemple suivant.
Considérons la dérivation X_iX_{i+1},

$$D_{X_iX_{i+1}} = \Big(\sum_{i=1}^{n-1} X_iX_{i+1}\partial_{X_i}\Big) + X_nX_1\partial_{X_n}.$$

Il a été montré dans [112] que les seuls polynômes de Darboux irréductibles de D sont les variables X_i. Ainsi une intégrale première Darbouxienne si elle existe est du type

FIGURE 6.1 – Représentation des polytopes N et $N_D \cap \mathbb{N}^2$.

$c\prod_i X_i^{\lambda_i}$, où $c, \lambda_i \in \mathbb{C}$. Un calcul direct montre alors que le seul cas possible apparaît lorsque tous les λ_i sont nuls. Ainsi, il n'existe pas d'intégrale première Darbouxienne non-triviale pour $D_{X_iX_{i+1}}$.
Pour la dérivation $D_{X_iX_{i+1}}$ nous avons $B = n$. Donc nous ne pouvons pas améliorer la borne donnée dans le théorème puisqu'il existe une dérivation possédant B polynômes de Darboux irréductibles et ne possédant pas d'intégrale première Darbouxienne.

La borne obtenue dans le cas des intégrales premières rationnelles est, elle aussi optimale.
En effet, il suffit de considérer la situation suivante : Soient $p(X_1) \in \mathbb{Z}[X_1]$ un polynôme irréductible de degré k, α une racine de p et $\xi_2, \ldots, \xi_n$ des nombres complexes distincts tels que $p'(\alpha), \xi_2, \ldots, \xi_n$ soient $\mathbb{Z}$-indépendants. On note alors D la dérivation suivante : $D = p(X_1)\partial_{X_1} + \xi_2 X_2 \partial_{X_2} + \cdots + \xi_n X_n \partial_{X_n}$.
Cette dérivation ne possède pas d'intégrales premières rationnelles d'après la Proposition 14 page 38 qui se généralise sans difficultés au cas de n variables.
Ici, $N_D \cap \mathbb{N}^n$ correspond au polytope de Newton des polynômes en une variable X_1 et de degré inférieur à $k-1$. Donc $B = k$.
De plus, $(X_1 - \alpha)$, $(X_1 - \alpha_2), \ldots, (X_1 - \alpha_d)$ où α_i sont les racines de p, et $X_2, \ldots, X_n$ sont des polynômes de Darboux irréductibles et distincts. Donc nous avons $d + n - 1$ polynômes de Darboux irréductibles et distincts.

Il en découle que nous ne pouvons pas améliorer la borne donnée dans le Théorème 33 puisqu'il existe une dérivation sans intégrales premières rationnelles et qui possède $B + n - 1$ polynômes de Darboux irréductibles et distincts.

Nous venons d'affiner les bornes classiques des théorèmes de Darboux et de Jouanolou en prenant en compte la structure avec laquelle est représentée la dérivation. Comme nous l'avons déjà fait dans le Chapitre 3, posons nous à présent la question de savoir si l'on peut obtenir le même genre de résultats en considérant des polynômes lacunaires ou bien donnés par des programmes d'évaluation. C'est à dire, peut on donner une borne pour le théorème de Darboux et de Jouanolou en fonction de la taille des polynômes A_i dans ces représentations ?

Comme précédemment la réponse est non. En effet, soit

$$D = (X^d - 1)\partial_X - (dX^{d-1}Y + 1)\partial_Y.$$

Cette dérivation a comme intégrale première $f(X,Y) = Y(X^d - 1) + X$, et $X - \omega^i$ comme polynômes de Darboux irréductibles, où ω est une racine d-ième de l'unité et $i = 1, \ldots, d$. La dérivation possède 4 termes et les entiers utilisés pour représenter cette dérivation sont de taille $\log(d)$. Or avec 4 ou $\log(d)$ polynômes du type $X - \omega^i$ nous ne pouvons pas construire d'intégrale première pour D.
Nous pouvons remarquer que le contre-exemple est une fois de plus fabriqué à partir du même polynôme $f(X,Y) = Y(X^d - 1) + X$ provenant de l'étude du spectre faite par Lorenzini.

6.2 Le retour du spectre

Nous avions utilisé le théorème de Jouanolou pour borner l'ordre total de réductibilité dans le Théorème 20 page 59. A présent, nous avons une version creuse du théorème de Jouanolou cela implique donc une version creuse pour le Théorème 20. On obtient avec les notations précédentes, voir [34] :

Théorème 34. *Soit D une dérivation et $F_1/F_2 \in \mathbb{C}(X,Y)$ une intégrale première rationnelle indécomposable de D. Soit B le nombre de points à coordonnées entières dans $N_D \cap \mathbb{N}^2$. Nous avons alors :*

$$\rho(F_1, F_2) < B + 2.$$

En considérant la dérivation $D = (X^d - 1)\partial_X - (dX^{d-1}Y + 1)\partial_Y$ qui a pour intégrale première $f(X,Y) = Y(X^d - 1) + X$, nous remarquons que cette borne est optimale puisque dans ce cas nous avons $\rho(f, 1) = d + 1$ et $B = d$.

6.3 Complexité des méthodes utilisant la courbe extatique

Nous présentons dans cette section une synthèse de l'article [31] dans lequel nous donnons des résultats de complexité obtenus à l'aide de la courbe extatique. Nous supposerons dans cette section les polynômes A et B à coefficients dans $\mathbb{Z}$ cela nous permettra de donner des résultats pour la complexité binaire.

6.3.1 Calcul des polynômes de Darboux de degrés bornés

Nous avons introduit la courbe extatique et présenté ses propriétés au Chapitre 2. Un algorithme de calcul des polynômes de Darboux de degrés bornés s'en déduit aisément. Voici cet algorithme :

Algorithme Lagutinskii-Pereira
Entrées : $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$, et $N \in \mathbb{N}$.
Sorties : S l'ensemble de tous les polynômes de Darboux de D absolument irréductibles et de degré $\leq N$ ou "∞ de Darboux".

1. $S = \{\}$.

2. Calculer $\mathcal{E}_N(D)$.
3. Si $\mathcal{E}_N(D) = 0$ alors Rendre "∞ de Darboux" sinon aller à l'étape 4.
4. Calculer $f_1, \ldots, f_m$ les facteurs absolument irréductibles de degré $\leq N$ de $\mathcal{E}_N(D)$.
5. Pour $i := 1, \ldots, m$ faire : Si $\gcd(f_i, D(f_i)) = f_i$ alors ajouter f_i à S.
6. Rendre S.

Nous rappelons qu'à l'heure actuelle, le calcul d'une borne sur le degré des polynômes de Darboux irréductibles et sur le degré d'une intégrale première rationnelle est encore ouvert. C'est pourquoi, dans les algorithmes que nous présentons, la borne sur le degré fait toujours partie des entrées de l'algorithme.

Cet algorithme utilise simplement le fait que les polynômes de Darboux de D de degré inférieur ou égal à N sont des facteurs de $\mathcal{E}_N(D)$. Comme tous les facteurs ne sont pas des polynômes de Darboux nous faisons une vérification à l'étape 5.

La *complexité binaire* de cet algorithme a été étudiée dans [31]. Rappelons que contrairement à la complexité arithmétique, la complexité binaire prend en compte la taille des objets manipulés. Nous avons montré :

Théorème 35. *Soit $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$ telle que :*
$A(X,Y), B(X,Y) \in \mathbb{Z}[X,Y]$, $\deg(A) \leq k$, $\deg(B) \leq k$, $\|A\|_\infty \leq \mathcal{H}$, $\|B\|_\infty \leq \mathcal{H}$ et A, B sont premiers entre eux.
*En utilisant l'*Algorithme Lagutinskii-Pereira *:*

1. *Nous pouvons décider s'il existe un nombre fini de polynômes de Darboux irréductibles de degré $\leq N$ de manière déterministe avec $\mathcal{O}\Big(\big(kN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ opérations binaires.*
2. *Si le nombre de polynômes de Darboux irréductibles de degré $\leq N$ est fini alors nous pouvons tous les calculer de manière déterministe avec $\mathcal{O}\Big(\big(kN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ opérations binaires.*

Nous rappelons que $\|A\|_\infty$ désigne la hauteur de A.

Ce théorème signifie donc que l'Algorithme Lagutinskii-Pereira a une complexité binaire polynomiale en le degré de la dérivation, la borne N sur le degré et la taille des coefficients de la dérivation.

Ce résultat s'obtient en remarquant que tous les calculs utilisés : calcul d'un déterminant, factorisation et pgcd peuvent s'effectuer avec un nombre polynomial d'opérations arithmétiques. Ensuite, nous majorons la taille des objets manipulés et nous en déduisons le théorème précédent.

Ce résultat est intéressant car habituellement c'est la méthode des coefficients indéterminés qui est utilisée pour calculer des polynômes de Darboux. Dans [31] la méthode des coefficients indéterminées est étudiée : la complexité de cette méthode est exponentielle. La raison est la suivante :

Tout d'abord rappelons que seuls les polynômes de Darboux irréductibles nous intéressent. En effet, tout polynôme de Darboux réductible a pour facteurs irréductibles des polynômes de Darboux, voir Proposition 9 page 34. Voila pourquoi nous pouvons nous contenter de calculer uniquement les polynômes de Darboux absolument irréductibles.
Ensuite, lorsque nous utilisons la méthode des coefficients indéterminés nous écrivons le système d'équations polynomiales correspondant à la définition d'un polynôme de Darboux, i.e. $D(f) = g.f$. Or dans cette écriture nous ne faisons pas apparaître que nous ne souhaitons obtenir seulement les polynômes de Darboux irréductibles. Ainsi, si une dérivation possède k polynômes de Darboux de degré 1 alors tous les produits de ces polynômes seront aussi solutions du système $D(f) = g.f$. Nous obtenons donc au moins 2^k polynômes de Darboux de degré inférieur ou égal à k. Donc en prenant $N \geq k$, le système polynomial à résoudre possède au moins 2^k solutions. La taille de la sortie de cet algorithme étant exponentielle, la complexité de la méthode utilisant les coefficients indéterminés est donc exponentielle. Des exemples de dérivations possédant k polynômes de Darboux de degré 1 ont été donnés dans [31].
Remarquons pour finir que le choix $N \geq k$ est naturel, il n'est pas là pour faire apparaître un nombre exponentiel de solutions. En effet, quitte à prendre une borne sur le degré des polynômes de Darboux autant prendre une borne qui nous permette de trouver une intégrale première polynomiale si elle existe. La borne donnée dans le Théorème 10 page 27 nous donne : $k + 1 \leq d$, où d est le degré d'une intégrale première polynomiale. Donc supposer $k \leq N$ est naturel.

La complexité exponentielle de la méthode des coefficients indéterminés provient d'un problème de recombinaison des polynômes de Darboux. La gestion de ce type de problème est au cœur des algorithmes de factorisation. Les problèmes de recombinaison sont bien maitrisés dans le cadre de la factorisation des polynômes. C'est pourquoi nous avons des algorithmes de complexité polynomiale. Ainsi, en ramenant le problème du calcul des polynômes de Darboux à un problème de factorisation l'Algorithme Lagutinskii-Pereira contrôle le problème de recombinaison et a une complexité polynomiale.

Résumons la situation :
Pour calculer des intégrales premières, Darboux a imaginé une méthode. Cette méthode consiste à *recombiner* des cofacteurs en les voyant comme des dérivées logarithmiques. Ensuite, le problème est de calculer des polynômes de Darboux. Nous venons de voir que la méthode "naïve" des coefficients indéterminés permet cela. Cependant, du point de vue de la complexité cette méthode est limitée à cause d'un problème de *recombinaison*. Pour éviter ce problème, nous venons de voir qu'un bonne façon de faire est d'utiliser l'Algorithme Lagutinskii-Pereira. Cette algorithme repose sur la factorisation d'un polynôme. Or, comment factorisons nous des polynômes de nos jours ? en résolvant un problème de *recombinaison* du type "recombinaison de cofacteurs" comme l'a présenté Darboux...

6.3.2 Calcul d'une intégrale première rationnelle de degré borné

L'algorithme précédent peut être modifié afin d'obtenir, lorsqu'elle existe, une intégrale première. Voyons quelle est la difficulté rencontrée et comment la contourner.

Si F_1/F_2 est une intégrale première rationnelle indécomposable de degré N alors F_1 et F_2 sont des polynômes de Darboux. De plus, quitte à effectuer une homographie nous pouvons supposer ces polynômes irréductibles et de degré N. Or, comme F_1/F_2 est une intégrale première de degré N nous avons $\mathcal{E}_N(D) = 0$ et donc nous ne pouvons pas calculer F_1 et F_2 comme des facteurs de $\mathcal{E}_N(D)$.

Le fait que nous ayons $\mathcal{E}_N(D) = 0$ provient du fait que nous avons une infinité de polynômes de Darboux irréductibles de degré N, à savoir les polynômes du type $\lambda F_1 - \mu F_2$ où $(\lambda : \mu) \notin \sigma(F_1, F_2)$. Afin d'éviter cela, nous calculons uniquement *le* polynôme de Darboux de degré N dont le terme constant est nul. Cela signifie que nous allons calculer uniquement $F_2(0,0)F_1 - F_2(0,0)F_1$. Pour cela, nous allons utiliser à nouveau une courbe extatique mais cette fois-ci la base $\mathcal{B}_0$ considérée pour la construction de cette courbe (voir Définition 19 page 33) est la base monomiale privée de la constante 1. Dans ce cas $\mathcal{E}_{\mathcal{B}_0,N}(D) \neq 0$. En effet, nous n'avons plus qu'un seul polynôme de Darboux pouvant être construit à partir de $\mathcal{B}_0$. Donc nous pouvons déduire le polynôme $F_2(0,0)F_1 - F_2(0,0)F_1$ à l'aide d'une factorisation de $\mathcal{E}_{\mathcal{B}_0,N}(D)$.
Le cofacteur g de ce polynôme $F_2(0,0)F_1 - F_2(0,0)F_1$ s'obtient immédiatement. Ensuite pour calculer F_1 et F_2, il reste à résoudre le système linéaire $D(f) = g.f$, où cette fois-ci g est connu et f inconnu.

Cela donne le résultat de complexité suivant :

Théorème 36. *Soit $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$ telle que :*
$A(X,Y), B(X,Y) \in \mathbb{Z}[X,Y]$, $\deg(A) \leq k$, $\deg(B) \leq k$, $\|A\|_\infty \leq \mathcal{H}$, $\|B\|_\infty \leq \mathcal{H}$ et A, B sont premiers entre eux.

1. *On peut décider s'il existe une intégrale première rationnelle de degré $\leq N$ avec $\mathcal{O}\Big(\big(kN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ opérations binaires.*
2. *S'il existe une intégrale première rationnelle de degré $\leq N$ alors nous pouvons la calculer de manière déterministe avec $\mathcal{O}\Big(\big(kN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ opérations binaires.*

6.4 Utilisation du spectre et de la méthode de Newton

Dans cette section nous allons présenter l'algorithme proposé dans [18]. Cet algorithme permet de calculer une intégrale première rationnelle de degré borné. L'objectif ici est d'obtenir un algorithme efficace en pratique. Afin de justifier l'efficacité de cette approche nous en donnons la complexité arithmétique. Ici nous supposons donc que les polynômes A et B appartiennent à $\mathbb{K}[X,Y]$, où $\mathbb{K}$ est un corps de caractéristique nulle.

L'idée de départ est d'améliorer la méthode de Ferragut-Giacomini, voir [54], qui est basée sur l'utilisation du lemme suivant :

Lemme 7. *Soit (E) l'équation différentielle ordinaire non-linéaire suivante :*

$$(E): \quad \frac{dY}{dX} = \frac{B(X,Y)}{A(X,Y)}.$$

où A est tel que $A(0,Y) \neq 0$.
Soit $c \in \mathbb{K}$ et $y_c(X)$ la série formelle solution de (E) qui satisfait $y(0) = c$.
Si D admet une intégrale première rationnelle indécomposable $F_1/F_2 \in \mathbb{K}(X,Y)$ alors $y_c(X)$ est une racine du polynôme non-nul :

$$F_2(0,c)F_1(X,Y) - F_1(0,c)F_2(X,Y) \in \mathbb{K}[X,Y].$$

Ce lemme signifie simplement que lorsque nous avons une intégrale première F_1/F_2, toute orbite du système différentiel est incluse dans une ligne de niveau de F_1/F_2. La preuve étant élémentaire nous rappelons son déroulement.

Démonstration. La fonction F_1/F_2 est une intégrale première indécomposable, nous pouvons donc supposer F_1 et F_2 irréductibles et premiers entre eux. Une application directe du Lemme 3 page 24 nous donne alors que nous avons soit $F_1(0,c) \neq 0$ soit $F_2(0,c) \neq 0$. A présent, supposons que nous avons $F_2(0,c) \neq 0$, dans le cas contraire on considèrera l'intégrale première F_2/F_1.
Comme nous avons $\mathcal{D}(F_1/F_2) = 0$, il vient :

$$\mathcal{D}(F_1/F_2)\big(X, y_c(X)\big) = 0.$$

Cela donne :

$$0 = \frac{\partial(F_1/F_2)}{\partial X}\big(X, y_c(X)\big) + \frac{B\big(X, y_c(X)\big)}{A\big(X, y_c(X)\big)} \cdot \frac{\partial(F_1/F_2)}{\partial Y}\big(X, y_c(X)\big).$$

Par définition de $y_c(X)$ nous avons :

$$0 = \frac{\partial(F_1/F_2)}{\partial X}\big(X, y_c(X)\big) + \frac{dy_c(X)}{dX} \cdot \frac{\partial(F_1/F_2)}{\partial Y}\big(X, y_c(X)\big).$$

En utilisant la règle de dérivation d'une fonction composée on en déduit :

$$0 = \frac{d\big(F_1/F_2\big(X, y_c(X)\big)\big)}{dX}.$$

Ainsi, $F_1/F_2\big(X, y_c(X)\big)$ est constante et on a $F_1/F_2\big(X, y_c(X)\big) = \sigma$, où $\sigma \in \mathbb{K}$. Il en découle $\big(F_1 - \sigma F_2\big)\big(X, y_c(X)\big) = 0$ et $\sigma = F_1(0,c)/F_2(0,c)$. □

Ferragut et Giacomini ont alors proposé une approche du type coefficients indéterminés. Cette méthode se présente ainsi :

Algorithme Ferragut-Giacomini
Entrées : $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$, et $N \in \mathbb{N}$.
Sortie : Une intégrale première rationnelle de degré inférieur à N, si elle existe.

1. Ecrire F_1 et F_2 comme deux polynômes de degré N avec des coefficients indéterminés.

2. Calculer $y_c(X)$ où c est une nouvelle variable.
3. Résoudre $F_2(0,c)F_1(X,y_c(X)) - F_1(0,c)F_2(X,y_c(X)) = 0$.

Ici, résoudre signifie la chose suivante : Tout d'abord, nous écrivons l'égalité ci-dessus à l'aide de séries formelles en X et en c. Ensuite, nous identifions les coefficients et cela donne un système polynomial quadratique à résoudre en les coefficients de F_1 et de F_2. Ferragut et Giacomini assurent que cette méthode est plus rapide que l'approche classique avec les coefficients indéterminés. Cependant, deux problèmes se posent :
Tout d'abord en pratique nous ne calculons pas des séries formelles mais simplement des approximations de celles-ci. Donc en pratique nous allons calculer $y_c(X)$ modulo X^e. Quelle est donc la précision nécessaire, e, pour garantir le succès de cette approche ?
Ensuite, nous savons que la résolution d'un système polynomial quadratique est un problème difficile, c'est à dire "coûteux" en pratique. Nous avons d'ailleurs fait en sorte d'éviter ce genre de calculs dans la section précédente. La question est donc : peut-on avec cette approche éviter de résoudre un système polynomial ?

En repartant du Lemme 7, nous pouvons développer l'approche suivante :

Algorithme IPR
Entrées : $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$, et $N \in \mathbb{N}$.
Sortie : Une intégrale première rationnelle indécomposable de degré inférieur à N, si elle existe, ou "Je ne sais pas".

1. Prendre deux éléments au hasard $c_1, c_2 \in \mathbb{K}$.
2. Calculer $y_{c_1}(X)$ et $y_{c_2}(X)$ modulo N^2+1.
3. Calculer le polynôme minimal P_1 de $y_{c_1}(X)$ et P_2 de $y_{c_2}(X)$.
4. Si $D(P_1/P_2) = 0$ alors rendre P_1/P_2, sinon rendre "Je ne sais pas".

IPR est l'acronyme d'Intégrale Première Rationnelle.

Détaillons à présent l'idée se trouvant derrière cette approche. Nous justifierons le choix de la précision N^2+1 et nous expliquerons comment calculer les polynômes minimaux par la suite.

Tout d'abord nous pouvons remarquer que l'idée est la même que celle utilisée lorsque nous avons étudié la courbe extatique : nous cherchons des polynômes P_i ayant un contact suffisamment grand avec une orbite donnée.
Maintenant supposons que D possède une intégrale première rationnelle indécomposable de degré N, alors toutes les orbites du système sont incluses dans une ligne de niveau du type $\lambda F_1 - \mu F_2$. Ces polynômes sont tous, sauf un nombre fini, irréductibles. Donc si les polynômes minimaux P_1 et P_2 calculés par l'algorithme sont de degré N alors P_1 et P_2 sont du type $\lambda F_1 - \mu F_2$, et le quotient P_1/P_2 est donc à une homographie près F_1/F_2. Ainsi, l'algorithme rend une intégrale première rationnelle. Cette approche échoue et rend "Je ne sais pas" lorsqu'une des solutions $y_{c_i}(X)$ est incluse dans une ligne de niveau du type $\lambda F_1 - \mu F_2$ où $(\lambda : \mu) \in \sigma(F_1, F_2)$. En effet, dans ce cas P_i est un facteur irréductible d'un polynôme du type $\lambda F_1 - \mu F_2$ et donc n'est pas de degré N.

Cette approche est probabiliste, mais nous pouvons la rendre déterministe. En effet, si une intégrale première de degré N existe et que notre algorithme ne la trouve pas alors nous sommes dans une "mauvaise situation" : nous avons une solution y_{c_i} qui se trouve sur une ligne de niveau du type $\lambda F_1 - \mu F_2$ avec $(\lambda : \mu) \in \sigma(F_1, F_2)$. L'algorithme calcule donc un polynôme P_i qui est un polynôme de Darboux irréductible de degré inférieur à N. En recommençant $k(k+1)/2+2$ fois notre algorithme nous avons dans le pire des cas calculer $k(k+1)/2+2$ polynômes de Darboux irréductibles. Le théorème de Jouanolou nous dit alors qu'en recombinant ces polynômes nous obtenons une intégrale première.
Autre façon de voir les choses : ce type de "mauvaise situation" est fini car le spectre est fini. Nous pouvons de plus borner la taille du spectre en fonction du degré de A et de B, voir Section 3.4 page 59. Donc en recommençant un nombre fini de fois cette approche nous sommes sûr de trouver une intégrale première rationnelle de degré inférieur à N si elle existe.

A présent rappelons pourquoi la précision N^2+1 est suffisante pour reconnaître un polynôme minimal. Ce type de résultat est classique lorsque l'on étudie la factorisation des polynômes, il a d'ailleurs été utilisé par Kaltofen dans [81]. Ce résultat a aussi été utilisé dans un contexte "différentiel" par Aroca, Cano, Feng et Gao dans [4].

Lemme 8. *Soit $y(X) \in \mathbb{K}[[X]]$ une série formelle algébrique dont le polynôme minimal $P(X,Y) \in \mathbb{K}[X,Y]$ est de degré inférieur à N.*
Si $\tilde{P} \in \mathbb{K}[X,Y]$ est un polynôme de degré inférieur à N satisfaisant

$$(\star) : \ \tilde{P}\big(X, y(X)\big) \equiv 0 \mod X^{N^2+1},$$

alors $\tilde{P}\big(X, y(X)\big) = 0$.

Démonstration. P satisfait$(\star)$ donc il existe un polynôme $\tilde{P} \in \mathbb{K}[X,Y]$ de degré inférieur à N satisfaisant $(\star)$.
Considérons $\mathcal{R}(X) := \mathrm{Res}_Y\big(P(X,Y), \tilde{P}(X,Y)\big)$.
Il existe deux polynômes S et T dans $\mathbb{K}[X,Y]$ tel que $S\,P + T\,\tilde{P} = \mathcal{R}$.
La condition $(\star)$ entraine $\mathcal{R}(X) \equiv 0 \mod X^{N^2+1}$.
D'autre part le théorème de Bezout nous donne : $\deg(\mathcal{R}) \leq \deg(P)\,\deg(\tilde{P}) \leq N^2$.
On en déduit alors $\mathcal{R} = 0$, ce qui signifie que le pgcd de P et $\tilde{P}$ est non-trivial. Comme P est irréductible, P divise $\tilde{P}$ et donc $\tilde{P}\big(X, y(X)\big) = 0$. □

Ce lemme implique que si nous connaissons une racine $y_{c_i}(X)$ avec une précision N^2+1 alors nous pouvons calculer son polynôme minimal. Ce type d'approche est classique et s'apparente à la méthode de factorisation développée par Kannan, Lenstra et Lovász dans [82]. En effet, nous adoptons la démarche suivante :

Calcul d'un polynôme minimal
Entrée : $y_c(X) \in \mathbb{K}[X]$ de degré N^2+1.
Sorties : Un polynôme $P(X,Y) \in \mathbb{K}[X,Y]$ de degré minimal et inférieur à N tel que $P\big(X, y_c(X)\big) \equiv 0 \mod X^{N^2+1}$, s'il existe, ou "Rien".

1. Soit $P(X,Y) = \sum_{i=0}^{N} \left(\sum_{j=0}^{N-i} p_{i,j}\, X^j\right) Y^i$, les $p_{i,j}$ sont des variables.

2. Construire le système linéaire $(\mathcal{L})$, d'inconnues les $p_{i,j}$, donné par :

$$P(X, y_c(X)) = \sum_{i=0}^{N} \left(\sum_{j=0}^{N-i} p_{i,j}\, X^j \right) y_c(X)^i \equiv 0 \mod X^{N^2+1}.$$

3. Si $(\mathcal{L})$ ne possède pas de solutions non-triviales alors rendre "Rien".
4. Sinon, calculer une base échelonnée réduite du noyau $(\mathcal{L})$ afin de trouver un polynôme $P(X, Y)$ de degré minimal en Y et rendre ce polynôme.

D'après le Lemme 8, cet algorithme calcule le polynôme minimal de $y_c(X) \in \mathbb{K}[[X]]$. On utilise ici une approche du type coefficients indéterminés mais les calculs reposent sur de l'algèbre linéaire et non pas sur la résolution d'un système quadratique.

En résumé, l'algorithme IPR calcule deux séries formelles tronquées $y_{c_i}(X)$. Cela s'effectue en pratique avec la méthode de Newton, voir l'article de Brent et Kung [20]. Puis nous avons à résoudre deux systèmes linéaires pour trouver P_1 et P_2. La complexité de cette méthode a été étudiée et on obtient, voir [18] :

Théorème 37. *Soient $D = A(X, Y)\partial_X + B(X, Y)\partial_Y$ où A et B sont de degré inférieur à k. Soit N un entier supérieur à k. On suppose k fixé et N tend vers l'infini.*
L'algorithme IPR utilise $\tilde{\mathcal{O}}(N^{2\theta})$ opérations arithmétiques.
En répétant l'algorithme IPR un nombre fini de fois nous obtenons une méthode déterministe de calcul d'intégrales premières.
Le nombre d'opérations arithmétiques utilisées par cette méthode déterministe est d'au plus $\tilde{\mathcal{O}}(k^2 N^{2\theta+1})$.

Bien que k soit fixé et donc constant nous avons choisi de faire apparaître cette constante dans la complexité afin de souligner la dépendance en k du nombre de répétitions de l'algorithme IPR.

Afin de juger la complexité de l'algorithme IPR nous rappelons que la méthode utilisant la courbe extatique utilise au moins $\tilde{\mathcal{O}}(k^{\theta+1} N^{4\theta+4})$ opérations arithmétiques. En effet, nous devons factoriser la courbe extatique qui est un polynôme en deux variables de degré au moins kN^4. Donc la stratégie utilisant la courbe extatique est surpassée par l'algorithme IPR. En effet, lorsque $\theta = 3$, c'est à dire lorsque nous utilisons l'élimination de Gauss, la factorisation de la courbe extatique coûte $\tilde{\mathcal{O}}(k^4 N^{16})$ opérations arithmétiques alors que l'algorithme IPR n'en utilise que $\tilde{\mathcal{O}}(N^6)$, et la version déterministe n'en utilise que $\tilde{\mathcal{O}}(k^2 N^7)$. Remarquons que l'algorithme IPR a une complexité cubique en la taille de la sortie.
Dans [18] diverses variations autour de l'approche utilisée dans l'algorithme IPR sont données. Une heuristique basée sur l'utilisation d'approximants de Padé-Hermite est proposée. Cette heuristique a une complexité arithmétique en $\tilde{\mathcal{O}}(N^{\theta+2})$.

Contrairement à la méthode utilisant la courbe extatique la complexité binaire de ces méthodes n'a pas été étudiée. Cependant, en pratique, l'algorithme IPR et ses variantes répondent à nos attentes : ils sont plus rapides que les autres algorithmes. Des exemples

et des temps de calculs sont donnés dans [18].

Enfin, mentionnons que l'approche utilisée dans l'algorithme IPR s'adapte pour calculer les polynômes de Darboux irréductibles de degré inférieur à N d'une dérivation donnée. En effet, il suffit de calculer une série formelle solution de (E) où c est une variable. Ensuite nous cherchons pour quelles valeurs de c la série formelle y_c est algébrique de degré inférieur à N. Cette adaptation et son comportement pratique sont présentés dans [18].

6.5 Problème ouvert

Le problème ouvert correspondant à cette section est le problème de Poincaré, à savoir "Etant donnée une dérivation $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$, où $A, B \in \mathbb{Z}[X,Y]$, calculer ou borner, si cela est possible, le degré des polynômes de Darboux irréductibles".

Troisième partie

Problèmes ouverts

Dans cette partie nous reprenons les problèmes énoncés à la fin des chapitres. Nous ajoutons aussi quelques problèmes ouverts en rapport avec les travaux présentés dans ce cours. L'ordre des problèmes suit l'ordre des chapitres.

Formes de Noether
Le théorème de Ruppert, Théorème 2 page 3, permet de borner le degré des formes de Noether par $d^2 - 1$. Est-ce que cette borne est optimale ?
La réponse à cette question n'est actuellement pas connue.

Bornes sur le spectre
La borne $d^2 - 1$ sur l'ordre total de réductibilité est-elle optimale ?
Autrement dit, peut-on trouver des exemples où $\rho(F_1, F_2) = d^2 - 1$?
Il existe de tels exemples pour $d \leq 3$, voir l'article de Lorenzini [101].
Ce problème est lié à la question précédente de l'optimalité de la borne $d^2 - 1$ pour les formes de Noether.

Borne de Jouanolou
Nous avons vu qu'en exprimant le théorème de Jouanolou à l'aide de la taille d'un polytope de Newton associé à la dérivation alors nous obtenons une borne optimale. Cependant, cela ne montre pas si la borne $k(k+1)/2 + 2$ est atteinte. Il se pose alors la question : la borne de Jouanolou est-elle optimale ?
Ce résultat aurait aussi un impact sur l'étude du spectre comme nous l'avons vu à la Section 3.4.

Problème de Poincaré pour une dérivation à coefficients entiers
Etant donnée une dérivation $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$, où $A, B \in \mathbb{Z}[X,Y]$, calculer ou borner, si cela est possible, le degré des polynômes de Darboux irréductibles.

Conjecture $R(m,n)$
La conjecture suivante baptisée $R(m,n)$ se trouve dans le travail récent de Furter à propos de la rigidité [59]. Voici cette conjecture :
Soient $f(X) = X(1 + a_1X + \cdots + a_mX^m)$, $g(X) = X(1 + b_1X + \cdots + b_nX^n) \in \mathbb{C}[X]$. On pose $f(g) = X(1 + c_1X + \cdots + c_NX^N)$, où $N = (m+1)(n+1) - 1$.
Si $c_1 = \cdots = c_{m+n} = 0$ alors $f = g = X$.

Racines entières et composition Le problème suivant se trouve dans le livre de Malajovich [105].
Soient $f_1, \ldots, f_k$ des polynômes d'une variable à coefficients entiers. Quel est le nombre maximum de racines entières de $f_1 \circ \cdots \circ f_k$? Est il possible que ce nombre soit égal au produit des degré des f_i ?
Il existe un exemple de 4 polynômes de degré 2 donnant après composition un polynôme ayant 16 racines entières. Le même type d'exemple avec 5 polynômes de degré 2 dont la composition a 32 racines entières n'est pas connue à ce jour.

Annexe A

Appendice : Rappel d'algèbre

Dans cet appendice nous rappelons quelques résultats classiques.

A.1 Critère jacobien

Ce que nous appelons critère jacobien dans ce mémoire est le résultat suivant :

Théorème 38. *Critère jacobien.*
Soient $f_1, \ldots, f_r \in \mathbb{C}(X_1, \ldots, X_n)$. On a équivalence entre :

1. *Les fractions $f_1, \ldots, f_r$ sont algébriquement indépendantes sur $\mathbb{C}$.*
2. *La matrice jacobienne*

$$\begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_r}{\partial X_1} & \cdots & \frac{\partial f_r}{\partial X_n} \end{pmatrix}$$

est de rang r.

Démonstration. Voir par exemple une preuve dans le livre de Hodge et Pedoe [77, Chapter 3, Section 7, Theorem 3]. □

A.2 Extension intermédiaire de type fini

Le théorème suivant est classique et parfois utilisé de manière implicite par certains auteurs.

Théorème 39. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps de type fini et soit $\mathbb{E}$ un corps intermédiaire. Alors $\mathbb{E}$ est aussi de type fini sur $\mathbb{K}$.*
Plus précisément, si $k \subset \mathbb{K} \subset k(X_1, \ldots, X_n)$ où $X_1, \ldots, X_n$ sont des variables, alors $\mathbb{K} = k(g_1, \ldots, g_t)$ où $g_i \in k(X_1, \ldots, X_n)$. De plus lorsque la caractéristique de k est nulle alors $t \leq trdeg_k \mathbb{K} + 1$, où $trdeg_k$ désigne le degré de transcendance sur k.

Démonstration. Une preuve complète de la première assertion se trouve dans le livre d'Isaacs [78, Theorem 24.9]. La preuve de l'assertion sur les corps intermédiaires de $k(X_1, \ldots, X_n)$ se trouve dans le livre de Schinzel [135, Theorem 1 p. 12].
L'idée est de compléter une base de transcendance de $\mathbb{E}$ sur $\mathbb{K}$. □

Ce théorème est fondamental. En effet, il n'est pas nécessaire qu'une structure intermédiaire d'une structure de type fini soit de type fini. Par exemple, le sous-anneau de $\mathbb{C}[X, Y]$ engendré par X, X^2Y, ..., X^nY^{n-1}, ... n'est pas de type fini. Cet exemple est dû à Samuel [132].
Cette problématique a été soulevé par Hilbert dans son quatorzième problème. Ce problème s'énonce ainsi : Soit $\mathbb{K}$ un sous-corps de $k(X_1, \ldots, X_n)$ contenant k. Est-ce que l'anneau $\mathbb{K} \cap k[X_1, \ldots, X_n]$ est de type fini ?
Nagata a montré que la réponse est non en général, voir [113]. Cependant, nous avons le résultat suivant dû à Zariski, [149].

Théorème 40. *Théorème de Zariski.*
Soit $\mathbb{K}$ un sous-corps de $k(X_1, \ldots, X_n)$ contenant k, où k est un corps de caractéristique nulle. Si $trdeg_k\mathbb{K} \leq 2$ alors l'anneau $\mathbb{K} \cap k[X_1, \ldots, X_n]$ est de type fini sur k.

Pour un contre-exemple où $\mathrm{trdeg}_k\mathbb{K} = 3$, voir l'article de Kuroda [88].

Dans [117], [116], Nagata et Nowicki utilisent le théorème de Zariski afin de montrer que $k[X_1, \ldots, X_n]^D$ est de type fini lorsque $n \leq 3$. En reprenant le contre-exemple de Nagata pour le quatorzième problème de Hilbert, Derksen a montré dans [45] que $k[X_1, \ldots, X_n]^D$ n'est pas nécessairement de type fini.

A.3 Théorème de Lüroth

Théorème 41. *Théorème de Lüroth classique.*
Soit $\mathbb{K}$ un corps tel que $\mathbb{C} \subsetneq \mathbb{K} \subset \mathbb{C}(X)$. Alors $\mathbb{K} = \mathbb{C}(F)$ où $F \in \mathbb{C}(X)$.

Démonstration. Voir par exemple dans le livre de Schinzel [135] le Théorème 2 p.13. □

Ce théorème a été énoncé en 1876 par Lüroth. Une généralisation à n variables a été donnée en 1887 par Gordan. Cette généralisation est souvent appelée théorème de Lüroth étendu.

Théorème 42. *Théorème de Lüroth étendu.*
Soit $\mathbb{K}$ un corps vérifiant $k \subsetneq \mathbb{K} \subset k(X_1, \ldots, X_n)$ et tel que $trdeg_k\mathbb{K} = 1$ où $trdeg_k$ désigne le degré de transcendance sur k. Alors $\mathbb{K} = k(F)$ où $F \in k(X_1, \ldots, X_n)$.
Supposons de plus que $\mathbb{K}$ contienne un polynôme alors on peut prendre un générateur polynomial de $\mathbb{K}$, c'est à dire $F \in k[X_1, \ldots, X_n]$.

Démonstration. Voir par exemple dans le livre de Schinzel [135] le Theorem 3 p.15. □

Bibliographie

[1] S. S. Abhyankar, W. J. Heinzer, and A. Sathaye. Translates of polynomials. In *A tribute to C. S. Seshadri (Chennai, 2002)*, Trends Math., pages 51–124. Birkhäuser, Basel, 2003.

[2] V. S. Alagar and Mai Thanh. Fast polynomial decomposition algorithms. In *EUROCAL '85, Vol. 2 (Linz, 1985)*, volume 204 of *Lecture Notes in Comput. Sci.*, pages 150–153. Springer, Berlin, 1985.

[3] C. Alonso, J. Gutierrez, and T. Recio. A rational function decomposition algorithm by near-separated polynomials. *J. Symbolic Comput.*, 19(6) :527–544, 1995.

[4] J. M. Aroca, J. Cano, R. Feng, and X. S. Gao. Algebraic general solutions of algebraic ordinary differential equations. In *ISSAC'05*, pages 29–36 (electronic). ACM, New York, 2005.

[5] M. Ayad. Sur les polynômes $f(X, Y)$ tels que $K[f]$ est intégralement fermé dans $K[X, Y]$. *Acta Arith.*, 105(1) :9–28, 2002.

[6] M. Ayad and P. Fleischmann. On the decomposition of rational functions. *J. Symbolic Comput.*, 43(4) :259–274, 2008.

[7] D. R. Barton and R. Zippel. Polynomial decomposition algorithms. *J. Symbolic Comput.*, 1(2) :159–168, 1985.

[8] K. Belabas, M. van Hoeij, J. Klüners, and A. Steel. Factoring polynomials over global fields. *J. Théor. Nombres Bordeaux*, 21(1) :15–39, 2009.

[9] J. Berthomieu and G. Lecerf. Reduction of bivariate polynomials from convex-dense to dense, with application to factorization. *Math. Comp.*, 81(279) :1799–1821, 2012.

[10] D. Bini and V. Y. Pan. *Polynomial and matrix computations. Vol. 1.* Progress in Theoretical Computer Science. Birkhäuser Boston Inc., Boston, MA, 1994. Fundamental algorithms.

[11] L. Blum, F. Cucker, and S. Shub, M.and Smale. *Complexity and real computation.* Springer-Verlag, New York, 1998. With a foreword by Richard M. Karp.

[12] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers : NP-completeness, recursive functions and universal machines. *Bull. Amer. Math. Soc. (N.S.)*, 21(1) :1–46, 1989.

[13] A. Bodin. Reducibility of rational functions in several variables. *Israel J. Math.*, 164 :333–347, 2008.

[14] A. Bodin. Decomposition of polynomials and approximate roots. *Proc. Amer. Math. Soc.*, 138(6) :1989–1994, 2010.

[15] A. Bodin, G. Chèze, and P. Dèbes. Specializations of indecomposable polynomials. *Manuscripta Math.*, 139(3-4) :391–403, 2012.

[16] A. Bodin, P. Dèbes, and S. Najib. Indecomposable polynomials and their spectrum. *Acta Arith.*, 139(1) :79–100, 2009.

[17] A. Bodin, P. Dèbes, and S. Najib. Irreducibility of hypersurfaces. *Comm. in Algebra*, 37(6) :1884–1900, 2009.

[18] A. Bostan, G. Chèze, T. Cluzeau, and J.-A. Weil. An efficient algorithm for computing rational first integrals of polynomial vector fields. A paraître dans Math. Comp., 2015, http ://dx.doi.org/10.1090/mcom/3007.

[19] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt. Complexity issues in bivariate polynomial factorization. In *ISSAC 2004*, pages 42–49. ACM, New York, 2004.

[20] R. P. Brent and H. T. Kung. Fast algorithms for manipulating formal power series. *J. Assoc. Comput. Mach.*, 25(4) :581–595, 1978.

[21] M. Bronstein. *Symbolic integration. I*, volume 1 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, second edition, 2005.

[22] L. Busé and G. Chèze. On the total order of reducibility of a pencil of algebraic plane curves. *J. Algebra*, 341 :256–278, 2011.

[23] L. Busé, G. Chèze, and S. Najib. Noether forms for the study of non-composite rational functions and their spectrum. *Acta Arith.*, 147(3) :217–231, 2011.

[24] M. Carnicer. The Poincaré problem in the nondicritical case. *Ann. of Math. (2)*, 140(2) :289–294, 1994.

[25] H. Cartan. *Cours de calcul différentiel*. Collection Méthodes. Hermann, Paris, 1977.

[26] D. Cerveau and A. Lins Neto. Holomorphic foliations in $\mathbf{C}\mathrm{P}(2)$ having an invariant algebraic curve. *Ann. Inst. Fourier (Grenoble)*, 41(4) :883–903, 1991.

[27] J. Chavarriga, H. Giacomini, J. Giné, and J. Llibre. Darboux integrability and the inverse integrating factor. *J. Differential Equations*, 194(1) :116–139, 2003.

[28] J. Chavarriga and M. Grau. Some open problems related to 16b Hilbert problem. *Sci. Ser. A Math. Sci. (N.S.)*, 9 :1–26, 2003.

[29] G. Chèze. Des méthodes symboliques-numériques et exactes pour la factorisation absolue des polynômes en deux variables. Thèse de l'Université de Nice-Sophia Antipolis, 2004.

[30] G. Chèze. Nearly optimal algorithms for the decomposition of multivariate rational functions and the extended Lüroth theorem. *J. Complexity*, 26(4) :344–363, 2010.

[31] G. Chèze. Computation of Darboux polynomials and rational first integrals with bounded degree in polynomial time. *J. Complexity*, 27(2) :246–262, 2011.

[32] G. Chèze. A recombination algorithm for the decomposition of multivariate rational functions. *Math. Comp.*, 82(283) :1793–1812, 2013.

[33] G. Chèze. Darboux theory of integrability in the sparse case. *J. Differential Equations*, 257(2) :601–609, 2014.

[34] G. Chèze. Bounding the number of remarkable values via Jouanolou's theorem. *J. Differential Equations*, 258(10) :3535–3545, 2015.

[35] G. Chèze and T. Cluzeau. On the nonexistence of Liouvillian first integrals for generalized Liénard polynomial differential systems. *J. Nonlinear Math. Phys.*, 20(4) :475–479, 2013.

[36] G. Chèze and G. Lecerf. Lifting and recombination techniques for absolute factorization. *J. Complexity*, 23(3) :380–420, 2007.

[37] G. Chèze and S. Najib. Indecomposability of polynomials via Jacobian matrix. *J. Algebra*, 324(1) :1–11, 2010.

[38] C. Christopher. Liouvillian first integrals of second order polynomial differential equations. *Electron. J. Differential Equations*, pages No. 49, 7 pp. (electronic), 1999.

[39] C. Christopher and C. Li. *Limit cycles of differential equations*. Advanced Courses in Mathematics. CRM Barcelona. Birkhäuser Verlag, Basel, 2007.

[40] C. Christopher, J. Llibre, and J. V. Pereira. Multiplicity of invariant algebraic curves in polynomial vector fields. *Pacific J. Math.*, 229(1) :63–117, 2007.

[41] S. C. Coutinho and L. Menasché Schechter. Algebraic solutions of holomorphic foliations : an algorithmic approach. *J. Symbolic Comput.*, 41(5) :603–618, 2006.

[42] S. C. Coutinho and L. Menasché Schechter. Algebraic solutions of plane vector fields. *J. Pure Appl. Algebra*, 213(1) :144–153, 2009.

[43] N. C. A. da Costa and F. A. Doria. Undecidability and incompleteness in classical mechanics. *Internat. J. Theoret. Phys.*, 30(8) :1041–1073, 1991.

[44] G. Darboux. Mémoire sur les équations diff'érentielles du premier ordre et du premier degré. *Bull. Sci. Math.*, 32 :60–96, 123–144, 151–200, 1878.

[45] H. G. J. Derksen. The kernel of a derivation. *J. Pure Appl. Algebra*, 84(1) :13–16, 1993.

[46] M. Dickerson. Polynomial decomposition algorithms for multivariate polynomials. Technical Report TR87-826, Comput. Sci., Cornell Univ., 1987.

[47] A. Dimca. *Singularities and topology of hypersurfaces*. Universitext. Springer-Verlag, New York, 1992.

[48] V. A. Dobrovol'skii, N. V. Lokot', and J.-M. Strelcyn. Mikhail Nikolaevich Lagutinskii (1871–1915) : un mathématicien méconnu. *Historia Math.*, 25(3) :245–264, 1998.

[49] F. Dumortier, J. Llibre, and J. C. Artés. *Qualitative theory of planar differential systems*. Universitext. Springer-Verlag, Berlin, 2006.

[50] Leonhardus Eulerus. *Commercium epistolicum*. Leonhardi Euleri Opera Omnia, Series Quarta A : Commercium Epistolicum, V. Birkhäuser Verlag, Basel, 1980. Correspondence with A. C. Clairaut, J. d'Alembert, and J. L. Lagrange, Edited and with an introduction by Adolf P. Juškevič [A. P. Yushkevich] and René Taton, With the assistance of Charles Blanc, Ašot T. Grigorijan [A. T. Grigor′jan], Walter Habicht and Guy Picolet.

[51] J.-C. Faugère and L. Perret. An efficient algorithm for decomposing multivariate polynomials and its applications to cryptography. *J. Symbolic Comput.*, 44(12) :1676–1689, 2009.

[52] J.-C. Faugère and L. Perret. High order derivatives and decomposition of multivariate polynomials. In *ISSAC 2009—Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, pages 207–214. ACM, New York, 2009.

[53] J.-C. Faugère, J. von zur Gathen, and L. Perret. Decomposition of generic multivariate polynomials. In *ISSAC 2010—Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 131–137. ACM, New York, 2010.

[54] A. Ferragut and H. Giacomini. A new algorithm for finding rational first integrals of polynomial vector fields. to appear in Qualitative Theory of Dynamical Systems, 2010.

[55] A. Ferragut and J. Llibre. On the remarkable values of the rational first integrals of polynomial vector fields. *J. Differential Equations*, 241(2) :399–417, 2007.

[56] M. D. Fried and M. Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2005.

[57] M. D. Fried and R. E. MacRae. On curves with separated variables. *Math. Ann.*, 180 :220–226, 1969.

[58] S. D. Furta. On non-integrability of general systems of differential equations. *Z. Angew. Math. Phys.*, 47(1) :112–131, 1996.

[59] J.-P. Furter. Polynomial composition rigidity and plane polynomial automorphisms. *J. London Math. Society*, 91(1) :180–202, 2015.

[60] Andrei Gabrielov. Multiplicity of a zero of an analytic function on a trajectory of a vector field. In *The Arnoldfest (Toronto, ON, 1997)*, volume 24 of *Fields Inst. Commun.*, pages 191–200. Amer. Math. Soc., Providence, RI, 1999.

[61] S. Gao. Factoring multivariate polynomials via partial differential equations. *Math. Comp.*, 72(242) :801–822 (electronic), 2003.

[62] S. Gao and V. M. Rodrigues. Irreducibility of polynomials modulo p via Newton polytopes. *J. Number Theory*, 101(1) :32–47, 2003.

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

[64] J. von zur Gathen. Functional decomposition of polynomials : the wild case. *J. Symbolic Comput.*, 10(5) :437–452, 1990.

[65] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

[66] J. von zur Gathen, J. Gutierrez, and R. Rubio. Multivariate polynomial decomposition. *Appl. Algebra Engrg. Comm. Comput.*, 14(1) :11–31, 2003.

[67] J. von zur Gathen and J. Weiss. Homogeneous bivariate decompositions. *J. Symbolic Comput.*, 19(5) :409–434, 1995.

[68] H. Giacomini, J. Llibre, and M. Viano. On the nonexistence, existence and uniqueness of limit cycles. *Nonlinearity*, 9(2) :501–516, 1996.

[69] H. Giacomini and S. Neukirch. Number of limit cycles of the Liénard equation. *Phys. Rev. E (3)*, 56(4) :3809–3813, 1997.

[70] J. Giné and J. Llibre. A note on Liouvillian integrability. *J. Math. Anal. Appl.*, 387(2) :1044–1049, 2012.

[71] J. Giné and J. Llibre. On Liouvillian integrability of the first-order polynomial ordinary differential equations. *J. Math. Anal. Appl.*, 395(2) :802–805, 2012.

[72] A. Goriely. *Integrability and nonintegrability of dynamical systems*, volume 19 of *Advanced Series in Nonlinear Dynamics*. World Scientific Publishing Co. Inc., River Edge, NJ, 2001.

[73] D. S. Graça, M. L. Campagnolo, and J. Buescu. Computability with polynomial differential equations. *Adv. in Appl. Math.*, 40(3) :330–349, 2008.

[74] J. Gutierrez, R. Rubio, and D. Sevilla. Unirational fields of transcendence degree one and functional decomposition. In *ISSAC '01 : Proceedings of the 2001 international symposium on Symbolic and algebraic computation*, pages 167–174, New York, NY, USA, 2001. ACM Press.

[75] J. Gutierrez and D. Sevilla. Building counterexamples to generalizations for rational functions of Ritt's decomposition theorem. *J. Algebra*, 303(2) :655–667, 2006.

[76] D. Hilbert. Ueber die irredueibilität ganzer rationaler Functionen mit ganzzahligen Coeffieienten. *J. reine angew. Math.*, 110 :104–129, 1892.

[77] W.V.D. Hodge and D. Pedoe. *Methods of Algebraic Geometry*. Number vol. 1,livr. 1 à 2 in Cambridge Mathematical Library. Cambridge University Press, 1994.

[78] M. Isaacs. *Algebra : A Graduate Course*. Brooks/Cole, 1994.

[79] J.-P. Jouanolou. *Équations de Pfaff algébriques*, volume 708 of *Lecture Notes in Mathematics*. Springer, Berlin, 1979.

[80] J.-P. Jouanolou. *Théorèmes de Bertini et applications*, volume 42 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1983.

[81] E. Kaltofen. Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM J. Comput.*, 14(2) :469–489, 1985.

[82] R. Kannan, A. K. Lenstra, and L. Lovász. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. *Math. Comp.*, 50(181) :235–250, 1988.

[83] S. L. Kleiman. Bertini and his two fundamental theorems. *Rend. Circ. Mat. Palermo (2) Suppl.*, 55 :9–37, 1998. Studies in the history of modern mathematics, III.

[84] J. Klüners. On polynomial decompositions. *J. Symbolic Comput.*, 27(3) :261–269, 1999.

[85] K.-I Ko. *Complexity theory of real functions*. Progress in Theoretical Computer Science. Birkhäuser Boston Inc., Boston, MA, 1991.

[86] D. Kozen and S. Landau. Polynomial decomposition algorithms. *J. Symbolic Comput.*, 7(5) :445–456, 1989.

[87] W. Krull. Über einen irreduzibilitätssatz von Bertini. *Journal für die reine und angewandte Mathematik*, 177 :94–104, 1937.

[88] S. Kuroda. A counterexample to the fourteenth problem of Hilbert in dimension three. *Michigan Math. J.*, 53(1) :123–132, 2005.

[89] M. N. Lagutinskii. L'application d'opérations polaires à l'intégration en termes finis des équations différentielles ordinaires. *Soobshcheniya Kharkovskogo Matematicheskogo Obshchestva*, 12(2) :111–243, 1911.

[90] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[91] G. Lecerf. Sharp precision in Hensel lifting for bivariate polynomial factorization. *Math. Comp.*, 75(254) :921–933 (electronic), 2006.

[92] G. Lecerf. Improved dense multivariate polynomial factorization algorithms. *J. Symbolic Comput.*, 42(4) :477–494, 2007.

[93] J. Lei and L. Yang. Algebraic multiplicity and the Poincaré problem. In *Differential equations with symbolic computation*, Trends Math., pages 143–157. Birkhäuser, Basel, 2005.

[94] N. Levinson and O. K. Smith. A general equation for relaxation oscillations. *Duke Math. J.*, 9 :382–403, 1942.

[95] A. Liénard. Étude des oscillations entretenues. *Revue générale de l'électricité*, 23(21) :901–912, 1928.

[96] J. Llibre and C. Valls. Liouvillian first integrals for Liénard polynomial differential systems. *Proc. Amer. Math. Soc.*, 138(9) :3229–3239, 2010.

[97] J. Llibre and J. Valls. Liouvillian first integrals for Liénard polynomial differential systems. *Proc. Amer. Math. Soc.*, 138(9) :3229–3239, 2010.

[98] J. Llibre and X. Zhang. Darboux theory of integrability for polynomial vector fields in $\mathbb{R}^n$ taking into account the multiplicity at infinity. *Bull. Sci. Math.*, 133(7) :765–778, 2009.

[99] J. Llibre and X. Zhang. Darboux theory of integrability in $\mathbb{C}^n$ taking into account the multiplicity. *J. Differential Equations*, 246(2) :541–551, 2009.

[100] J. Llibre and X. Zhang. Rational first integrals in the Darboux theory of integrability in $\mathbb{C}^n$. *Bull. Sci. Math.*, 134(2) :189–195, 2010.

[101] D. Lorenzini. Reducibility of polynomials in two variables. *J. Algebra*, 156(1) :65–75, 1993.

[102] A. J. Maciejewski, J. Moulin Ollagnier, and A. Nowicki. Generic polynomial vector fields are not integrable. *Indag. Math. (N.S.)*, 15(1) :55–72, 2004.

[103] A. J. Maciejewski, J. Moulin Ollagnier, and A. Nowicki. Correction to : "Generic polynomial vector fields are not integrable" [Indag. Math. (N.S.) **15** (2004), no. 1, 55–72]. *Indag. Math. (N.S.)*, 18(2) :245–249, 2007.

[104] A. J. Maciejewski, J. Moulin Ollagnier, A. Nowicki, and J.-M. Strelcyn. Around Jouanolou non-integrability theorem. *Indag. Math. (N.S.)*, 11(2) :239–254, 2000.

[105] G. Malajovich. *Nonlinear equations*. Publicações Matemáticas do IMPA. [IMPA Mathematical Publications]. Instituto Nacional de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 2011. With an appendix by Carlos Beltrán, Jean-Pierre Dedieu, Luis Miguel Pardo and Mike Shub, 28o Colóquio Brasileiro de Matemática. [28th Brazilian Mathematics Colloquium].

[106] Y.-K. Man. Computing closed form solutions of first order ODEs using the Prelle-Singer procedure. *J. Symbolic Comput.*, 16(5) :423–443, 1993.

[107] Y.-K Man and M. A. H. MacCallum. A rational approach to the Prelle-Singer algorithm. *J. Symbolic Comput.*, 24(1) :31–43, 1997.

[108] Y. Matiyasevich. *Hilbert's Tenth Problem*. Foundations of Computing. The MIT Press, Cambridge, London, 1993.

[109] J. Moulin Ollagnier. Some remarks about the integration of polynomial planar vector fields. *Qual. Theory Dyn. Syst.*, 3(1) :19–28, 2002.

[110] J. Moulin Ollagnier. Algebraic closure of a rational function. *Qual. Theory Dyn. Syst.*, 5(2) :285–300, 2004.

[111] J. Moulin Ollagnier and A. Nowicki. Derivations of polynomial algebras without Darboux polynomials. *J. Pure Appl. Algebra*, 212(7) :1626–1631, 2008.

[112] J. Moulin Ollagnier, A. Nowicki, and J.-M. Strelcyn. On the non-existence of constants of derivations : the proof of a theorem of Jouanolou and its development. *Bull. Sci. Math.*, 119(3) :195–233, 1995.

[113] M. Nagata. *Lectures on the fourteenth problem of Hilbert*. Tata Institute of Fundamental Research, Bombay, 1965.

[114] S. Najib. Une généralisation de l'inégalité de Stein-Lorenzini. *J. Algebra*, 292(2) :566–573, 2005.

[115] E. Noether. Ein algebraisches Kriterium für absolute Irreduzibilität. *Math. Ann.*, 85(1) :26–40, 1922.

[116] A. Nowicki. Polynomial derivations and their ring of constants. N. Copernicus University, Torun, 1994.

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

[118] A. Nowicki and J.-M. Strelcyn. Generators of rings of constants for some diagonal derivations in polynomial rings. *J. Pure Appl. Algebra*, 101(2) :207–212, 1995.

[119] K. Odani. The limit cycle of the van der Pol equation is not algebraic. *J. Differential Equations*, 115(1) :146–152, 1995.

[120] K. Odani. The integration of polynomial Liénard systems by elementary functions. *Differential Equations Dynam. Systems*, 5(3-4) :347–354, 1997. Planar nonlinear dynamical systems (Delft, 1995).

[121] A. M. Ostrowski. On multiplication and factorization of polynomials. I. Lexicographic orderings and extreme aggregates of terms. *Aequationes Math.*, 13(3) :201–228, 1975.

[122] F. Pakovich. Algebraic curves $P(x) - Q(y) = 0$ and functional equations. *Complex Var. Elliptic Equ.*, 56(1-4) :199–213, 2011.

[123] J. V. Pereira. Vector fields, invariant varieties and linear systems. *Ann. Inst. Fourier (Grenoble)*, 51(5) :1385–1405, 2001.

[124] É. Picard. Sur les intégrales doubles de fonctions rationnelles dont tous les résidus sont nuls. *Bulletin des sciences mathématiques, série 2*, 26, 1902.

[125] H. Poincaré. Sur l'intégration algébrique des équations différentielles. *Comptes rendus de l'Académie des Sciences*, 112 :761–764, 1891.

[126] H. Poincaré. Sur l'intégration algébrique des équations différentielles du premier ordre et du premier degré. *Rend. Circ. Mat. Palermo*, 5 :161–191, 1891.

[127] M. J. Prelle and M. F. Singer. Elementary first integrals of differential equations. *Trans. Amer. Math. Soc.*, 279(1) :215–229, 1983.

[128] D. Richardson. Some undecidable problems involving elementary functions of a real variable. *J. Symbolic Logic*, 33 :514–520, 1968.

[129] J.-J. Risler. A bound for the degree of nonholonomy in the plane. *Theoret. Comput. Sci.*, 157(1) :129–136, 1996.

[130] J. F. Ritt. Prime and composite polynomials. *Trans. Amer. Math. Soc.*, 23(1) :51–66, 1922.

[131] W. Ruppert. Reduzibilität Ebener Kurven. *J. Reine Angew. Math.*, 369 :167–191, 1986.

[132] P. Samuel. Travaux de Zariski sur le 14e problème de Hilbert. In *Séminaire Bourbaki, Vol. 2*, pages Exp. No. 99, 441–446. Soc. Math. France, Paris, 1995.

[133] P. Scheiblechner. On the complexity of deciding connectedness and computing Betti numbers of a complex algebraic variety. *J. Complexity*, 23(3) :359–379, 2007.

[134] J. Schicho. A note on a theorem of Fried and MacRae. *Arch. Math. (Basel)*, 65(3) :239–243, 1995.

[135] A. Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier.

[136] D. Schlomiuk. Algebraic and geometric aspects of the theory of polynomial vector fields. In *Bifurcations and periodic orbits of vector fields (Montreal, PQ, 1992)*, volume 408 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 429–467. Kluwer Acad. Publ., Dordrecht, 1993.

[137] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. Assoc. Comput. Mach.*, 27(4) :701–717, 1980.

[138] T. W. Sederberg. Improperly parametrized rational curves. *Computer Aided Geometric Design*, 3(1) :67–75, 1986.

[139] M. F. Singer. Liouvillian first integrals of differential equations. *Trans. Amer. Math. Soc.*, 333(2) :673–688, 1992.

[140] Y. Stein. The total reducibility order of a polynomial in two variables. *Israel J. Math.*, 68(1) :109–122, 1989.

[141] G. Turnwald. On Schur's conjecture. *J. Austral. Math. Soc. Ser. A*, 58(3) :312–357, 1995.

[142] A. van den Essen, J. Moulin Ollagnier, and A. Nowicki. Rings of constants of the form $k[f]$. *Comm. Algebra*, 34(9) :3315–3321, 2006.

[143] A. Vistoli. The number of reducible hypersurfaces in a pencil. *Invent. Math.*, 112(2) :247–262, 1993.

[144] S. Walcher. On the Poincaré problem. *J. Differential Equations*, 166(1) :51–78, 2000.

[145] S. Watt. Functional decomposition of symbolic polynomials. In *International Conference on Computational Sciences and its Applications*, pages 353–362. IEEE Computer Society, 2008.

[146] S. Watt. Algorithms for the functional decomposition of laurent polynomials. In *Conferences on Intelligent Computer Mathematics 2009 : 16th Symposium on the Integration of Symbolic Computation and Mechanized Reasoning and 8th International Conference on Mathematical Knowledge Management , (Calculemus 2009)*, pages 186–200. Springer-Verlag LNAI 5625, 2009.

[147] J.-A. Weil. Constantes et polynômes de darboux en algèbre différentielle : applications aux systèmes différentiels linéaires. Thèse de l'école Polytechnique, 1995.

[148] M. Weimann. A lifting and recombination algorithm for rational factorization of sparse polynomials. *J. Complexity*, 26(6) :608–628, 2010.

[149] O. Zariski. Interprétations algébrico-géométriques du quatorzième problème de Hilbert. *Bulletin des Sciences Mathémattiques*, 78 :155–168, 1954.

[150] R. Zippel. Rational function decomposition. In *Proceedings of the 1991 international symposium on Symbolic and algebraic computation*, pages 1–6. ACM Press, 1991.

[151] R. Zippel. *Effective polynomial computation*. Kluwer Academic Publishers, 1993.

[152] H. Żołądek. Algebraic invariant curves for the Liénard equation. *Trans. Amer. Math. Soc.*, 350(4) :1681–1701, 1998.

[153] H. Żołądek. Multi-dimensional Jouanolou system. *J. Reine Angew. Math.*, 556 :47–78, 2003.