Etude algébrique et algorithmique des singularités des équations différentielles implicites

Evelyne Hubert

Thèse

présentée par

Evelyne HUBERT

pour obtenir le titre de Docteur

de l'Institut National Polytechnique Grenoble

(arrêtés ministériels du 5 juillet 1984 et du 30 mars 1992)

Spécialité : Mathématiques Appliquées

Étude Algébrique et Algorithmique des Singularités des Équations Différentielles Implicites

---

Date de soutenance : 23 avril 1997

Composition du jury

Président :	Pr. Bernard MALGRANGE
Rapporteurs :	Pr. Michael SINGER
	Pr. Daniel LAZARD
Examinateurs :	Pr. Jacques BLUM
	Pr. Jean DELLA DORA

Thèse préparée au sein du
Laboratoire de Modélisation et de Calcul
(Informatique et Mathématiques Appliquées de Grenoble)

Puisque la Terre est ronde et que l'espace est courbe, le bout du monde est l'endroit juste derrière soi.

J. Meunier.

Préface

Nous proposons quelques algorithmes pour étudier l'ensemble des solutions des équations différentielles algébriques, ordinaires ou aux dérivées partielles. Cet ensemble se scinde en solutions générales et en solutions singulières. Ces notions peuvent être définies de manière rigoureuse dans le cadre de l'algèbre différentielle, une théorie fondée par J.F.Ritt.

Avant d'entrer dans cette théorie algébrique, nous avons tenu à comprendre l'interprétation analytique des problèmes posés par les solutions singulières. Celle-ci est d'autant plus intrigante qu'elle est à l'origine du travail fondateur de J.F.Ritt et qu'elle a été quelque peu délaissée depuis. Dans l'introduction, nous présentons donc les motivations analytiques de ce travail ainsi qu'un résumé en termes accessibles du travail accompli.

Dans la deuxième partie de ce mémoire nous présentons des éléments de cette théorie. Nous avons voulu y séparer clairement les résultats purement algébriques des aspects algorithmiques, bien qu'ils soient interdépendants.

Ceci nous permet tout d'abord de mettre en évidence les équivalents de l'algèbre polynomiale - théorème de la base, décompositions en idéaux premiers... . Ce sont ces résultat qui permettent de donner une définition algébrique des solutions des systèmes différentiels. La définition de la solution générale d'une équation différentielle s'obtiendra naturellement dans ce contexte, et c'est là la motivation de cette présentation.

D'autre part, nous avons souhaité montrer comment obtenir un algorithme de décomposition effectif en modifiant très légèrement l'algorithme théorique de Ritt (Chapitre F). L'algorithme obtenu est en fait une version allégée de l'algorithme Rosenfeld-Gröbner de F.Boulier. Les principes mis en œuvre lui sont d'ailleurs très largement empruntés. Cependant le lien entre l'algorithme de Ritt et l'algorithme de F.Boulier n'avait pas encore été établi à ma connaissance.

Si le regain d'intérêt scientifique de ces dernières années a permis d'aboutir à des algorithmes effectifs, il reste néanmoins des problèmes ouverts tels la détermination de la décomposition minimale et le calcul de bases différentielles, qui est équivalent au problème d'inclusion.

Dans la dernière partie de ce mémoire nous avons voulu répondre à ces deux questions pour les équations différentielles, c'est à dire pour les systèmes différentiels constitués d'une seule équation.

Nous avons établi des algorithmes et leur implantation pour déterminer la décomposition minimale. Au cœur de cette détermination se tient le très difficile Théorème des petites puissances. La réalisation effective est soutenue par l'algorithme Rosenfeld-Gröbner.

En outre, nous proposons un algorithme et quelques critères qui permettent de calculer dans certains cas les bases différentielles des composantes essentielles. Le point bloquant de cet algorithme est le *problème de Ritt*.

Pour exposer ces algorithmes nous avons adopté un ordre qui nous fait découvrir au fur et à mesure les démonstrations de nécessité et de suffisance du Théorème des petites puissances.

L'algorithme effectif de décomposition minimale le plus direct est exposé dans le paragraphe G . Nous prolongeons l'algorithme Rosenfeld-Gröbner pour obtenir une décomposition en idéaux premiers, comme celle de Ritt. On peut alors appliquer le Théorème des petites puissances pour éliminer les composantes redondantes. Un algorithme plus fin, qui évite les factorisations, requiert plus d'expertise sur les conditions de suffisance et de nécessité. Quant à l'algorithme de calcul des bases différentielles, il réclame une relecture encore plus poussée de la nécessité.

Aussi avons-nous choisi de présenter dans le Chapitre H notre algorithme de calcul de bases différentielles, puis dans le Chapitre I notre deuxième algorithme de décomposition minimale.

Après avoir maîtrisé ces démonstrations nous pourrons établir au Chapitre J quelques critères pour résoudre le problème de Ritt et donc nous permettre de calculer dans plus de cas les bases différentielles.

La dernière partie de ce mémoire est relativement indépendante et est consacrée à l'étude des équations différentielles ordinaires du premier ordre. Pour de telles équations nous savons toujours calculer une base différentielle de la solution générale. Nous proposons un algorithme plus simple que dans le cas général pour ce faire (Paragraphe N.1). Nous verrons que cette base différentielle nous permet d'apporter une expertise sur les points singuliers des solutions non singulières (Paragraphe N.3).

Aussi, dans cette partie nous exposerons au préalable les analyses, géométriques et analytiques, déjà existantes pour l'étude des points singuliers des équations différentielles du premier ordre. Celles-ci sont cependant insuffisantes lorsqu'il s'agit de considérer les solutions dans leur globalité. D'où l'intérêt d'une approche algébrique.

Table des matières

I Introduction **13**

A Motivations **15**

A.1 Premiers méfaits 15

A.2 Solutions singulières essentielles et particulières 17

B Histoires singulières **23**

B.1 L'âge de la solution singulière 23

B.2 Algèbre différentielle 25

B.3 Le Théorème des Petites Puissances 27

C Résumé **31**

C.1 La solution générale 31

C.2 Algèbre différentielle 32

C.3 Les décompositions minimales 33

C.4 Le calcul de bases différentielles 34

C.5 Équations différentielles du premier ordre 34

D Les problèmes ouverts **37**

D.1 Propriétés enveloppantes des solutions singulières 37

D.2 Solutions particulières 43

II Algèbre et Algorithmes pour les systèmes différentiels **47**

E Algèbre différentielle **49**

E.1 Anneaux différentiels 49
E.2 Anneaux de polynômes différentiels 53
E.3 Notion algébrique de solution 56
E.4 Idéaux quotients 59

F Les algorithmes de décomposition 61
F.1 Réduction 61
F.2 Cohérence et lemme de Rosenfeld 65
F.3 Décomposition en idéaux premiers 68
F.4 Décomposition en idéaux réguliers 70

III Équations différentielles algébriques 73

G Composantes essentielles 75
G.1 La composante générale 76
G.2 Le procédé de préparation 81
G.3 Le Théorème des Petites Puissances 84
G.4 Algorithme effectif et exemples 87

H Calcul des bases différentielles 89
H.1 Processus théorique 89
H.2 Le lemme de Levi 90
H.3 Le problème de Ritt 95

I Decomposition regulière minimale 101
I.1 Définition 101
I.2 Suffisance du Théorème des Petites puissances 103
I.3 Necessité du Théorème des Petites Puissances 104
I.4 Algorithme 106

J Retour sur le Problème de Ritt 109
J.1 A propos du calcul de bases differentielles 109
J.2 Quelques critères pour le problème de Ritt 112

J.3 Perspectives 114

IV Points singuliers des équations différentielles ordinaires du premier ordre 115

K Notations d'Algèbre 119

K.1 Variétés algébriques 119

K.2 Idéaux quotient 120

K.3 Décompositions 121

L Géométrie des équations différentielles du premier ordre 123

L.1 Courbes intégrales 123

L.2 Points singuliers 126

L.3 Courbes intégrales singulières 129

M Étude analytique 133

M.1 Points Cauchy 133

M.2 Points de branchement 134

M.3 Le polygone 135

N La solution générale 137

N.1 Calcul de la base de la composante générale 137

N.2 Série entières solutions 139

N.3 Développement en série des solutions non-singulières 140

Notations

$\mathbb{N}$, the set of natural integers.

$\mathbb{Z}$, the set of integers.

$\mathbb{Q}$, the set of rationnal numbers.

$\mathbb{C}$, the set of complex numbers.

$\mathcal{K}$, a field of characteristic zero.

$\bar{\mathcal{K}}$, an algebraic closure of a field $\mathcal{K}$.

$\Delta = \{\delta_1, \ldots, \delta_\mu\}$, a set of derivations (Section E.1).

Θ, a monoid of derivation operators (Section E.1).

$\mathcal{R}$, a differential ring that contains a field isomorphic to $\mathbb{Q}$ and which is Nœtherian w.r.t. to its radical differential ideal (Section E.1).

$\mathcal{R}\{Y\} = \mathcal{R}\{y_1, \ldots, y_n\}$, a ring of differential polynomials with coefficients in $\mathcal{R}$ (Section E.2).

$\mathcal{F}$, a differential field of characteristic zero.

$\mathcal{F}\{Y\} = \mathcal{F}\{y_1, \ldots, y_n\}$, a ring of differential polynomials with coefficients in $\mathcal{F}$.

$\deg m$, $\mathrm{wt} m$, the degree and the weight of a differential monomial m (Section E.2).

(Σ), the ideal generated by a set Σ of elements in a ring (Section F.1 and Section K).

$\langle\Sigma\rangle$, the radical ideal generated by a set Σ of elements in a ring (Section F.1 and Section K).

$[\Sigma]$, the differential ideal generated by a set Σ of elements in a differential ring (Section E.1).

$\{\Sigma\}$, the radical differential ideal generated by a set Σ of elements in a differential ring (Section E.1).

ΘY, the set of derivatives in $\mathcal{R}\{Y\}$ (Section E.2).

$\Theta_v Y$, the set of derivatives less or equal to a derivative v in $\mathcal{R}\{Y\}$ endowed with a ranking (Section F.1).

$\Theta_v \Sigma$, the set of all differential polynomials θq, where $q \in \Sigma$ and $\theta \in \Theta$, that have no derivative rnking higher than v (Section F.1).

$\Theta_\Sigma Y$, the set of derivatives present in the differential polynomials of a subset Σ of some $\mathcal{R}\{Y\}$ (Section F.1).

u_p, s_p, the leader and the separant of a differential polynomial p in a differential polynomial ring endowed with a ranking (Section F.1).

$\mathcal{G}_p$, the general component of an irreducible differential polynomial p (Section G.1).

$\Theta_\omega p$, the set of derivatives of p of order less or equal to an integer ω (Section H.2).

$\mathcal{G}_p^\omega$, the radical differential ideal generated by $(\Theta_\omega p) : s_p^\infty$ (Section H.1 and H.2).

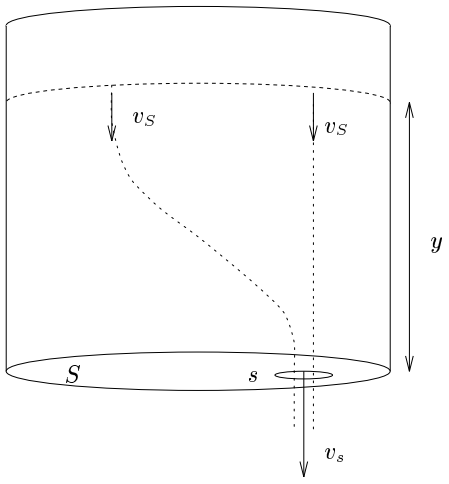
I

Introduction

A Motivations

A.1 Premiers méfaits

Considérons un seau cylindrique, plein d'eau, au fond duquel il y a un trou minuscule. Nous essayons de déterminer la hauteur d'eau y dans le seau en fonction du temps.



Le seau percé.

Constatons tout d'abord que la masse d'eau qui s'écoule correspond à la masse d'eau qui descend dans le seau.

$$S\,\rho\,\dot{y} = s\,\rho\,v_s,$$

où S est la surface d'une section du seau, s celle du trou; ρ est la masse volumique de l'eau et v_s la vitesse du fluide au sortir du seau.

Le long d'une ligne d'eau menant de la surface supérieure à la fuite, la loi de Bernoulli s'écrit

$$\frac{v_S^2}{2} + \frac{P}{\rho} + \rho g y = \frac{v_s^2}{2} + \frac{P}{\rho}.$$

Nous nous permettrons de négliger la vitesse du fluide sur la surface supérieure

v_S, étant donnée que $s \ll S$. L'équation différentielle satisfaite par la hauteur d'eau y est donc donnée par la loi de Toricelli, soit

$$\dot{y}^2 - 2\alpha y = 0 \qquad \text{où } \alpha = \frac{s^2}{S^2}\rho g.$$

Par les règles usuelles d'intégration, nous obtenons une solution qui, comme nous pouvions l'espérer, dépend d'une constante arbitraire c.

$$y(t) \;=\; \alpha\,(t-c)^2.$$

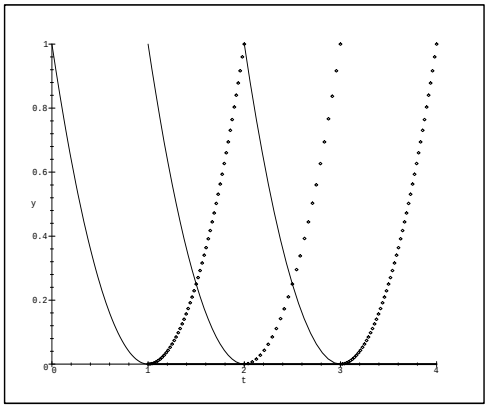
On voit aisément que l'équation admet également la solution $y = 0$ et, fait plus remarquable, cette solution ne s'obtient pas en donnant une valeur à la constante arbitraire c.

Nous dirons quelques fois que l'équation différentielle admet deux *types* de solutions. En outre $y = 0$ est une *solution singulière*, et, avant d'en préciser le sens exact, nous dirons que $y(t) \;=\; \alpha\,(t-c)^2$ est la *solution générale*

Constatons que la solution singulière que nous avons obtenue est une enveloppe des courbes définies par la solution générale. Le graphe de la solution singulière est donc contenu dans l'ensemble des points (x, y) pour lesquels le polynôme $y'^2 - 2\alpha y$ admet une racine double en y'.

A supposer que le seau soit plein, c'est-à-dire $y = 1$ au temps $t = 0$, il se vide donc selon la fonction $y(t) \;=\; \alpha\,(t-\frac{1}{\alpha})^2$. La hauteur d'eau suit donc une solution dans la solution générale. Le seau sera vide au temps $t = \frac{1}{\alpha}$, suite à quoi il restera vide. La hauteur d'eau quitte donc la solution générale pour suivre la solution singulière.

Ce saut de la solution générale à la solution singulière se fait de façon continue et différentiable grâce aux propriétés enveloppantes de la solution singulière. La solution physique est donc différentiable.



Une fois le seau vide, il reste vide!

Constatons que du point de vue mathématique, une fois le seau vide (y=0) il y avait une infinité de possibilités pour obtenir une solution différentiable.

On pourrait objecter à la validité de ce modèle non déterministe que lorsqu'il ne reste que très peu d'eau dans le seau il faut considérer d'autres phénomènes physiques. Cependant, une modélisation non-linéaire, en tenant compte des solutions singulières, simplifie l'étude sur toute la durée.

A.2 Solutions singulières essentielles et particulières

Équations différentielles algébriques du premier ordre

Soit donc une équation différentielle algébrique

$$(E_1) \quad p\,(x,\, y,\, y') \;=\; 0.$$

C'est dire que p est polynomiale en y et y'.

Une solution de cette équation est singulière si elle satisfait l'équation différentielle obtenue comme la dérivée partielle de p par rapport à y',

$$(E_1') \quad \frac{\partial p}{\partial y'}\,(x,\, y,\, y') \;=\; 0.$$

Aussi, une solution singulière satisfait-elle l'équation algébrique obtenue en e'liminant y' entre p et $\frac{\partial p}{\partial y'}$. Soit

$$(E_0) \quad r(x,\, y) \;=\; 0.$$

Si la *solution générale* de (E_1) admet une enveloppe, alors cette enveloppe est une solution singulière de (E_1), comme nous l'avons présenté dans l'exemple précédent. Mais qu'en est il de la réciproque?

EXEMPLE: Soit l'équation différentielle

$$(E_1) \quad y'^3 - 4\,x\,y\,y' + 8\,y^2 \;=\; 0.$$

Les solutions singulière doivent satisfaire

$$3\,y'^2 - 4\,x\,y \;=\; 0$$

et par conséquent

$$y\,\left(27\,y - 4x^3\right) \;=\; 0.$$

Nous vérifions que

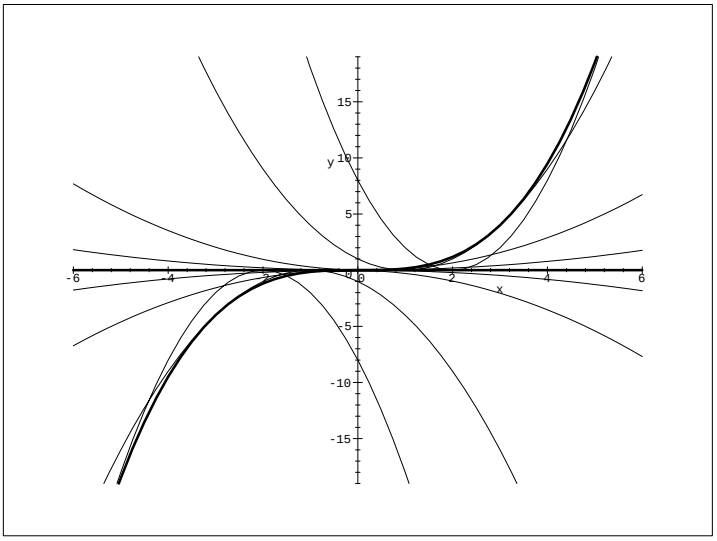
$$\bar{y}(x) = 0 \quad \text{et} \quad \tilde{y}(x) = \frac{4}{27}x^3$$

sont solutions. Ce sont donc les deux solutions singulières de l'équation différentielle considérée.

La solution générale est elle donnée par

$$\hat{y}(x) \;=\; a\;(x-a)^2$$

où a est une constante arbitraire. Nous représentons quelques un de ces solutions ainsi que les solutions singulières.



$$y'^3 - 4\,x\,y\,y' + 8\,y^2 = 0$$

Nous constatons que les deux solutions singulières touchent tangentiellement les courbes de la solution générale. Il y a un contact du premier ordre. Mais il faut également remarquer que les paraboles de la solution générale s'évasent et tendent vers la solution singulière $\bar{y}(x) = 0$.

De même que dans l'exemple précédent, $\tilde{y}(x) = \frac{4}{27}x^3$ ne s'obtient à partir de $\hat{y}(x) = a\,(x+a)^2$ pour aucune valeur de a. Au contraire, lorsque $a = 0$ on obtient la deuxième solution singulière, $\bar{y}(x) = 0$. Nous qualifierons $\tilde{y}(x) = \frac{4}{27}x^3$ de *solution singulière essentielle* et $\bar{y}$ de *solution singulière particulière*, ou simplement de solution particulière.

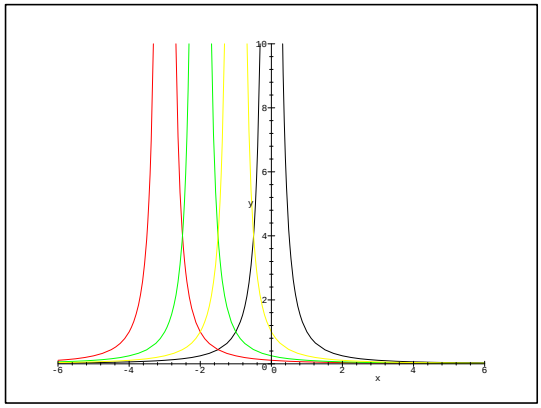
EXEMPLE: Considérons à présent un exemple où la distinction est moins aisée. Soit l'équation différentielle

$$y'^2 - 4\,y^3 \;=\; 0.$$

Nous vérifions aisément que $\bar{y}(x) = 0$ est l'unique solution singulière. Il est d'autre part simple de trouver la solution générale de cette équation

$$\hat{y}(x) \;=\; \frac{1}{(x-a)^2}$$

où a est une constante arbitraire. Nous représentons quelques unes de ces solutions.



$$y'^2 - 4\,y^3 = 0$$

$\bar{y}(x) = 0$ n'est pas l'enveloppe des solutions non singulières. Quant à être obtenue en spécialisant a, il faut considérer a infini. Mais remarquons le simple fait, qui était également exact dans l'exemple précédent:

Le développement de Taylor de $\hat{y}(x) = \frac{1}{(x-a)^2}$ en $x = 0$ est donné, lorsque $a \neq 0$, par

$$\hat{y}(x) \;=\; \frac{1}{a^2} + \frac{2}{a^3}\,x + \frac{3}{a^4}\,x^2 + \cdots \;=\; \sum_{n\geq 0} \frac{n+1}{a^{n+2}}\,x^n.$$

Soit ϵ un réel quelconque et N un entier positif quelconque. Il est possible de trouver a, de sorte que tous les coefficients de cette série de Taylor jusqu'à l'ordre N soient inférieur à ϵ. En $x = 0$ la série de Taylor de la solution singulière peut être approchée à tout ordre par la série de Taylor d'une solution non singulière. Ceci est également vrai pour tout réel x_o. Nous dirons que la solution singulière peut être approchée à tous les ordres par des solutions non singulières[1].

C'est dans ce sens que nous devons comprendre ce qu'est une solution particulière, d'autant plus que la solution singulière ne peut pas toujours être trouvée sous forme close.

Équations différentielles algébriques d'ordre supérieur

Soit une équation différentielle algébrique

$$(E_n) \quad p\left(x,\, y,\, y',\, \ldots,\, y^{(n)}\right) \;=\; 0.$$

C'est dire que p est polynomial en y et ses dérivées.

Une solution de cette équation est singulière si elle satisfait l'équation différentielle obtenue comme la dérivée partielle de p par rapport à la dérivée de plus grand ordre

$$(E'_n) \quad \frac{\partial p}{\partial y^{(n)}}\left(x,\, y,\, y',\, \ldots,\, y^{(n)}\right) \;=\; 0.$$

Ainsi, une solution singulière satisfait une équation d'ordre inférieur à n qui est le résultat de l'élimination de $y^{(n)}$ entre p et $\frac{\partial p}{\partial y^{(n)}}$. Soit

$$(E_m) \quad r\left(x,\, y,\, y',\, \ldots,\, y^{(m)}\right) \;=\; 0, \qquad m < n.$$

Exemple : Soit l'équation différentielle ordinaire

$$(E_2) \quad 4\,y'^2\,y''^2 - 16\,y'^2\,y'' + 12\,y'^2 + 16\,y \;=\; 0$$

Les solutions singulières doivent satisfaire

$$(E'_2) \quad 8\,y'^2\,y'' - 16\,y'^2 \;=\; 0$$

et donc

$$(E_1) \quad y'^2 - 4y \;=\; 0.$$

Notons que (E_1) admet deux types de solutions : $\hat{y}(x) = (x + a)^2$, la solution générale, et $\bar{y}(x) = 0$, la solution singulière. Toutes deux sont solutions singulières

[1] Pour plus de précision, il faut se référer à la définition de l'adhérence donnée par Ritt [Rit66, chapitre VI]

de (E_2). Mais comme nous le montrons dans l'exemple suivant, il se pourrait qu'aucune ou juste une de ces solutions soit solution de (E_2).

EXEMPLE : Soit l'équation

$$(E_2) \quad (1+x^2)\,y'^2 - \left(2\,x\,y' + \frac{x^2}{2}\right)\,y'' + y'^2 + x\,y' \;=\; 0.$$

S'il existe des solutions singulières, elles doivent vérifier

$$(E_2') \quad 2\,(1+x^2)y' - \left(2\,x\,y' + \frac{x^2}{2}\right) \;=\; 0$$

et par conséquent

$$(E_1) \quad 16\,y'^2 + 16\,x\,y' + 8\,x^3\,y' + 16\,x^2\,y - x^4 \;=\; 0.$$

Remarquons que (E_1) admet une solution singulière $\tilde{y}(x) = \frac{1}{16}\,(x^4 + 4\,x^2)$ qui n'est pas solution de (E_2).

Reste à déterminer s'il y a des solutions communes à (E_1) et (E_2). On peut faire un parallèle entre cette question et le problème algébrique qui est de savoir quand un ensemble de polynômes admet des zéros communs.

Quant à déterminer les propriétés enveloppantes des solutions singulières, nous verrons, dans un paragraphe suivant, que la difficulté croit avec l'ordre.

B Histoires singulières

B.1 L'âge de la solution singulière

Il revient à Gaston Darboux d'avoir défini les solutions singulières d'une équation différentielle

$$p(x, y, y') = 0$$

comme les solutions de cette équation qui satisfont de surcroît

$$\frac{\partial p}{\partial y'}(x, y, y') = 0.$$

Cette définition fut d'abord controversée puisqu'elle rompait avec la définition alors admise.

En effet, dans un mémoire adressé a l'Académie des sciences de Paris en 1734, Claude Clairaut constatait qu'*il y a des équations différentielles qu'on peut intégrer par la différenciation, et que les intégrales trouvées de la sorte ne sont jamais comprises dans les intégrales complètes que donnent les règles ordinaires de l'intégration, quoique d'ailleurs ces mêmes intégrales satisfassent aux équations différentielles proposées.*

Bien que constatées dans de nombreux calculs de géométrie analytique, les solutions singulières furent considérées comme un paradoxe qu'il fallait démêler. Cependant, Euler et d'Alembert avaient déjà établi quelques règles pour déterminer si une solution de l'équation différentielle est comprise ou non dans l'intégrale complète de cette équation différentielle, sans connaître cette intégrale.

Dans son Mémoire pour l'Académie des Sciences de 1772, Pierre-Simon Laplace formule les deux aspects soulevés par les solutions singulières. Pour une équation différentielle donnée d'un ordre quelconque, il s'agit de

- déterminer toutes les solutions singulières,
- déterminer si l'intégrale complète d'une équation d'ordre inférieur est dans la solution générale.

Que le premier problème mentionné soit encore irrésolu tient à la définition encore admise que les solutions singulières s'obtiennent en éliminant la constante arbitraire de la solution générale.

Il revient à Lagrange d'avoir élevé le phénomène des solutions singulières en théorie. Dans son mémoire pour l'Académie royale des Sciences et Belles-Lettres de Berlin en 1774, Lagrange interroge l'origine et la nature des solutions singulières et montre, que loin d'être des exceptions, elles apparaissent naturellement dans les calculs.

La définition de la solution singulière commence alors à s'affranchir de l'intégrale complète : sont considérées comme singulières les solutions qui ne peuvent pas être complétées par une constante arbitraire. Une solution ϕ est singulière s'il n'existe pas de solution sous la forme $\phi + c\,\xi$ où c est une constante arbitraire et ξ une fonction de x et c. C'est l'esprit précurseur des solutions singulières essentielles d'aujourd'hui. Dans ce même mémoire sont présentées des heuristiques pour déterminer si une solution est singulière.

En 1806 Poisson dépasse le cadre de la géométrie où les solutions singulières s'étaient alors cantonnées. Au travers de systèmes dynamiques, il montre que l'existence d'une solution singulière ôte le déterminisme au modèle mathématique. Dans son mémoire présenté au Journal de l'École Polytechnique, il reprend les problèmes posés par Laplace et développés par Lagrange. Il fait de plus cette remarque étonnante sur la nature des solutions singulières des équations différentielles du premier ordre : *les solutions singulières*[1] *d'une équation différentielle ne sont autre chose que des facteurs algébriques que l'on peut mettre en évidence, et séparer entièrement de cette équation par une transformation convenable.*

La définition de la solution singulière admise au début du $XIX^{\text{ème}}$ siècle figure que toute équation différentielle admet une intégrale complète du type $f(x, y, a) = 0$, où f est une fonction exprimable dans les termes de l'analyse connue et a une constante arbitraire. On en retiendra l'idée que la solution singulière ne peut être correctement définie qu'en ayant défini au préalable la solution générale.

En 1893 Hamburger mit en évidence que les solutions singulières définies par Monsieur Darboux ne correspondait pas toujours à l'esprit dans lequel elles avaient été définies, c'est à dire comme enveloppes de courbes.

1734 Clairaut, dans un mémoire pour l'Académie des Sciences relève l'existence de solutions d'équations différentielles qui ne sont pas comprises dans l'intégrale complète que donne les règles ordinaires de l'intégration.

1756 Un mémoire pour l'Académie des Sciences d'Euler illustre ce *paradoxe* du calcul intégral dans plusieurs exemples tirés de la géométrie.

[1] à l'époque, on parle de solution particulière. Nous avons remplacé ce terme pour ne pas prêter à confusion avec son sens moderne.

1769 D'Alembert donne les premières formules pour déterminer si une solution d'une équation différentielle est comprise ou non dans l'intégrale complète, sans connaître cette intégrale. Les méthodes paraissent dans les publications de l'Académie des sciences.

1772 Laplace *Mémoire sur les solutions particulières des équations différentielles et sur les inégalités séculaires des planètes*, Mémoires de l'Académie des Sciences (ou Œuvres complètes, tome VIII)

1774 Lagrange, *Sur les Intégrales particulières des Équations différentielles*, Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin (ou Œuvres complètes, tome IV).

1779 Lagrange *Sur Différentes questions d'analyse relatives à la théorie des intégrales particulières*, Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin (ou Œuvres complètes, tome IV).

1806 Poisson *Mémoire sur les solutions particulières des équations différentielles et des équations aux différences*, Journal de l'École Polytechnique.

1870 Darboux, *Sur les solutions singulières des équations aux dérivées ordinaires du premier ordre*, Bulletin des Sciences Mathématiques et Astronomiques.

1873 Cayley, *On the theory of the Singular Solutions of Differential Equations of the First Order*, Messenger of Mathematics.

1893 Hambuger, *Über die singulären Lösungen der algebraischen Differenzialgleichnungen ester Ordnung*, Journal für die reine und angewandte Mathematik, volume 112.

B.2 Algèbre différentielle

Il y a peu de doute que ce soit l'École française qui motiva Joseph Fels Ritt dans ses premiers travaux sur les équations différentielles algébriques. Précisons qu'il s'agit alors d'équations différentielles qui se présentent sous la forme de polynômes, en les inconnues et leurs dérivées, à coefficients dans le corps des fonctions méromorphes.

L'idée que la solution singulière peut se factoriser dans l'équation a permis de définir, dès les premiers articles sur le sujet en 1930, la solution générale [Rit30].

Le premier objectif de Ritt fut en effet de trouver les équivalents différentiels de la géométrie algébrique. La décomposition des variétés de fonctions analytiques, solutions d'un système d'équations différentielles ordinaires, en variétés irréductibles permet de classifier les différents types de solutions.

La solution générale est donc l'unique variété de fonctions sur laquelle le *séparant*, c'est-à-dire la dérivée partielle de l'équation par rapport à la dérivée la plus haute, ne s'annule pas.

Une difficulté à circonvenir est la non existence de clôture différentielle algébrique. On introduira les *extensions différentielles universelles*, comme le corps des fonctions analytiques, qui à défaut de contenir toutes les solutions, en contiennent suffisamment pour permettre de discuter les propriétés globales d'un système d'équations différentielles.

La formulation purement algébrique sera développée dans les années 40 par Raudenbush [Rau33]. Ce langage remplacera celui de l'analyse complexe dans les démonstrations. Il permettra aussi de contourner les problèmes liés à l'existence des extensions différentielles; la décomposition des variétés solutions trouve son écho dans la décomposition des idéaux différentiels radiciels en idéaux différentiels premiers. Dès lors, la solution générale est définie par l'ensemble des équations différentielles qu'elle satisfait. Cet ensemble est un idéal différentiel premier.

La théorie algébrique permet d'étendre les principes à des anneaux de coefficients abstraits. De plus, elle permet d'unifier l'étude des équations différentielles aux dérivées partielles à celle des équations différentielles ordinaires. Au lieu de considérer un unique opérateur de dérivation agissant sur un anneau, on en considère simplement plusieurs. Cela ne va certes pas sans quelques difficultés supplémentaires. Mais, tous les résultats *ordinaires* trouveront leurs équivalents *partiels*, y compris la définition et les résultats sur la solution générale et les solutions singulières d'une équation différentielle algébrique.

Pour mener les démonstrations, Joseph Fels Ritt mit en place une généralisation de la réduction et de l'élimination. Celle-ci se développait alors dans les algèbres polynomiales autour de la notion de résultant.

L'élaboration de cette théorie repose sur les idées et les heuristiques de Riquier et Janet. Elle permet un traitement systématique, mais parfois uniquement théorique, des systèmes d'équations différentielles. Modulo des opérations algébriques, telle la factorisation dans des tours d'extensions, on peut décider si un système d'équations différentielles admet une solution (le test de trivialité) et si une équation va s'annuler sur toutes les solutions de ce système (le test d'appartenance à l'idéal différentiel radiciel).

Notons que, contrairement à l'algèbre polynomiale où les deux tests précédents, relatifs à un idéal, peuvent s'effectuer grâce à une base de Gröbner unique, le procédé complet d'élimination en algèbre différentielle comporte des décompositions. Aussi, les propriétés - trivialité, appartenance, dimension ... - d'un idéal différentiel radiciel sont lues sur un nombre fini d'*ensembles caractéristiques*. L'existence et les propriétés des ensembles caractéristiques sont au cœur des démonstrations à travers tout l'algèbre différentielle.

Indépendamment, Seidenberg proposa une théorie alternative de l'élimination. [Sei56]. Cette théorie permet de tester l'appartenance et la trivialité. On perd néanmoins les informations procurées par une représentation par des ensembles caractéristiques.

Ce sont essentiellement ces notions algorithmiques, pas toujours effectives, qui ont retenu l'attention scientifique ces dernières années.

La méthode de Seidenberg fut améliorée et implantée par S.Diop [Dio89]. Reprenant les idées mises en œuvre et avec la complicité d'un lemme de Rosenfeld et un lemme de Lazard, F.Boulier [Bou94] a aboutit à un algorithme qui permet une décomposition ayant des propriétés d'une nature voisine à celle de Ritt.

En restant sur l'approche de Ritt, K.Rody a également obtenu une décomposition similaire pour les équations différentielles ordinaires.

Des approches complètement différentes de celles de Ritt et de Seidenberg ont également été abordées. L'idée sous-jacente est de généraliser l'algorithme de Bucheberger pour le calcul des bases de Gröbner. À notre connaissance ces études ont été menées de front par G.Carra-Ferro, F.Ollivier et E.Mansfield. Nous devons cependant admettre notre manque d'expertise sur ce domaine.

Les décompositions obtenues, que ce soit la décomposition théorique de Ritt, ou effective de Boulier, ne sont pas minimales. Un moyen d'en extraire une décomposition minimale serait de tester l'inclusion de deux idéaux différentiels premiers définis par leurs ensembles caractéristiques. Ceci est un problème ouvert.

Dans le cas d'une unique équation différentielle, trouver la décomposition minimale revient à décider quelles sont les solutions singulières essentielles. Par une approche différente de celle de l'inclusion de deux idéaux, Ritt a répondu à cette question avec le Théorème des Petites Puissances (*Low Power Theorem* dans la langue originelle). C'est ce que nous nous proposons de développer et d'implanter dans ce mémoire.

B.3 Le Théorème des Petites Puissances

Nous avons vu dans le Paragraphe A.2 que l'on pouvait distinguer dans les solutions singulières d'une équation différentielle du premier ordre les solutions singulières essentielles des solutions particulières. Cette distinction induit un comportement différent des solutions non singulières dans leur voisinage.

Il revient en effet à Hamburger d'avoir montré, dans le cas des équations différentielles du premier ordre, que les premières étaient des enveloppes des solutions non singulières alors que les secondes pouvaient être approchées à tout ordre par des solutions non singulières.

Reconsidérons deux exemples du chapitre A . Soient donc

$$(\mathrm{E}_1) \quad y'^2 - 2\,\alpha\, y = 0$$

et

$$(\mathrm{E}'_1) \quad y'^2 - 4\,y^3 = 0.$$

$y = 0$ est l'unique solution singulière de ces deux équations. Dans (E_1) c'est une solution singulière essentielle, alors que dans (E'_1) c'est une solution particulière. Pouvons nous à la lecture des équations déterminer cette distinction?

La réponse est relativement simple à énoncer. En considérant $y'^2 - 2\,\alpha\, y$ comme un polynôme en y et y', nous constatons que le terme de plus petit degré ne fait intervenir que y. Au contraire, dans $y'^2 - 4\,y^3$, le terme de plus petit degré contient une dérivée de y.

Dans les équations d'ordre plus élevé, le critère pour déterminer si $y = 0$ est une solution singulière essentielle recourt de la même simplicité : soit une équation différentielle d'ordre $n > 0$, polynômiale en y et ses dérivées

$$(\mathrm{E}_n) \quad p(x, y, y', \ldots, y^{(n)}) \;=\; 0$$

qui admette $y = 0$ comme solution. $y = 0$ est une solution singulière essentielle si, et seulement si, le terme de plus petit degré ne contient que y, et aucune dérivée propre de y.

Supposons donc qu'une solution singulière de (E_n) soit définie par une équation différentielle (E_m) d'un ordre m inférieur à n. Pour déterminer si la solution générale de (E_m) est une solution singulière essentielle de (E_n), il faudra réécrire préalablement l'équation (E_n) en fonction de (E_m). Modulo cette réécriture, le critère reste le même. C'est le tandem du Procédé de Préparation et du Théorème des Petites Puissances.

La simplicité de ce critère est frappante comparée à la difficulté des preuves qui font du Théorèmes des Petites Puissances un des théorèmes les plus aboutis de l'algèbre différentielle. De plus, le goût algébrique de ce critère semble en complète contradiction avec la nature de la première démonstration proposée par Joseph Fels Ritt dans son papier de 1936 [Rit36].

En effet la démonstration de la suffisance y était abordé par des transformations de Painlevé, une technique d'analyse pour l'étude des singularités. Quant à la nécessité, il est assez amusant de voir qu'elle repose, en quelque sorte, sur la définition que Lagrange donnait des solutions singulières. Lorsque $y = 0$ est solution, mais que les termes de plus petit degré de l'équation différentielle contiennent des dérivées de y, on peut construire une série *formelle* d'une constante

$$\xi_1(x)\, c^{\rho} + \xi_2(x)\, c^{\rho+1} + \cdots$$

qui soit solution de l'équation.

Les preuves ont cependant gagné un peu en lisibilité grâce à leur algébrisation. Le chapitre IV de la bible de l'algèbre différentielle écrite par Elis Kolchin [Kol73] est pratiquement tout entier consacré à ce théorème. Il donne l'exposé le plus récent et le plus global des preuves apportées par Howard Levi, pour la nécessité, et A. Hillman, pour la suffisance.

En effet, en 1942 Howard Levi [Lev42] apporte la première pierre pour algébriser la preuve. Cette pierre consiste à déterminer les monômes qui appartiennent à l'idéal différentiel $[y^\rho]$. Avec ce résultat il montre qu'on peut factoriser l'équation différentielle définissant la solution singulière. La méthode n'a rien de commun avec la proposition de Poissson que nous avons mentionnée ci-dessus. Il ne s'agit pas d'obtenir la factorisation par le biais d'une transformation. Ceci relèverait plus d'une approche géométrique et nous n'avons pas connaissance d'un résultat plus récent de cette sorte. La factorisation obtenue par H.Levi se fait en combinant les dérivées de l'équation.

La preuve de suffisance est généralisée au Théorème du coefficient de tête montré par Hillman et Mead [HM62], [Hil43]. On y retrouve le polygone introduit par Ritt pour construire la solution série d'une constante.

A nouveau, les démonstrations algébriques vont permettent d'étendre les résultats aux équations différentielles partielles. Pour la nécessité, il suffit, mais cela n'est pas trivial, d'étudier les monômes $[y^\rho]$ dans le cas où il y a plusieurs dérivations.

Ainsi, pour une équation aux dérivées partielles, il est possible de déterminer si une équation différentielle d'ordre inférieur définit une solution singulière essentielle. Mais lorsqu'on considère des équations aux dérivées partielles ou des équations avec plusieurs indéterminées différentielles, une solution singulière peut être définie par plusieurs équations. Illustrons notre propos par l'exemple suivant.

Exemple: Soit l'équation aux dérivées partielles

$$x\,u_x^2 + u_y^2 - u \;=\; 0$$

Les procédés d'élimination dont nous avons parlé ci-dessus déterminent deux solutions singulières. L'une est $u = 0$. D'après le Théorème des Petites Puissances, c'est une solution singulière essentielle. L'autre satisfait à

$$\left\{ \begin{array}{rcl} u_x & = & 0 \\ u_y^2 - u & = & 0 \end{array} \right.$$

et nous somme bien en mal d'appliquer le même théorème.

La généralisation de tout le procédé aux équations différentielles partielles et aux équations ayant plusieurs indéterminées différentielles, ne peut être valable sans le résultat de J.F. Ritt : toute solution singulière essentielle d'une équation différentielle est la solution générale d'une équation différentielle d'ordre inférieur [Rit45b]. Aussi dans l'exemple précédent savons nous que la solution singulière définie par le système de deux équations n'est pas essentielle.

C Résumé

C.1 La solution générale

Naturellement, les solutions non singulières d'une équation différentielle, ordinaire ou aux dérivées partielles, font partie de la solution générale de cette équation. Et c'est à présent un lieu commun de dire qu'elles ne peuvent pas toujours être exprimées sous forme close.

Mais considérons l'ensemble des équations algébriques différentielles que les solutions non singulières satisfont. Cet ensemble peut être compris comme un *idéal différentiel radiciel*.

Il se peut qu'une solution singulière satisfasse toutes ces équations. C'est ainsi qu'on peut définir algébriquement la notion de solution particulière. A travers la notion *d'adhérence* introduite par Ritt [Rit66, chapter IV], cette définition est en accord avec l'idée que nous avons donnée : dans le cas des équations algébriques différentielles ordinaires à coefficients dans le corps des fonctions méromorphes, les solutions singulières particulières peuvent être approchées à tout ordre par des solutions non singulières.

Une *base différentielle* de la solution générale est un ensemble fini d'équations algébriques différentielles qui engendrent l'idéal différentiel définissant la solution générale. En d'autres mots, si une équation fait partie de cet idéal, alors une de ses puissances peut être exprimée comme la combinaison linéaire des équations de la base et de leurs dérivées. L'existence d'une telle base est donnée par le *Théorème de la base* de Ritt et Raudenbush.

Nous avons obtenu les équations différentielles définissant les solutions singulières par des procédés d'élimination. Dans un exemple nous avons de plus constaté que si l'équation définissant une solution singulière admettait elle-même une solution singulière, celle-ci n'était pas forcément solution de l'équation de départ.

En effet, c'est un résultat que nous avons déjà mentionné, une solution singulière essentielle d'une équation différentielle est la solution générale d'une équation différentielle d'ordre inférieur.

Nous voyons donc à combien de titres une définition rigoureuse de la solution

générale est primordiale dans l'étude des solutions des équations différentielles algébriques.

C.2 Algèbre différentielle

Dans la deuxième partie de ce mémoire nous décrirons les deux aspects de l'algèbre différentielle qui constituent les équivalents différentiels de

- la bijection entre les idéaux radiciels dans les anneaux de polynômes et les variétés algébriques.
- la décomposition en idéaux premiers de ces mêmes idéaux radiciels dans les anneaux de polynômes.

L'ensemble des solutions analytiques d'un système différentiel algébrique, ordiaire ou aux dérivées partielles, est constitué d'un nombre fini de types de solution, chacun défini par un idéal différentiel premier.

Que l'aspect algorithmique de la théorie soit présenté en second n'est pas commun car ce sont les principes algorithmiques qui sont au coeur de nombreuses démonstrations. Mais nous avons préféré séparer ces deux aspects pour mieux montrer comment faire glisser l'algorithme théorique de décomposition de Ritt vers un algorithme effectif.

Les algorithmes de décomposition prennent en entrée un système différentiel et calculent des idéaux différentiels qui décrivent les différents types de solutions du système. Chacun de ces idéaux différentiels est donné par un ensemble caractéristique.

En termes plus précis, un algorithme de décomposition prend en entrée un ensemble fini Σ de polynômes différentiels et ressort un nombre fini d'ensembles auto-reduits cohérents A_i, $i = 1 \ldots r$ tels que

$$\{\Sigma\} \;=\; \bigcap_{i=1}^{r} [A_i] : h_{A_i}^{\infty},$$

où h_{A_i} est le produit des initiaux et séparants de A_i, et les A_i sont des ensembles caractéristiques des idéaux $[A_i] : h_{A_i}^{\infty}$. Dans le cas de la décomposition de Ritt, ces idéaux différentiels sont premiers. F.Boulier a montré qu'on pouvait se contenter d'idéaux différentiels *réguliers*. Nous présentons un algorithme de décomposition en idéaux réguliers, qui est une version allégée de l'algorithme Rosenfeld-Gröbner de F.Boulier, et qui s'obtient facilement à partir de l'algorithme de Ritt.

Les décompositions obtenues ne sont pas *minimales*. Certains $[A_i] : h_{A_i}^{\infty}$ peuvent en contenir d'autres. En d'autres termes, cela signifie que l'ensemble des solutions

n'est pas décrit de façon minimale : certaines solutions présentes sont les solutions particulières d'autres.

C.3 Les décompositions minimales

Dans le cas où le système n'est constitué que d'une unique équation, on peut obtenir la décomposition minimale à partir d'une des décompositions susmentionnée. Au coeur de cette affirmation se tient le Théorème des Petites Puissances de Ritt.

Supposons que nous ayons obtenu une décomposition en idéaux différentiels premiers ou en idéaux différentiels réguliers. Ils sont décrits par des ensembles caractéristiques. Si un de ces ensembles caractéristiques contient plus d'un élément, nous savons que la solution singulière qu'il définit n'est pas essentielle.

Ce résultat appartient à Ritt dans le cas d'une décomposition en idéaux différentiels premiers. Dans le cas d'idéaux différentiels réguliers, un pas intermédiaire dans cette affirmation est le lemme de Lazard, qui implique que les idéaux réguliers sont l'intersection d'idéaux premiers dont les ensembles caractéristiques ont le même nombre d'éléments.

Après cette première élimination nous avons donc un ensemble fini de polynômes différentiels dont les solutions générales sont potentiellement des solutions singulières essentielles de notre polynôme différentiel de départ.

Si ces polynômes différentiels sont algébriquement irréductibles le Procédé de Préparation et le Théorème des Petites Puissances déterminent si la solution singulière définie est essentielle. Dans le cas de la décomposition de Ritt, les polynômes différentiels obtenus sont irréductibles.

Mais dans la pratique, nous obtenons des polynômes différentiels réguliers. Pour se ramener au cas précédent, il *suffit* de factoriser chaque polynôme différentiel obtenu. C'est cette manière directe que nous exposerons en premier, pour sa simplicité.

Selon le corps dans lequel est effectué la factorisation, nous obtiendrons plus ou moins de facteurs. Aussi il n'y a pas d'intérêt à casser la structure régulière de la décomposition. Nous proposerons donc un algorithme du type Duval pour éliminer dans les polynômes différentiels réguliers les facteurs ne donnant pas de solution essentielle. La présentation de cet algorithme nous donnera une occasion naturelle de nous pencher sur la preuve de la condition de suffisance du Théorème des Petites Puissances.

C.4 Le calcul de bases différentielles

Les ensembles caractéristiques décrivent d'une certaine manière les idéaux différentiels premiers ou réguliers. Ce ne sont néanmoins pas des bases. Une solution des éléments d'un ensemble caractéristique n'est pas forcement une solution de l'idéal qu'il représente.

Une base de la solution générale d'une équation différentielle contient des équations différentielles qui se sont affranchies de solutions singulières. Elles peuvent donc être plus faciles à intégrer, sous forme close ou numériquement.

Si l'on détient une telle base on peut déterminer si une solution singulière qui n'est pas essentielle est une solution particulière de la solution générale. C'est le problème de Ritt.

La méthode employée pour calculer une base différentielle consiste à ramener le problème à de l'algèbre polynômiale. Il suffit pour cela de considérer le polynôme différentiel et un nombre suffisant de ses dérivées. Le point difficile est de déterminer le nombre de dérivations à effectuer.

La clé de ce problème devait se trouver dans les démonstrations du Théorème des Petites Puissances. Et en effet en étudiant la preuve de la condition de nécessité du Théorème des petites puissance, c'est à dire le lemme de Levi, on peut déterminer une borne. Cette borne correspond en fait au nombre de dérivations à effectuer pour s'affranchir des solutions singulières essentielles. Reste à s'affranchir des solutions singulières qui ne sont pas essentielles. Nous sommes en fait bloqués par ce même problème de Ritt.

Il existe néanmoins quelques critères pour résoudre ce problème. C'est que nous évoquerons dans le dernier chapitre de ce mémoire. Si ce problème d'inclusion est le plus souvent posé sous sa forme algébrique, il serait regrettable d'en négliger son interprétation sur les propriétés analytiques des solutions. C'est ce point que nous avons voulu rappeler, aux algébristes et aux algorithmiciens, dans le chapitre suivant.

C.5 Équations différentielles du premier ordre

Le cas des équations différentielles algébriques du premier ordre est relativement simple. Une solution singulière qui n'est pas essentielle est une solution particulière de la solution générale. C'est la raison pour laquelle nous pouvons calculer une base différentielle de la solution générale. Cette base différentielle permet de réduire l'ensemble des point singuliers de l'équation différentielle.

Aussi avons-nous voulu dans cette denière partie présenter les différentes approches déjà existantes pour l'étude des points singuliers des équations différen-

tielles algébriques. Ce sont les points où le théorème d'existence et d'unicité d'une solution ne peut être appliqué.

Les premières études sur ce thème furent analytiques. On détermine les séries solutions de l'équation différentielle à un point donné. Une approche géométrique permet de mieux comprendre et de visualiser les différents types de points singuliers exhibés.

L'approche géométrique des équations différentielles n'est pas présentée dans son intégralité, et ce pour deux raisons. L'étude des points singuliers que nous présentons dans le Chapitre L n'est pas, à ma connaissance, généralisée aux équations d'ordre supérieur. D'autre part, cette approche repose sur la supposition que l'équation différentielle n'a pas de singularités purement algébriques. Elle s'avère donc insuffisante pour l'étude globale des solutions et donc pour étudier les équations admettant une solution singulière.

Les solutions singulières sont des solutions qui vivent dans le lieu singulier de l'équation différentielle considérée. Leur graphe est en fait constitué de points singuliers de contact. A ces points, il n'existe pas de méthode complète pour déterminer les propriétés analytiques des solutions non singulières.

Mais ce lieu est factorisable - du moins lorsque la solution singulière est essentielle - dans l'équation différentielle. C'est ce que nous faisons en calculant une base différentielle de la solution générale. Aussi, après avoir *nettoyé* l'équation de la solution singulière, il apparait que l'on peut trouver un ensemble plus grand de points où il existe une série entière convergente solution.

Cette analyse s'étend sans difficulté à toute équation ordinaire d'ordre supérieur dont on peut calculer une base de la solution générale.

D Les problèmes ouverts

D.1 Propriétés enveloppantes des solutions singulières

Si l'on considère une équation différentielle d'ordre n qui admet une solution singulière essentielle définie par une équation différentielle d'ordre $n-1$, alors cette solution singulière fournit des enveloppes de la solution générale. Ceci est un résultat de Hamburger [Ham93].

Plus récemment, le Théorème des Petites Puissances a montré le chemin pour déterminer les propriétés enveloppantes des solutions singulières des équations aux dérivées partielles du premier ordre [Rit45a].

Étudions quelques exemples pour voir quelle diversité de comportements peut être rencontrée lorsqu'une équation différentielle du second ordre admet une solution singulière algébrique, c'est à dire d'ordre zéro.

Exemple: Soit l'équation différentielle

$$(E_2) \quad y''^3 - 18\, y''\, y' + 108\, y = 0$$

En éliminant y'' de cette équation et de sa dérivée partielle par rapport à y'', on obtient l'équation différentielle du premier ordre

$$(E_1) \quad 2\, y'^3 - 27\, y^2 = 0.$$

Cette équation admet une solution singulière $y = 0$. Celle-ci est également solution de l'équation (E_1). Dans les deux cas c'est une solution singulière essentielle.

Par conséquent, $y = 0$ est une enveloppe des solutions non singulières de (E_1). Le contact est au moins du premier ordre.

Grâce au *procédé de préparation*, que nous ne détaillons pas ici, on peut affirmer que la solution générale de (E_1) est une solution singulière essentielle de (E_2).

Par conséquent, la solution générale de (E_1) fournit une famille d'enveloppes aux solutions non singulières de (E_2). Le contact est au moins du second ordre.

Il suit que $y = 0$ est une enveloppe de solutions non singulières de (E_2).

Ceci peut être vérifié en intégrant les diverses équations différentielles en présence. La solution générale de (E_1) est donnée par

$$\tilde{y}_1(x) \;=\; \frac{1}{2}\,(x+c)^3.$$

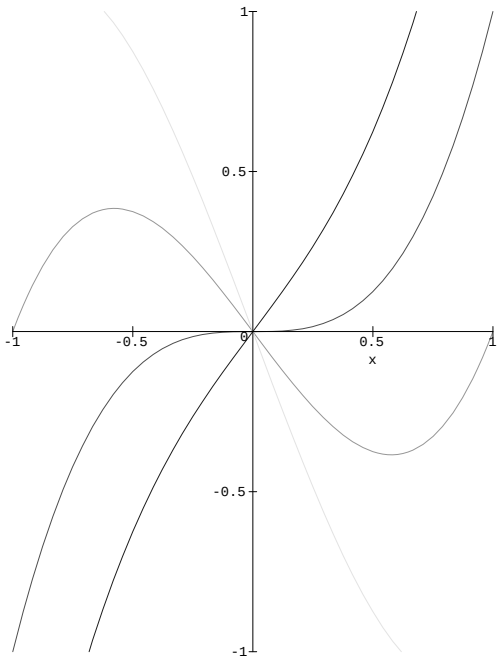
Par conséquent le contact avec $y = 0$ est du second ordre.

La solution générale de (E_2) peut être donnée par

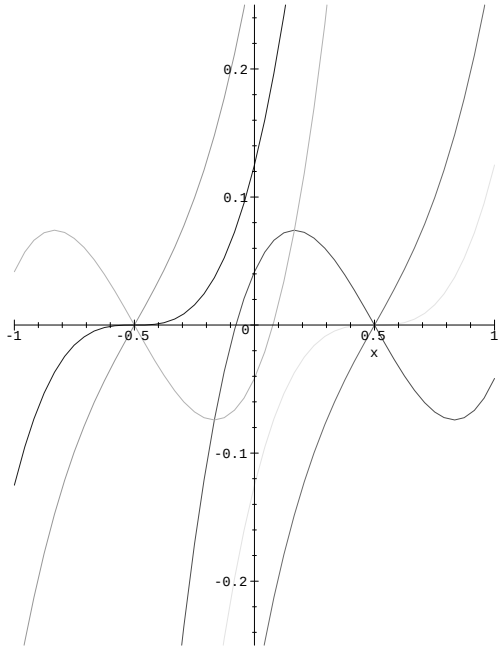
$$\tilde{y}_2(x) \;=\; (x+a)^3 + b\,(x+a)$$

L'ensemble de ces courbes intégrales qui sont tangentes à $y = 0$ sont celles qui correspondent à $b = 0$. Le contact est du second ordre comme on pouvait s'y attendre après la remarque précédente.

Si on trace des courbes de la solution générale de (E_2), on peut voir le contact avec $y = 0$.

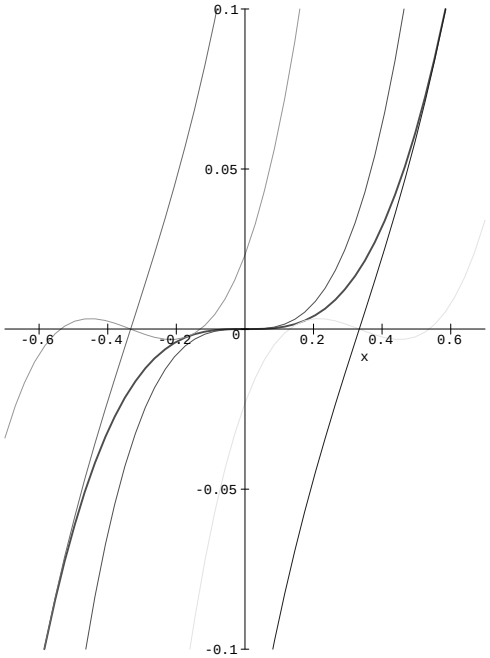


$\tilde{y}_2(x)$
pour $a = 0$ et $b = -2, -1, 0, 1$



$\tilde{y}_2(x)$
pour $a = -\frac{1}{2}, \frac{1}{2}$ et $b = -\frac{1}{3}, 0, \frac{1}{3}$

Nous voyons dans le dessin suivant, la solution $y(x) = \frac{1}{2}x^3$ de (E_1) comme enveloppe de solutions non singulières de (E_2).



$\tilde{y}_1(x)$ et $\tilde{y}_2(x)$,
pour $c = 0$ et $(a, b) = (0, 0), (\pm\frac{1}{3}, \frac{1}{3}), (\pm\frac{1}{3}, -\frac{1}{24})$

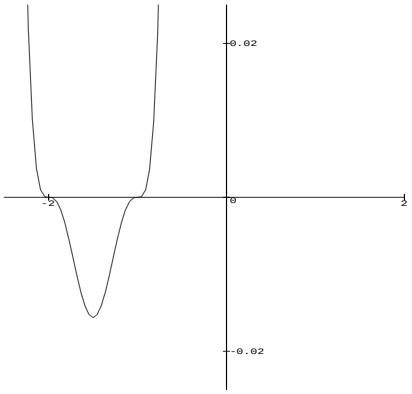
Exemple : Soit l'équation différentielle

$$(6\,y\,y'' - 5\,y'^2)^3 + 729\,y^4 \;=\; 0.$$

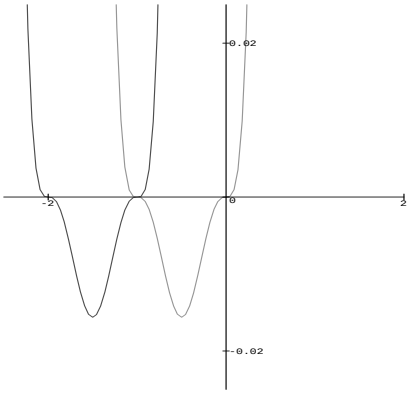
dont l'unique solution singulière est $y_0(x) = 0$. La solution générale peut être donnée par

$$y_2(x) = \Big((x-a) + b\,(x-a)^2\Big)^3$$

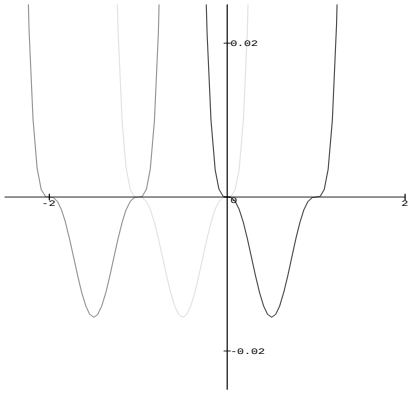
où a et b sont les constantes arbitraires. $y_0(x) = 0$ est donc une enveloppe des courbes de la solution générale et le contact est d'ordre 3. Nous représentons quelques unes de ces solutions.



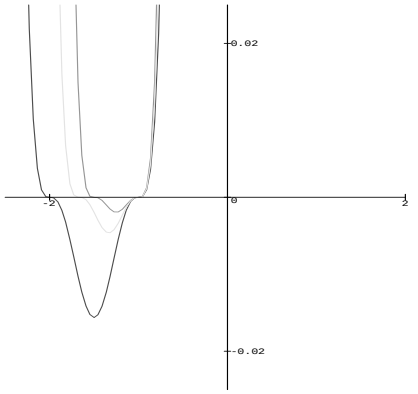
$a = -1,\ b = 1$



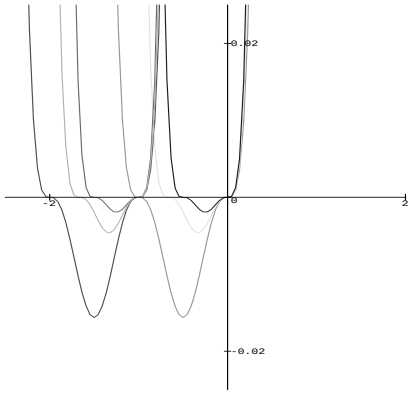
$a = -1, 0,\ b = 1$



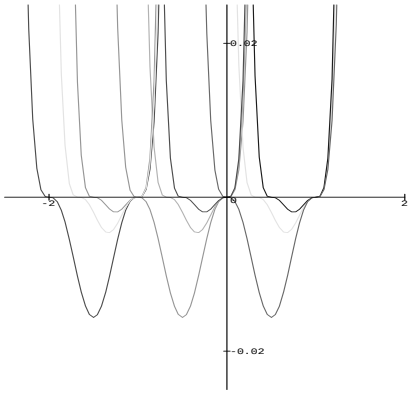
$a = -1, 0, 1,\ b = 1$



$a = -1,\ b = 1, \frac{3}{2}, 2$



$a = -1, 0,\ b = 1, \frac{3}{2}, 2$



$a = -1, 0, 1,\ b = 1, \frac{3}{2}, 2$

EXEMPLE : Soit

$$y''^3 - 216\, y \;=\; 0$$

L'unique solution singulière est $y = 0$, qui s'avère être une solution singulière essentielle. Par les règles usuelles de l'intégration nous pouvons trouver une intégrale première

$$y'^2 - 9\, y^{\frac{4}{3}} \;=\; c$$

où c est une constante arbitraire. Les solutions qui sont tangentes à la droite $y = 0$ correspondent à $c = 0$. Ce sont les courbes algébriques

$$y^2 \;=\; (x + a)^6.$$

Par conséquent $y = 0$ n'est enveloppe que de cette sous famille de courbes de la solution générale.

EXEMPLE : Cet exemple est très similaire au précédent, à une distinction près. Soit l'équation différentielle

$$y'^2\, y'' - 8\, y = 0$$

L'unique solution singulière est $y = 0$, qui s'avère être une solution singulière essentielle. D'après les règles d'intégration, on peut trouver une intégrale première à cette équation sous la forme

$$y'^4 - 16\, y^2 = c$$

où c est une constante. Les solutions qui sont tangentes à la droite $y = 0$ correspondent à $c = 0$. Ce sont les courbes algébriques

$$y^2 \;=\; (x + a)^4.$$

Dans le cas présent, le contact entre cette sous-famille de courbes de la solution générale et la solution singulière est du premier ordre seulement. Il était du second ordre dans l'exemple précédent.

D.2 Solutions particulières

Au premier ordre, qu'une solution singulière ne soit pas essentielle revient à dire qu'elle appartient à la solution générale. Et pour cette raison nous l'appelons particulière. Aux ordres supérieurs, la situation se corse. Une solution singulière qui n'est pas essentielle peut effectivement appartenir à la solution générale. Dans ce cas elle peut être approchée à tout ordre par des solutions non singulières. Mais il se peut aussi qu'elle appartienne à une autre solution singulière, essentielle celle-ci.

Pour illustration, considérons les deux équations différentielles très proches.

EXEMPLE : Soit

$$y''^2 - y'\, y = 0.$$

Les solutions singulières sont données par $y = 0$ et $y' = 0$. La première est triviallement incluse dans la seconde. De sorte que $y' = 0$ définit en fait l'unique solution singulière essentielle.

Une intégrale première de cette équation peut être donnée sous la forme

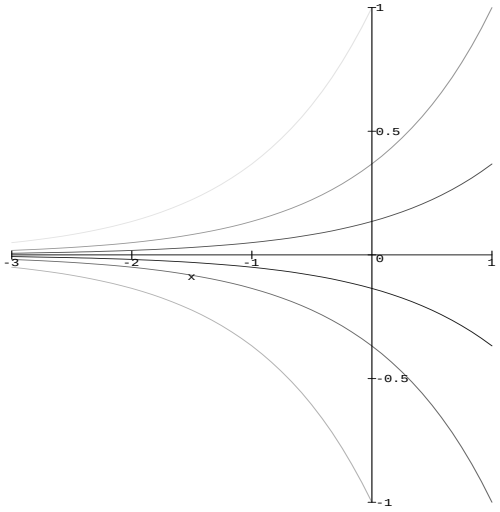
$$y'^{\frac{3}{2}} \pm y^{\frac{3}{2}} = c$$

où c est une constante. De sorte que les solutions qui sont tangentes à $y = 0$ sont les solutions correspondant à $c = 0$. Ce sont les fonctions

$$\tilde{y}_a(x) = e^{x+a} \quad \text{et} \quad \bar{y}_a(x) = -e^{x+a}$$

qui ne touchent $y = 0$ qu'à l'infini. Cependant, on peut approcher $y = 0$ en tous ses points par une de ces exponentielles. Ainsi $y = 0$ est dans la solution générale.

Une autre manière de le voir et de considérer une solution non singulière ϕ de $y''^2 - y' y = 0$. Comme cette équation est homogène, $c\,\phi$ est également solution de l'équation, où c est une constante arbitraire. On peut donc glisser le long de la solution générale jusqu'à $y = 0$. A ce titre, $y = 0$ est une solution particulière.



$\tilde{y}_a(x) = e^{x+a}$ et $\bar{y}_a(x) = -e^{x+a}$,
solutions de $y''^2 - y' y = 0$

Exemple : Soit à présent l'équation différentielle où on a uniquement changé la puissance de y'',

$$y''^3 - y' y = 0.$$

A nouveau les solutions singulières sont données par $y = 0$ et $y' = 0$. La première est triviallement incluse dans la seconde. De sorte que $y' = 0$ définit l'unique solution singulière essentielle.

Une intégrale première de cette équation peut être donnée sous la forme

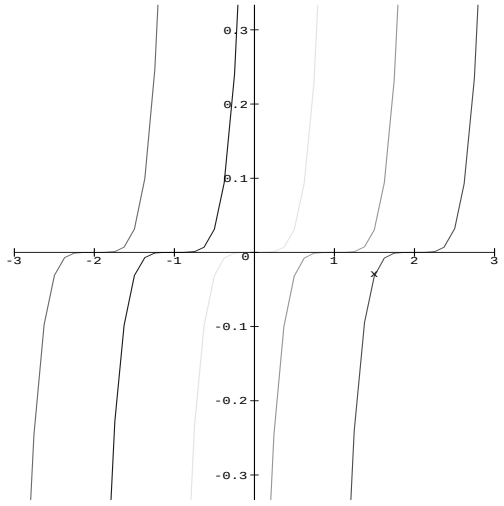
$$y'^{\frac{5}{3}} - \frac{5}{4} y = c$$

où c est une constante. De sorte que les solutions qui sont tangentes à $y = 0$ sont les solutions correspondant à $c = 0$. Ce sont les fonctions

$$\tilde{y}_b(x) = \frac{125}{4}\,(x+b)^5.$$

A présent, $y = 0$ est donc une enveloppe de solutions non singulières. Elle n'est pas incluse dans la solution générale.

Dans les deux cas présentés, $y = 0$ est une solution singulière qui n'est pas essentielle. Cependant, dans le second cas elle n'appartient qu'à la solution singulière essentielle alors que dans le premier cas elle est dans l'intersection de la solution générale et de la solution singulière. Ceci se ressent dans le comportement des solutions non singulières dans son voisinage.



$\tilde{y}_b(x) = \frac{125}{64}\,(x+b)^5$
solutions de $y''^3 - y'\,y = 0$

Déterminer si une solution est dans la solution générale a été nommé *le problème de Ritt*. Joseph Fels Ritt a lui-même apporté une réponse longue et difficile pour les équations du second ordre dans la deuxième partie de l'article où était présenté pour la première fois le Théorème des Petites Puissances [Rit36]. Comme le notait R.Cohn, ce résultat très spécifique et terriblement ardu n'a pas encore suscité beaucoup d'enthousiasme ni de valeureux successeurs.

Part II

Algebra and algorithms for differential systems

E Differential algebra

In this section, we give a cursory presentation of some features of differential algebra. The scattered proofs of the stated properties are not given in a concern of completeness but rather to get the casual reader familiar with the differential algebra objects.

E.1 Differential Rings

Derivation

Let $(\mathcal{R}, +, \cdot)$ be a commutative ring. A derivation δ on $\mathcal{R}$ is an additive morphism that satisfies Leibniz rule

$$\delta(a \cdot b) = \delta a \cdot b + a \cdot \delta b \ \ \forall a, b \in \mathcal{R}$$

We consider $\Delta = \{\delta_1, \ldots, \delta_\mu\}$ a finite set of derivations acting on $\mathcal{R}$ and Θ the commutative free monoid of the derivation operators generated by Δ. Any derivation operator $\theta \in \Theta$ can be written $\theta = \delta_1^{\alpha_1}\delta_2^{\alpha_2}\ldots\delta_\mu^{\alpha_\mu}$, where the α_i are natural integers. The *order* of θ is then ord $\theta = \sum_{i=1}^{\mu} \alpha_i$.

Endowed with the derivations set Δ, $(\mathcal{R}, +, \cdot, \Delta)$ is a differential ring. When Δ consists of a single derivation δ we shall speak of the ordinary differential ring $(\mathcal{R}, +, \cdot, \delta)$.

E.1.1 Example: The set of functions analytic in a region of $\mathbb{C}$ together with the usual derivation is an ordinary differential ring.

If $\mathcal{R}$ is an integral domain, the derivations on $\mathcal{R}$ can be extended to the field of quotients $K = (\mathcal{R}^*)^{-1}\mathcal{R}$ of $\mathcal{R}$ in a unique way. Indeed:

$$\delta(a) = \delta(\frac{a}{b}b) = \delta(\frac{a}{b})b + \frac{a}{b}\delta(b) \ \Rightarrow \ \delta(\frac{a}{b}) = \frac{\delta(a)b - a\delta(b)}{b^2} \ \ \forall a, b \in \mathcal{R}, \ \forall \delta \in \Delta$$

As for a commutative $\mathcal{R}$-algebra E, a derivation $\tilde{\delta}$ on E which *extends* the derivation δ on $\mathcal{R}$ satisfies

$$\tilde{\delta}(a \cdot e) = \delta(a) \cdot e + a \cdot \tilde{\delta}(e) \quad \forall a \in A,\ e \in E.$$

There will be no harm to identify the derivations on E with the derivations on $\mathcal{R}$.

E.1.2 EXAMPLE: Any commutative ring $\mathcal{R}$ can be considered as a differential ring, if endowed with the trivial derivation that maps any element of $\mathcal{R}$ to zero. On $\mathcal{R}[x]$, the ring of polynomials with coefficients in $\mathcal{R}$, we can define a derivation δ that extends the derivation on $\mathcal{R}$ and satisfies $\delta x = 1$. Then

$$\delta(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a.$$

E.1.3 DEFINITION: Let $(\mathcal{R}, \Delta)$ to $(\mathcal{R}', \Delta)$ be two differential rings. A differential morphism ψ from $(\mathcal{R}, \Delta)$ to $(\mathcal{R}', \Delta)$, is a ring morphism from $\mathcal{R}$ to $\mathcal{R}'$ that commutes with the derivations:

$$\forall a \in \mathcal{R},\ \forall \delta \in \Delta,\ \ \psi(\delta a) = \delta(\psi(a))$$

Differential ideals

E.1.4 DEFINITION: An non-empty subset I of a differential ring $(\mathcal{R}, \Delta)$ is a *differential ideal* if

- I is an ideal of $\mathcal{R}$: $a, b \in I,\ \ c \in A \quad \Rightarrow \quad a + b \in I,\ \ c \cdot a \in I$
- I is stable under derivation: $a \in I \ \Rightarrow\ \forall \delta \in \Delta,\ \delta a \in I$

The intersection of differential ideals is a differential ideal. We can therefore define the differential ideal $[\Sigma]$ generated by a non-empty subset Σ of $\mathcal{R}$: it is the intersection of all differential ideals containing Σ, or, equivalently, the smallest differential ideal containing Σ. $[\Sigma]$ can also be seen as the ideal generated by Σ together with all the derivatives of any order of the elements of Σ. Consequently, an element of $\mathcal{R}$ is in $[\Sigma]$ on condition it can be written as a linear combinations of derivatives of the elements of Σ.

We introduce next the radical differential ideals. They will be seen to have an even more prominent role in differential algebra than in polynomial algebra.[1]

E.1.5 DEFINITION: A differential ideal R of a differential ring $(\mathcal{R}, \Delta)$ is radical if it contains an element $a \in \mathcal{R}$ whenever it contains a positive power of a.

$$a^\alpha \in R,\ \alpha \in \mathbb{N}^* \ \Rightarrow\ a \in R$$

[1] Indeed, we can not expect all the differential ideals in a differential polynomial ring to be finitely generated. Only radical differential ideals will have this property.

Again the intersection of radical differential ideals is a radical differential ideal. $\{\Sigma\}$ shall be the radical differential ideal generated by an non-empty subset Σ of $\mathcal{R}$.

Beside, we define the radical of a subset Σ of $\mathcal{R}$ as

$$\sqrt{\Sigma} = \{p \in \mathcal{R} \mid \exists \alpha \in \mathbb{N}^* \text{ tq } p^\alpha \in \Sigma\}.$$

It is quite immediate to see that if I is an ideal, $\sqrt{I}$ is also an ideal. But can we insert the adjective *differential* in both part of the sentence? To answer this question, we need to check if the radical of a differential ideal is stable under derivation.

E.1.6 Example: Consider the differential ring $\mathbb{Z}[x]$ endowed with the traditional derivation. Let I be the ideal generated by $3x^2$: $I = [3x^2]$. Thus I is the ideal generated by $3x^2$, $6x$ and 6 in $\mathbb{Z}[x]$.

$3x$ belongs to the radical of I since $(3x)^2 = 3 \cdot 3x^2$. Nonetheless its derivative, 3, does not belong to this radical.

E.1.7 Proposition: Let $\mathcal{R}$ be a differential ring. Whenever $\mathcal{R}$ contains a field isomorphic to $\mathbb{Q}$, the radical of a differential ideal of $\mathcal{R}$ is a differential ideal, and thus a radical differential ideal.

Proof: Consider any derivation $\delta \in \Delta$. For an element a of $\mathcal{R}$ and an integer $\alpha \in \mathbb{N}^*$ we show by induction that for any r, $0 \leq r \leq \alpha - 1$,

$$q_r = \alpha(\alpha-1)\dots(\alpha-r)p^{\alpha-r-1}(\delta p)^{2r+1} \in [p^\alpha]$$

This is true for $r = 0$ since $q_0 = \alpha\, p^{\alpha-1}\delta p = \delta p^\alpha \quad \in [p^\alpha]$.

Assume $q_r \in [p^\alpha]$ for $0 \leq r < \alpha - 1$. Then

$$\begin{aligned}\delta q_r = \quad & \alpha(\alpha-1)\dots(\alpha-r-1)p^{\alpha-r-2}(\delta p)^{2r+1} \\ & +(2r+1)\alpha(\alpha-1)\dots(\alpha-r)p^{\alpha-r-1}(\delta p)^{2r}\,\delta^2 p \quad \in [p^\alpha]\end{aligned}$$

and therefore $\delta q\,\delta q_r = q_{r+1} + (2r+1)q_r\,\delta^2 p \quad \in [p^\alpha]$, which drives us to the desired conclusion.

We thus have $\alpha!(\delta p)^{2\alpha-1} \in [p^\alpha]$. As $\mathcal{R}$ contains a field isomorphic to $\mathbb{Q}$, $\alpha! \cdot \mathbf{1}$ is invertible in $\mathcal{R}$, we conclude that $(\delta p)^{2\alpha-1} \in [p^\alpha]$.

Now, let I be a differential ideal of $\mathcal{R}$. If p is an element in the radical of I, then a power of p is in I: $\exists \alpha \in \mathbb{N}^*$, $[p^\alpha] \subset I$. As a consequence $(\delta p)^{2\alpha-1} \in I$ and therefore $\delta p \in \sqrt{I}$. Thus $\sqrt{I}$ is stable under derivation and is therefore a differential ideal. □

The differential rings we will consider from now on will have this property. We could consider them as algebras over $\mathbb{Q}$ and they are sometimes called *Ritt algebras*. But most of the time, it is simply said that **we work in characteristic zero**.

Thus, for any non-empty subset Σ of $\mathcal{R}$,

$$\sqrt{[\Sigma]} = \{\Sigma\} = \{p \in A \mid \exists \alpha \in \mathbb{N}^* \ p^\alpha \in [\Sigma]\},$$

and an element a of $\mathcal{R}$ belongs to $\{\Sigma\}$ on condition that a power of a can be written as a linear combination of derivatives of elements of Σ.

E.1.8 PROPOSITION: Let p and q be elements of a differential ring $\mathcal{R}$ and let Σ be a subset of $\mathcal{R}$. Then

$$\theta q \, \theta' p \in \{p\, q\}, \ \forall \theta, \theta' \in \Theta$$

and

$$\{\Sigma, p\, q\} = \{\Sigma, p\} \cap \{\Sigma, q\}$$

PROOF: We show the first property by induction on $n_{\theta\theta'} = \text{ord}\ \theta + \text{ord}\ \theta'$. The property is trivial when $n_{\theta\theta'} = 0$. Let us assume this is true for all pair θ, θ' the sum of the order is equal to some $n \geq 0$

$$\theta q \, \theta' p \in \{p\, q\}, \ \forall \theta, \theta' \in \Theta \text{ such that } n_{\theta\theta'} = n$$

Consider a pair θ, θ' such that the sum of their orders is $n_{\theta\theta'} = n+1$. It is no loss of generality to assume that $\theta = \delta\theta_1$ where $\delta \in \Delta$ and $\text{ord}\ \theta_1 + \text{ord}\ \theta' = n$. That $\theta_1 p \, \theta' q$ belongs to $\{p\, q\}$ obviously induces that $\delta(\theta_1 p \, \theta' q)$ and $\theta' q$ $(\delta(\theta_1 p \, \theta' q))$ are elements of $\{p\, q\}$. As

$$\delta\ (\theta_1 p \, \theta' q) = \theta p \, \theta' q \ + \ \theta_1 p \ \delta\theta' q$$

and

$$\theta' q \ (\delta\ (\theta_1 p \, \theta' q)) = \theta p \ (\theta' q)^2 \ + \ \underbrace{\theta_1 p \, \theta' q}_{\in \{p\, q\}} \ \delta\theta' q.$$

$\theta p \ (\theta' q)^2$ and therefore $\theta p \, \theta' q \in \{p\, q\}$.

As for the second property, the inclusion $\{\Sigma, p\, q\} \subset \{\Sigma, p\} \cap \{\Sigma, q\}$ is trivial.

Assume that an element r of $\mathcal{R}$ belongs to $\{\Sigma, p\} \cap \{\Sigma, q\}$. Then there exist two integers α and β, two finite sets of elements of $\mathcal{R}$, say $(a_i)_{i\in I}$ and $(b_j)_{j\in J}$, and two elements ξ and ϵ of $\{\Sigma\}$ such that

$$r^\alpha = \epsilon + \sum_{i\in I} a_i \theta_i p \quad \text{ and } \quad r^\beta = \xi + \sum_{j\in J} b_j \theta_j p \text{ where } \theta_i,\, \theta_j \in \Theta.$$

We have $r^{\alpha+\beta} = \sum_{i\in I,\, j\in J} a_i\, b_j\, \theta_i p\ \theta_j q + \underbrace{\epsilon \left(\sum_{j\in J} b_j \theta_j q\right) + \xi \left(\sum_{i\in I} a_i \theta_i p\right) + \epsilon\,\xi}_{\in\{\Sigma\}}$.

According to the previous property, $\theta_i p\, \theta_j q \in \{p\, q\}$. Hence $r \in \{\Sigma, p\, q\}$. □

E.1.9 COROLLARY: Let Σ be a subset of the differential ring $\mathcal{R}$. Let a_i, $1 \leq i \leq r$, be elements of $\mathcal{R}$. Then

$$\{\Sigma, \prod_{i=1}^{r} a_i\} \ = \ \bigcap_{i=1}^{r} \{\Sigma, a_i\}$$

This property suggests that we can decompose a radical ideal as long as it contains some reducible elements. Actually any radical differential ideal is the intersection of *prime differential ideals*, and we shall see in next section under which condition this intersection is finite.

E.1.10 DEFINITION: A differential ideal P of $\mathcal{R}$ is prime if $P \neq \mathcal{R}$ and P contains a or b, elements of $\mathcal{R}$, whenever their product $a\,b$ belongs to P.

$$\forall a, b \in \mathcal{R}, a \cdot b \in P \ \Rightarrow\ a \in P \text{ ou } b \in P$$

E.2 Differential polynomial ring

Consider a differential ring $(\mathcal{R}, \Delta)$. The ring of differential polynomials in the differential indeterminates $y_1, \ldots, y_n$ with coefficients in $\mathcal{R}$ is the associative and commutative free $\mathcal{R}$-algebra of the set $\Theta \times Y$, where $Y = \{y_1, \ldots, y_n\}$. In other words, it is the polynomial algebra in infinitely many indeterminates

$$\mathcal{R}\{y_1, \ldots, y_n\} = \mathcal{R}\{Y\} = \mathcal{R}[\Theta Y] = \mathcal{R}[\{\theta y_i,\ y_i \in Y,\ \theta \in \Theta\}].$$

It is naturally endowed with derivations that extend the derivations of Δ acting on $\mathcal{R}$.

When considering an ordinary differential polynomial ring $(\mathcal{R}\{y_1, \ldots, y_n\}, \delta)$ we shall often use the notation y_{ij} for $\delta^j y_i$, where $1 \leq i \leq n$ and $j \in \mathbb{N}$. Most of the time we will give examples in the ordinary differential polynomial ring with one indeterminate $(\mathcal{R}\{y\}, \delta)$ and thus $\delta^j y$ will be simply shorten in y_j.

E.2.1 EXAMPLE: We can associate to the ordinary differential equation

$$\frac{\mathrm{d}^2 y}{\mathrm{d}x^2} + xy\frac{\mathrm{d}y}{\mathrm{d}x} + x^2 = 0$$

the differential polynomial, with coefficients in $(\mathbb{Q}[x], \delta)$,

$$p = \delta^2 y + xy\,\delta y + x^2 \qquad \text{or} \qquad p = y_2 + xy_0\, y_1 + x^2$$

Differential monomials

Quite naturally a differential monomial of $\mathcal{R}\{Y\}$ is a monomial of $\mathcal{R}[\Theta Y]$. The degree of a monomial of $\mathcal{R}\{Y\}$ is its degree in $\mathcal{R}[\Theta Y]$ and a polynomial is homegeneous if all its monomial have the same degree. Note that if p is such a homogeneous differential polynomial then any of its derivatives is a homogeneous differential polynomial of the same degree. Furthermore, $\mathcal{R}\{Y\}$ is a graded algebra according to the degree [Kol73, I.7]. If $\mathcal{D}_k$ is the set of homogeneous differential polynomials of degree k we have a direct sum decomposition

$$\mathcal{R}\{Y\} = \bigoplus_{k\in\mathbb{N}} \mathcal{D}_k.$$

It is possible to define a wider class of gradings of the ring $\mathcal{R}\{Y\}$ among which the weight. The weight of a derivative θy_i is simply the order of θ. The weight of the monomial is the sum of the weight of its factors. Hence

$$\text{wt}\ \left(\prod_{k=1}^{r}\ \theta_k y_{l_k}\right) = \sum_{k=1}^{r} \text{ord}\ \theta_k \quad \text{where } \theta_k \in \Theta \ \text{ and } \ 1 \leq l_k \leq n.$$

A differential polynomial is said to be isobaric if all of its monomials have the same weight. If p is an isobaric differential polynomial of weight k then $\theta\, p$ is an isobaric differential polynomial of weight $k + \text{ord}\ \theta$, for any derivation operator $\theta \in \Theta$. If $\mathcal{W}_k$ is the set of isobaric differential polynomials of weight k, we have a direct sum decomposition [Kol73, I.7]

$$\mathcal{R}\{Y\} = \bigoplus_{k\in\mathbb{N}} \mathcal{W}_k.$$

We shall also speak of differential monomials in a single differential indeterminate, say y_n. It shall be considered as monomials in

$$(\mathcal{R}\{y_1, \ldots, y_{n-1}\})\{y_n\}.$$

It is therefore possible to define the degree and weight in the differential indeterminate y_n.

The basis theorem

A commutative ring is said to be Nœtherian, with respect to its ideals, if one of the equivalent properties is satisfied

- all the ideals are of finite type.
- any strictly increasing sequence of ideals is finite

- every non-empty set of ideals has a maximal element.

Then the Hilbert basis theorem states that if a ring is Nœtherian, with respect to its ideals, then any ring of polynomials in a finite set of indeterminates with coefficient in that ring is also Nœtherian, with respect to its ideals.

To be in a position to handle differential polynomial ideals we would like to have a similar property on differential polynomial rings. Unfortunately, we can only expect the radical differential ideals to be finitely generated.

E.2.2 Example: $\mathbb{Q}$ is a field and is thus Nœtherian, with respect to its ideals. Endowed with the trivial derivation, $\mathbb{Q}$ can be considered as a differential field. Its differential ideals correspond exactly to its ideals and are thus all finitely generated. Nonetheless the differential ideal $[y_0^2, (y_1)^2, (y_2)^2, \cdots]$ in the ordinary differential polynomial ring $(\mathbb{Q}\{y\}, \delta)$ is not finitely generated. Note that conversely, $\{y_0^2, (y_1)^2, (y_2)^2, \cdots\} = \{y_0^2\} = \{y_0\}$.

E.2.3 Definition: A differential ring $(\mathcal{R}, \Delta)$ is said to be Nœtherian with respect to its radical differential ideals if it satisfies one of the equivalent properties [Kol73, 0.9]

- any radical differential ideal R of $\mathcal{R}$ is finitely generated: there exists a finite set Σ of elements of $\mathcal{R}$ such that $R = \{\Sigma\}$.
- every strictly increasing sequence of radical differential ideals, according to the inclusion, is finite.
- every non-empty set of radical differential ideals has a maximal element according to the inclusion

Trivially any differential field satisfy this property as well as any ring which is Nœtherian with respect to its ideals, as for instance $\mathbb{Q}[x]$.

The differential counter-part of the Hilbert basis theorem is the Ritt-Raudenbush Basis Theorem which follows.

E.2.4 Theorem: A necessary and sufficient condition for $(\mathcal{R}\{Y\}, \Delta)$ to be Nœtherian with respect to its radical differential ideals is that $(\mathcal{R}, \Delta)$ is itself Nœtherian with respect to its radical differential ideals.

The proof can be found in[Rit66, I.12], [Kol73, III.4].

We assume from now on and for the whole of this memoir that we have chosen a ground ring $\mathcal{R}$ which is Nœtherian with respect to its radical differential ideals . For computational purposes we will typically choose $A = \mathcal{K}[x]$ or $\mathcal{K}(x)$ where $\mathcal{K}$ is an algebraic extension of $\mathbb{Q}$.

E.2.5 Definition: For a radical differential ideal R, a finite set Σ such that

$$R = \{\Sigma\}$$

is called a *differential basis* of R.

Such a basis will always exists in the hypothesis we have just done.

This restriction of Nœtherianity to radical differential ideals induces cunning difficulties when trying to generalize proofs or algorithms of polynomial algebra. For illustration, consider the Hilbert Nullstellensatz: the algebraic variety of a set Σ of polynomials is not empty on condition that the ideal generated by Σ does not contain the unit element. This can be proved directly ([CLD92], for instance) while a differential version of this theorem is achieved through the property below. This indirect proof discloses the prominent role of prime differential ideals in the development of the theory.

E.2.6 Proposition: In a differential ring that is Nœtherian wr.t. its radical differential ideals, any radical differential ideal R is a finite intersection of prime differential ideals.

Furthermore, when we get rid of the prime ideals containing other ones, we get a minimal decomposition that is unique.

E.2.7 Definition: Assume the minimal decomposition into prime differential ideals of a radical differential ideal R is

$$R = \bigcap_{k=1}^{r} P_k.$$

Then the prime differential ideals P_k are called the *essential components* of R.

E.3 Components of an algebraic differential system

The aim of this section is to give an algebraic sense to the informal notion of *types of solution* and to make the first connections with the actual solution of a system of differential equations.

We shall stress that we have made the assumptions that the ground ring $\mathcal{R}$ contained a field isomorphic to $\mathbb{Q}$ and was furthermore Nœtherian w.r.t. its radical differential ideals.

Generic zero of a prime ideal

Let $(\mathcal{R}', \Delta)$ be a differential over-ring of $(\mathcal{R}, \Delta)$. Let $\nu = (\nu_1, \ldots, \nu_n)$ be an $n-$uplet of $\mathcal{R}'$. We define the Ψ_ν to be the differential $\mathcal{R}$-morphism from $\mathcal{R}\{y_1, \ldots, y_n\}$

to $\mathcal{R}'$ such that $\Psi_\nu(y_i) = \nu_i$, for any $1 \leq i \leq n$. For a differential polynomial $p \in \mathcal{R}\{Y\}$ we write $\psi_\nu(p) = p(\nu)$. If $p(\nu) = 0$, we say that p vanish on ν.

$$\begin{array}{rccl} \Psi_\nu : & \mathcal{R}\{Y\} & \longrightarrow & \mathcal{R}' \\ & a & \longmapsto & a, \quad \forall a \in \mathcal{R} \\ & y_i & \longmapsto & \nu_i \\ \\ & p & \longmapsto & p(\nu) \end{array}$$

If $\mathcal{R}'$ is an integral domain, the kernel of Ψ_ν, that is the set of differential polynomials of $(\mathcal{R}\{Y\}, \Delta)$ that vanish on ν, is a prime differential ideal, $\mathcal{P}(\nu)$.

Conversely, consider a prime differential ideal P in $(\mathcal{R}\{Y\}, \Delta)$. A generic zero of P is an element ν in an integral over-ring of $\mathcal{R}$ such that $\mathcal{P}(\nu) = P$. Assume P has no element in $\mathcal{R}$, 0 excepted. Then $\mathcal{R}\{Y\}/P$ is an integral differential over-ring of $\mathcal{R}$ and P is the kernel of the projection of $\mathcal{R}\{Y\}$ on $\mathcal{R}\{Y\}/P$. The class of $(y_1, \ldots, y_n)$ in $\mathcal{R}\{Y\}/P$ is a generic zero of P.

This proves that any prime differential ideal P with $P \cap \mathcal{R} = \{0\}$ has a generic zero.

The differential Nullstellensatz

E.3.1 Definition: Let Σ be any subset of $\mathcal{R}\{Y\}$. A zero of Σ is an $n-$uplet $\nu = (\nu_1, \ldots, \nu_n)$ in an integral over-ring $\mathcal{R}'$ of $\mathcal{R}$, such that $\Sigma \subset \mathcal{P}(\nu)$.

Thus if ν is a zero of a subset Σ of $\mathcal{R}\{Y\}$, $\{\Sigma\} \subset \mathcal{P}(\nu)$, and consequently, at least one of the essential component of $\{\Sigma\}$ is included in $\mathcal{P}(\nu)$. Therefore $\{\Sigma\}$ can not contain any element of $\mathcal{R}$ except 0.

Conversely, if $\{\Sigma\} \cap \mathcal{R} = \{0\}$, at least one of the essential component of $\{\Sigma\}$ has an intersection reduced to $\{0\}$ with $\mathcal{R}$. A generic zero of this essential component provides a zero of Σ.

We thus ensured a necessary and sufficient condition for Σ to admit a zero.

E.3.2 Theorem: Let $(\mathcal{R}, \Delta)$ be a differential ring. For a set Σ in $\mathcal{R}\{Y\}$ to admit a zero it is necessary and sufficient that $\{\Sigma\}$ does not contain any elements in $\mathcal{R}$, 0 excepted.

Assume further that no essential component of $\{\Sigma\}$ has an intersection with $\mathcal{R}$ bigger than $\{0\}$. Then each essential component of $\{\Sigma\}$ admits a generic zero, which is a zero of Σ. Now, let p be a differential polynomial of $\mathcal{R}\{Y\}$ which vanishes for any zero of Σ. It will vanish on the generic zeros of all essential components of $\{\Sigma\}$. Thus p is in the intersection of all the essential components of $\{\Sigma\}$, that is to say it is in $\{\Sigma\}$.

Note that if $\mathcal{R}$ is a field, no prime differential ideal of $\mathcal{R}\{Y\}$ has an intersection with $\mathcal{R}$ bigger than $\{0\}$.

E.3.3 THEOREM: Let $(\mathcal{F}, \Delta)$ be a differential field. If Σ is such that $1 \notin \{\Sigma\}$, then for any differential polynomial p in $\mathcal{F}\{Y\}$ which does not belong to $\{\Sigma\}$, there exists a zero of Σ which is not a zero of p.

This is the Theorem of zeros, a constructive proof of which can be found in [Coh41].

From now on we shall thus consider **differential polynomial rings with coefficients in a differential field $\mathcal{F}$ of characteristic zero.**

Algebraic differential systems

A system of differential algebraic equations $\mathcal{S}$ can be considered as a set Σ of differential polynomials in some $\mathcal{F}\{Y\}$. The minimal decomposition of $\{\Sigma\}$ gives a complete description of the zeros of Σ: to each prime component we can associate at least one (generic) zero and conversely a zero of Σ is a zero of at least one of the essential components. In an informal way we shall say that each essential component of Σ defines a *type* of solution of $\mathcal{S}$.

For the main point of the present work, we concentrate on differential systems consisting of a single equation: Σ consists of a single differential polynomial. In this case, one of the essential component can be defined as the *general component* (see Section G.1). This is the component that defines the so-called *general solution* of the differential equation under consideration.

E.3.4 EXAMPLE: Consider the differential polynomial $p = y_1^2 - 4y_0 \in \mathbb{Q}\{y\}$ associated to the differential equation $y'^2 - 4y = 0$.

Thanks to property E.1.9 we can write:

$$\begin{aligned} \{p\} &= \{p, \delta p\} = \{y_1^2 - 4y_0, 2y_1(y_2 - 2)\} \\ &= \{y_1^2 - 4y_0, y_1\} \cap \{y_1^2 - 4y_0, y_2 - 2\}. \end{aligned}$$

The decomposition in essential components of $\{p\}$ is actually $\{p\} = \{y_0\} \cap \{y_1^2 - 4y_0, y_2 - 2\}$. The differential equation has thus two types of solutions. The first is given by $\bar{y}(x) = 0$, the second is the solution of the system

$$\begin{cases} y'' - 2 = 0 \\ y'^2 - 4y = 0 \end{cases}$$

and thus can be given by $\tilde{y}(x) = (x + a)^2$, where a is an arbitrary constant. Note that $\bar{y}$ can not be obtained from $\tilde{y}$ by specializing a.

As seen in the introduction $\bar{y}$ is a singular solution. The component $\{y_1^2 - 4y_0, y_2 - 2\}$ is the component defining the *general solution*.

Without going to far in that direction, we would like to point out that the actual continuously differentiable solutions of the algebraic differential system $\mathcal{S}$ are not obviously completely defined by the zeros of Σ. In the introduction, Section A.1, we indeed gave a sample of examples where the actual solutions *jumps*, in a differentiable way, from one type of solution to the other. Such solutions live in non-integral rings.

E.3.5 EXAMPLE: Consider the two continuously differentiable functions f and g defined on $\mathbb{R}$ by

$$\begin{cases} f(x) = (x-1)^2 & \text{for } x \leq 1 \\ f(x) = 0 & \text{for } x \geq 1 \end{cases} \quad \text{and} \quad \begin{cases} g(x) = 0 & \text{for } x \leq 1 \\ g(x) = (x-1)^2 & \text{for } x \geq 1 \end{cases}$$

Both f and g are continuously differentiable *solutions* of $y'^2 - 4y = 0$ and none of f or g is zero. Nonetheless the product $f\,g$ is the zero function.

E.4 Quotient ideals

Quotient ideals bridge differential algebra to polynomial algebra. They are hence at the crux in algorithms as we shall see when studying the decomposition algorithms.

Recall that $\mathcal{R}$ is a differential ring containing a field isomorphic to $\mathbb{Q}$.

E.4.1 DEFINITION: Consider an ideal I in $\mathcal{R}$. For a non-empty subset S of $\mathcal{R}$ we define the quotient of I w.r.t. S to be

$$I : S = \{a \in \mathcal{R} \text{ such that } \forall s \in S\, sa \in I\}.$$

When S consist of a single element s we simply write $I : s$.

We immediately see that $I \subset I : S$ and, further, that $I : S$ is an ideal which is equal to the quotient of I w.r.t. to the ideal generated by S. But is it stable under derivation?

Let a be an element of $I : S$, where I is a differential ideal. Therefore

$$\forall s \in S \;\; s\,a \in I \;\; \Rightarrow \;\; \forall s \in S,\, \forall \delta \in \Delta \;\; \delta(s\,a) = \delta s\, a + s \delta a \in I$$

If $\delta s \in S$ then $\delta a \in I : S$. Hence

E.4.2 PROPOSITION: The quotient of a differential ideal by a subset which is stable under derivation is a differential ideal.

Now if R is a radical differential ideal, we know by Proposition E.1.8 that

$$s\,a \in R, \quad s,\, a \in \mathcal{R} \quad \Rightarrow \quad s\,\delta a \in R$$

Furthermore, if S is any subset of $\mathcal{R}$,

$$a^n \in R\!:\!S,\, n \in \mathbb{N} \quad \Rightarrow \quad \forall s \in S,\; s\,a^n \in R \;\Rightarrow\; \forall s \in S,\; s^n\,a^n \in R$$

and thus $a \in R\!:\!S$.

E.4.3 PROPOSITION: The quotient of a radical differential ideal of $\mathcal{R}$ by any subset of $\mathcal{R}$ is a radical differential ideal of $\mathcal{R}$.

E.4.4 DEFINITION: For an element s of $\mathcal{R}$, we define the saturation of I w.r.t. s as

$$I\!:\!s^\infty \;=\; \bigcup_{e=0}^{\infty} I\!:\!s^e \;=\; \{a \in \mathcal{R} \text{ such that } \exists \alpha \in \mathbb{N}\; s^\alpha a \in I\}$$

Note that $I\!:\!s^\infty$ is a differential ideal whenever I is a differential ideal.

The properties below give some insight on the nature of quotient ideals. Proving these properties is just a matter of writing down the definitions.

E.4.5 PROPOSITION:

- Let I be a differential ideal in $(\mathcal{R}, \Delta)$, and S a subset of $\mathcal{R}$.

$$S \subset I \;-\; I\!:\!S = \mathcal{R}.$$

- Let I be a differential ideal and s an element of $(\mathcal{R}, \Delta)$. Then

$$\sqrt{I}\!:\!s = \sqrt{I\!:\!s^\infty}$$

- If P is a prime differential ideal and s an element of $(\mathcal{R}, \Delta)$,

$$s \notin P \;\Rightarrow\; P\!:\!s = P.$$

A generalization of Proposition E.1.9 will be at the heart of the definition of the general solution.

E.4.6 PROPOSITION: Let Σ be a non-empty subset of $(\mathcal{R}, \Delta)$ and s an element of $\mathcal{R}$. Then

$$\{\Sigma\} = \{\Sigma\}\!:\!s \,\cap\, \{\Sigma, s\}.$$

F Decomposition algorithms

F.1 Reductions

Let $\mathcal{F}$ be a differential field of characteristic zero. We shall consider $\mathcal{F}\{Y\} = \mathcal{F}\{y_1, \ldots, y_n\}$ a ring of differential polynomials with coefficents in this differential field field.

Rankings

A ranking over $\mathcal{F}\{Y\}$ is a total order on $\Theta Y = \{\theta y_i,\ i = 1, \ldots, n,\ \theta \in \Theta\}$ such that for any derivation δ of Δ and for any derivatives $u, v \in \Theta Y$,

$$\delta u \geq u \quad \text{and} \quad u \geq v \ \Rightarrow\ \delta u \geq \delta v.$$

An essential property of these orders is that any sequence of derivatives in ΘY that is decreasing according to a ranking is finite.

For a given ranking over $\mathcal{F}\{Y\}$ and a given $v \in \Theta Y$, we define $\Theta_v Y$, the set of derivatives less or equal to v;

$$\Theta_v Y = \{\theta y_i,\ 1 \leq i \leq n,\ \theta \in \Theta \text{ such that } \theta y_i \leq v\}$$

A ranking is *sequential* if $\Theta_v Y$ is finite for any $v \in \Theta Y$. A ranking which satisfies

$$\text{ord } \theta > \text{ord } \theta' \ \Rightarrow\ \theta y_i > \theta' y_j \ \ \forall 1 \leq i, j \leq n$$

is said to be *orderly* and is sequential.

On the contrary, a ranking which satisfies

$$1 \leq i < j \leq n \quad \Rightarrow \quad \theta y_i \leq \theta' y_j,\ \forall \theta, \theta' \in \Theta.$$

is said to be lexigraphical and is not sequential.

For a subset Σ of $\mathcal{F}\{Y\}$, $\Theta_v \Sigma$ denotes the set of differential polynomials θq, where $q \in \Sigma$ and $\theta \in \Theta$, such that all the derivatives present in θq have equal or lower rank than v.

For a finite subset Σ of $\mathcal{F}\{Y\}$, we define $\Theta_\Sigma Y$ to be the set of derivatives present in the differential polynomials of Σ. Furthermore (Σ) and $\langle\Sigma\rangle$ will be respectively the ideal and the radical ideal generated by Σ in the polynomial ring $\mathcal{F}[\Theta_\Sigma Y]$.

F.1.1 EXAMPLE: In $(\mathbb{Q}\{y\},\delta)$, there is only one possible ranking: $y_0 < y_1 < y_2 < \cdots$.

Consider $p = y_1^2 - 4\,y_0$. Then

$$\Theta_{y_3} p \quad \text{is the set} \quad \{p,\, \delta p,\, \delta^2 p\} = \{y_1^2 - 4\,y_0,\ 2\,y_1\,y_2 + y_1,\ 2\,y_1\,y_3 + 2\,y_2^2 + y_2\}$$

and

$$\Theta_p Y \quad \text{is the set} \quad \{y_0, y_1\}$$

Auto reduced sets

Let $\mathcal{F}\{Y\}$ be endowed with a ranking. Let p be a differential polynomial of $\mathcal{F}\{Y\}$. The *leader* u_p and the *initial* i_p of p are respectively the highest ranking derivative appearing in p and the coefficient of its highest power in p. The *separant* of p is $s_p = \frac{\partial p}{\partial u_p}$. θu_p and s_p are respectively the leader and the initial of θp when θ is a *proper* derivation operator, that is when ord $\theta > 0$.

$$\begin{aligned} p &= i_p\, u_p^d + i_{d-1}\, u_p^{d-1} + \cdots + i_0 \\ \theta p &= s_p \theta u_p + \ldots \end{aligned}$$

F.Boulier, wrote a nice presentation of reduction algorithms in terms of rewrite systems [Bou94]. The reader can also refer to [Kol73, I.8] for a more detailed treatment of what follows.

A differential polynomial q is *partially reduced w.r.t.* p if no proper derivatives of u_p appears in q. If q is not partially reduced, let θu_p be the highest ranking derivative of u_p present in q. Let q' be the remainder of the pseudo-division of q by θp according to θu_p:

$$\exists \alpha' \in \mathbb{N},\quad s_p^{\alpha'}\, q \ \equiv\ q' \mod \theta p.$$

q' involves no derivatives of u_p higher or equal to θu_p. If q' is partially reduced w.r.t. p, we say that q' is the *partial differential remainder* of q w.r.t. p. Otherwize the process can be repeated with q' instead of q, so as to obtain, after a finite number of steps, q'' partially reduced w.r.t. p. We shall call d-prem the procedure which takes two differential polynomials q and p as entry and returns q'', partially reduced w.r.t. p such that

$$\exists \alpha \in \mathbb{N}\ \ s_p^{\alpha}\, q \ \equiv\ q'' \mod [p].$$

Furthermore, $q \in \mathcal{F}\{Y\}$ is *reduced w.r.t.* p if q is partially reduced w.r.t. to p and the degree of q in u_p is strictly less then the degree of p in u_p: $\deg_{u_p} q < \deg_{u_p} p$. If q is partially reduced w.r.t. p, the remainder $\bar{q}$ of the pseudo-division of q by p according to u_p is reduced w.r.t. p. It is called the *differential remainder* of q w.r.t. p.

$$\exists \beta \in \mathbb{N} \;\; i_p^\beta \, q \;\equiv\; \bar{q} \quad \mod p.$$

We shall call **d-rem** a procedure which takes two differential polynomials q and p as entry and returns $\bar{q}$, reduced w.r.t. p such that

$$\exists \alpha, \beta \in \mathbb{N} \quad i_p^\beta \, s_p^\alpha \, q \;\equiv\; \bar{q} \quad \mod [p].$$

Now, a subset A of $\mathcal{F}\{Y\}$ is *auto-reduced* if each of its element is reduced w.r.t. every other element of A. Such a set is finite and *triangular*: no pair of differential polynomials in A have the same leader. A differential polynomial q of $\mathcal{F}\{Y\}$ is reduced w.r.t. an auto-reduced set A if it is reduced w.r.t. any element of A.

Let A be an auto-reduced set. For any q in $\mathcal{F}\{Y\}$, we can compute h, a product of initials and separants of elements of A, and $\bar{q}$, reduced w.r.t. A, such that

$$h \, q \;\equiv\; \bar{q} \quad \mod [A]. \tag{1}$$

Computing $\bar{q}$ and h consists in a well organized sequence of partial reductions and reductions by the differential polynomials of A [Kol73, I.9]. We write $q \longrightarrow_A \bar{q}$ and we generalize the procedure **d-rem** to take as entry a differential polynomial q and an auto-reduced set A and to return the differential polynomial $\bar{q}$ reduced w.r.t. A satisfying (1).

When A is an auto-reduced set of $\mathcal{F}\{Y\}$, we will note $mathbf{h}_A$ the product of all initials and separants of the differential polynomial in A.

Characteristic sets

A ranking on $\mathcal{F}\{Y\}$ induces a pre-order on the set of all auto-reduced subsets of $\mathcal{F}\{Y\}$. Let $A = a_1, \ldots, a_r$ and $B = b_1, \ldots, b_s$ be two auto-reduced subsets. Assume their elements are arranged in order of increasing leaders: $u_{a_1} < \ldots < u_{a_r}$ and $u_{b_1} < \ldots < u_{b_r}$. A is said to have lower rank than B if there exists a positive integer k such that for i, $1 \leq i < k$, $u_{a_i} = u_{b_i} = u_i$ and $\deg_{u_i} a_i = \deg_{u_i} b_i$, and either

- k is less than r and s and

$$u_{a_k} \;<\; u_{b_k} \quad \text{or} \quad u_{a_k} = u_{b_k} = u_k \;\text{ and }\; \deg_{u_k} a_k < \deg_{u_k} b_k.$$

- $k = s + 1$ and then $r > s$.

F.1.2 PROPOSITION: Any sequence of stricly decreasing auto-reduced subsets of $\mathcal{F}\{Y\}$ is finite. Or, equivalently, among every non-empty set of auto-reduced subsets of $\mathcal{F}\{Y\}$ there exists an auto-reduced set of lowest rank.

This non-trivial result is proved in [Kol73, I.10]. It is a crucial point in many proofs of termination of algorithms and in the following definition.

F.1.3 DEFINITION: Let Σ be an non-empty subset of $\mathcal{F}\{Y\}$. An auto-reduced subset A of Σ is a characteristic set of Σ if it satisfies one of the equivalent properties [Bou94, 1.3]:

- A is an auto-reduced subset of Σ of lowest rank
- Σ has no non-zero element reduced w.r.t. A.

If Σ is a finite subset, determining a characteristic set of Σ is simply a question of making a finite number of comparisons of rank. We call **CharasteriX** a procedure which will extract a characteristic set from a finite set of differential polynomials.

If A is a characteristic set of a differential ideal I then

$$q \in I \quad \Rightarrow \quad q \longrightarrow_A 0$$

and

$$[A] \subset I \subset [A] : h_A^\infty .$$

If A is a characteristic set of a prime differential ideal P then

$$q \in P \quad - \quad q \longrightarrow_A 0$$

and

$$P = [A] : h_A^\infty .$$

Note that P being prime is only a sufficient condition to have this property, and this is a somewhat restrictive condition.

If A is an auto-reduced set of $\mathcal{F}\{Y\}$, A is not obviously a characteristic set of $[A] : h_A^\infty$, nor of $(A) : h_A^\infty$, even if these ideals are prime. Actually, determining when A is a characteristic set of $(A) : h_A^\infty$ and of $[A] : h_A^\infty$, is a crucial point in the decomposition algorithms, as we shall see it in the next sections.

F.1.4 EXAMPLE: Consider the set $A = a_1, a_2$ where

$$\begin{cases} a_1 &= (y_1 - 1)\, y_2 + 1 \\ a_2 &= y_1^2 - 1. \end{cases}$$

For any ranking for which $y_1 < y_2$, A is an auto-reduced set.

$y_1 + 1$ belongs to $(A) : h_A^\infty$ though it is reduced w.r.t. to A. Thus A is not a characteristic set of $(A) : h_A^\infty$.

F.2 Coherence and Rosenfeld's lemma

The main purpose of the decomposition algorithms is the following: given a finite set of differential polynomials Σ, find a finite number of auto-reduced sets $A_i,\ i = 1 \ldots r$, such that

- $\{\Sigma\} = \bigcap_{i=1}^{r} [A_i] : h_{A_i}^{\infty}$,
- A_i is a characteristic set of $R_i = [A_i] : h_{A_i}^{\infty}$. This implies

$$q \in R_i - q \longrightarrow_{A_i} 0.$$

Note that a membership test to the radical differential ideal $\{\Sigma\}$ immediately follows.

$$\begin{array}{rcl} q \in \{\Sigma\} & - & \forall i,\ 1 \leq i \leq r,\ q \in R_i \\ & - & \forall i,\ 1 \leq i \leq r,\ q \longrightarrow_{A_i} 0 \end{array}$$

To achieve this result, three stages can be distinguished in the algorithms:

(D) A typically differential treatment consisting of reductions.

(B) A bridge that transposes the differential problem into an algebraic one.

(A) An algebraic test and some splittings.

The phase **(D)** aims at constructing a *coherent* auto-reduced subset of $\{\Sigma\}$, because this notion of coherence together with the results of A.Rosenfeld [Ros59] are the key points of **(B)**. It is in **(A)** that the main differences among the decomposition algorithms live.

F.2.1 DEFINITION: An auto-reduced set A is coherent if it satisfies the following condition: whenever the leaders u_a, $u_{a'}$, of some $a,\ a' \in A$, admits a common derivative, say $v = \theta u_a = \theta' u_{a'}$, there exists a derivative $w < v$ such that $s_{a'}\,\theta a - s_a\,\theta' a' \in (\Theta_w A) : h_A^{\infty}$, s_a, $s_{a'}$ being the respective separant of a and a'.

It is in fact necessary and sufficient to check the condition on the minimal common derivatives [Kol73, IV.9]. We call **s-dpoly** the procedure which returns $s_{a'}\,\theta a - s_a \theta' a'$ when given two differential polynomials a and a' admitting $v = \theta u_a = \theta' u_{a'}$ as minimal common derivative. It returns zero otherwise.

Coherence is a sort of *involution*, as defined in other languages dealing with over determined partial differential equations. So to speak, an auto-reduced coherent set is *formally integrable*.

F.2.2 EXAMPLE: Consider the system of algebraic partial differential equations

$$\left\{ \begin{array}{lcl} a_1 & = & u_x^2 - 4u = 0 \\ a_2 & = & u_y - u = 0 \end{array} \right.$$

$A = a_1, a_2$ constitutes an auto-reduced set of $\mathbb{Q}(x,y)\{u\}$ endowed with derivations according to x and y.

We look in a straightforward way for a formal power series solution of that system at $x = 0, y = 0$.

$$\begin{array}{rcl} u(x,y) & = & u(0,0) + u_x(0,0)\,x + u_y(0,0)\,y \\ & & +u_{xx}(0,0)\,\dfrac{x^2}{2} + u_{xy}(0,0)\,x\,y + u_{yy}(0,0)\,\dfrac{y^2}{2} + \cdots \end{array}$$

When c is any non-zero complex number, $u(0,0) = c^2$ in a non-singular initial condition (the initials and the separants of a_1, a_2 do not vanish). It comes out that $u_x(0,0) = 2\,c$ and $u_y(0,0) = c^2$. If we wish to have the coefficients of the higher degree terms in the series solution, it should be enough to differentiate the equations.

Differentiating the first equation brings out

$$\begin{array}{rcl} u_x\,u_{xx} - 2\,u_x = 0 & \Rightarrow & u_{xx}(0,0) = 2, \\ u_x\,u_{xy} - 2\,u_y = 0 & \Rightarrow & u_{xy}(0,0) = \dfrac{c}{2}, \end{array}$$

while differentiating the second gives

$$\begin{array}{rcl} u_{xy} - u_x = 0 & \Rightarrow & u_{xy}(0,0) = 2c, \\ u_{yy} - u_y = 0 & \Rightarrow & u_{yy}(0,0) = c^2. \end{array}$$

We obtained two inconsistent values for $u_{xy}(0,0)$. That is typically the sort of problem that coherence avoids.

Coherence induces a sufficient condition for the existence of power series solution: when A is an auto-reduced coherent set, if there exists an algebraic zero of the ideal $(A) : h_A^\infty$ of $\mathcal{F}[\Theta_A Y]$ for which the initials and the separants of A do not vanish, then you can construct a zero of $[A] : h_A^\infty$. The algebraic zero thus found can be taken as the initial condition. This formalizes into the ROSENFELD LEMMA given below.

F.2.3 LEMMA: Let A be an auto-reduced coherent set. A necessary and sufficient condition for a differential polynomial q partially reduced w.r.t. A to belong to $[A] : h_A^\infty$ is that it belongs to $(A) : h_A^\infty$.

This immediately induces the following corollary.

F.2.4 COROLLARY: Let A be an auto-reduced coherent set. A necessary and sufficient condition for A to be a characteristic set of $[A] : h_A^\infty$ is that A is a characteristic set of $(A) : h_A^\infty$.

That A is coherent is only a sufficient condition: there exist auto-reduced sets which satisfy the above property though they are not coherent (see the example of [Bou96, section 5]). Nonetheless, when dealing with prime differential ideals this becomes a necessary and sufficient condition [Kol73, IV.9, lemma 2].

F.2.5 COROLLARY: A is a characteristic set of a prime differential ideal of $\mathcal{F}\{Y\}$ if and only if A is a coherent auto-reduced subset and A is a characteristic set of a prime ideal in $\mathcal{F}[\Theta_A Y]$.

The mentioned prime differential ideal must be $[A] : h_A^\infty$, and the prime ideal $(A) : h_A^\infty$.

Assume we are given a finite subset Σ of $\mathcal{F}\{Y\}$. The first common step **(D)** to any decomposition algorithm consists thus in computing a coherent auto-reduced subset A of $\{\Sigma\}$ such that all the element of Σ are reduced to zero by A.

F.2.6 ALGORITHM: **Coherent-Auto-Reduced** .

INPUT: Σ a set of non-zero differential polynomials in $(\mathcal{F}\{Y\}, \Delta)$, endowed with a ranking

OUTPUT: A pair A, Σ where A is an auto-reduced coherent set such that

$$[A] \subset [\Sigma] \subset [A] : h_A^\infty.$$

If $\Sigma \cap \mathcal{F} \neq \emptyset$ and $\Sigma \cap \mathcal{F} \neq \{0\}$ then return $\emptyset$;

$A :=$ CharasteriX (Σ);

$R :=$ { d-rem(q, A) | $q \in \Sigma \setminus A$ }

$S :=$ { d-rem (s-dpoly (a, a'), A) | a, $a' \in A$}

If $R \cup S = \{0\}$ or $\emptyset$

then return A, Σ;

else $A :=$ Coherent-Auto-Reduced $(\Sigma \cup R \cup S)$;

fi;

end;

A characteristic set of $\Sigma \cup R \cup S$ has strictly lower rank than one of Σ. By Proposition F.1.2, any strictly decreasing sequence of auto-reduced sets is finite, thus this algorithm will always terminate.

F.3 Decomposition into prime differential ideals

Let Σ be a finite subset and let $A =$Coherent-Auto-Reduced(Σ).

First, if A is the characteristic set of a prime ideal, this ideal must be $(A) : h_A^\infty$ and by Corollary F.2.5, A is the characteristic set of the prime ideal $[A] : h_A^\infty$.

We have $[A] \subset [\Sigma] \subset [A] : h_A^\infty$. By Rosenfeld's lemma (Lemma F.2.5), $[A] : h_A^\infty$ is prime. Thus $[A] \subset \{\Sigma\} \subset [A] : h_A^\infty$ and finally $\{\Sigma\} : h_A = [A] : h_A^\infty$.[1]

Then the idea of the algorithm is to split the system as thanks to Proposition E.4.6 and Proposition E.1.9

$$\{\Sigma\} = \{\Sigma\} : h_A \cap \{\Sigma, h_A\} = [A] : h_A^\infty \cap \bigcap_{a \in A} \{\Sigma, i_a\} \cap \bigcap_{a \in A} \{\Sigma, s_a\}.$$

And $\{\Sigma, i_a\}$ and $\{\Sigma, s_a\}$ contain auto-reduced sets of lower rank than A.

What we thus want is to determine when A is the characteristic set of a prime ideal. Ritt proposed a method [Rit66, IV.15] to check that A is the characteristic set of a prime ideal. It consists in factoring successively the elements of A according to a tower of extensions thus constructed. This process is in fact not really effective.

In case A is not a characteristic set of $(A) : h_A^\infty$, there exists an element $\bar{q} \in (A) : h_A^\infty$, reduced with respect to A. Then

$$\{\Sigma\} = \{\Sigma, q\}$$

and the set $\{\Sigma, q\}$ contains an auto-reduced set of strictly lower order than A.

Now, if $(A) : h_A^\infty$ is not prime, by definition, we may find $q_1, q_2 \notin (A) : h_A^\infty$ such that $q_1 q_2 \in (A) : h_A^\infty$. Let $\bar{q}_1, \bar{q}_2$ be the respective differential remainders of q_1, q_2. Obviously they are non-zero, and $\bar{q}_1 \bar{q}_2$ also belong to $(A) : h_A^\infty$. Therefore, whenever $(A) : h_A^\infty$ is not prime, there exist non-zero $\bar{q}_1, \bar{q}_2$ reduced w.r.t. A such that $\bar{q}_1 \bar{q}_2$ belongs to $(A) : h_A^\infty$. We have

$$\{\Sigma\} = \{\Sigma, q_1\} \cap \{\Sigma, q_2\}$$

and $\{\Sigma, \bar{q}_i\}$, for $i = 1$ or 2, contains an auto-reduced set of lower rank.

We shall call **Ritt-tower** the procedure which takes an auto-reduced coherent set as entry and returns either a single differential polynomial $\bar{q}$ or a pair of differential polynomials $\bar{q}_1, \bar{q}_2$ as described above, whenever A is not the characteristic set of a prime ideal.

The algebraic resolution **(A)** proposed by Ritt thus consists into recursive call to the whole algorithm with entry finite sets having a lower characteristic set until we

[1] To ensure that $\{\Sigma\} : h_A = [A] : h_A^\infty$, it would have been enough that $[A] : h_A$ was radical.

obtain characteristic set of prime ideals. The process certainly ends: decreasing sequences of auto-reduced sets are constructed and according to Proposition F.1.2 the sequences must be finite.

The complete Ritt decomposition algorithm is given below

F.3.1 ALGORITHM: **Ritt-Decomposition**

INPUT: Σ, a finite set

OUTPUT: $U = A_1, \ldots, A_r$, a finite sequence of characteristic sets of prime ideals such that $\{\Sigma\} = \bigcap_{i=1}^{r} [A_i] : h_{A_i}^{\infty}$

$A :=$ Coherent-Auto-Reduced (Σ) ;

$Q :=$ Ritt-Tower (A);

If $Q = \emptyset$ # *i.e. A is a characteristic set of a prime ideal,* $(A) : h_A^{\infty}$

then $U = A$, Ritt-Decomposition $(\{\Sigma, s_a\})_{a \in A}$, Ritt-Decomposition $(\{\Sigma, i_a\})_{a \in A}$;

else $U =$ Ritt-Decomposition $(\{\Sigma, q\})_{q \in Q}$;

fi;

end;

The Gröbner bases techniques, which appeared after Ritt's work, brought some effective way to decide if A is a characteristic set of a prime ideal. This can be decomposed into solving the two problems.

1. when does $(A) : h_A^{\infty}$ contain an element q reduced w.r.t. A, and exhibit such an element.

2. when is $(A) : h_A^{\infty}$ prime and, if it is not, find the $\bar{q}_1$, $\bar{q}_2$.

The first question can be answered by the computation of a Gröbner basis.

A term order on $\mathcal{F}[\Theta_A Y]$ *induced* by the ranking on $\mathcal{F}\{Y\}$ is a lexicographical term order which respects the ordering given by the ranking.

Let G be a Gröbner basis of $(A) : h_A^{\infty}$ in $\mathcal{F}[\Theta_A Y]$ according to such an order. $(A) : h_A^{\infty}$ contains an element reduced w.r.t. A if and only if G contains such an element [Bou94].

One could also answer on the primality of $(A) : h_A^{\infty}$. In [BW93, chapter 8] or [GTZ88] are presented algorithms to compute a prime and a primary decomposition of an algebraic ideal. Thus if $(A) : h_A^{\infty}$ is radical[2] and has only one algebraic prime component, then it is a prime ideal.

[2] this reveals in fact to be always the case thanks to Lazard's lemma

But this is a quite costly algorithm. So one should first question the need for $(A) : h_A^\infty$ to be prime since Rosenfeld's lemma has a wider range of application. This question was first raised by F.Boulier [Bou94].

F.4 Decomposition into regular ideals

The notion of regular ideals was introduced with the algorithm Rosenfeld-Gröbner [Bou94] which first handled them. Basically, an ideal R is *regular*, for a certain ranking, if $R = (A) : h_A^\infty$, where A is an auto-reduced coherent subset of $\mathcal{F}\{Y\}$. Identically, a differential ideal R is *regular*, for a certain ranking, if $R = [A] : h_A^\infty$, where A is an auto-reduced coherent subset of $\mathcal{F}\{Y\}$.

Unfortunately, regular differential ideals have not yet gained a more intrinsic definition, we mean a definition that would be independent of the ranking. Yet they are the best thing after prime differential ideals.

First, consider $\mathcal{F}'$ a field extension of $\mathcal{F}$. Let P be a differential ideal of $\mathcal{F}\{Y\}$. If P is a prime differential ideal of $\mathcal{F}\{Y\}$, then the radical differential ideal generated by P in $\mathcal{R}'\{Y\}$ is a regular differential ideal.

Secondly, it appears that these ideals together with the Rosenfeld-Gröbner decomposition could replace the prime differential ideals in the fundamental role they play in the development of the theory [PG97, part I].

Lazard's lemma [BLOP95] settles the crucial properties of regular ideals in polynomial rings. These properties are readily lifted to the polynomial differential ring by Rosenfeld's lemma to give the following theorem, which can be seen as a generalization of [Ros59, III, Theorem 3].

F.4.1 THEOREM: Let $\mathcal{F}\{Y\}$ be endowed with a given ranking and let $A = a_1, \ldots, a_r$ be an auto-reduced coherent subset of $\mathcal{F}\{Y\}$.

- The regular differential ideal $R = [A] : h_A^\infty$ is radical.
- A characteristic set B of an essential prime component of R is such that $B = b_1, \ldots, b_r$ and $u_{b_i} = u_{a_i}$ for any $1 \leq i \leq r$.

The proof of this theorem can be found in [BLOP95].

Just as in previous section, let us consider a finite set Σ of differential polynomials of $\mathcal{F}\{Y\}$ and let

$$A = \text{Coherent-Auto-Reduced } (\Sigma)$$

As we noticed it in the previous section, that $[A] : h_A^\infty$ is radical, thanks to Theorem F.4.1, is sufficient to have $\{\Sigma\} : h_A = [A] : h_A^\infty$.

We thus can make the splittings

$$\{\Sigma\} = \{\Sigma\}:h_A \cap \{\Sigma,\, h_A\} = [A]:h_A^\infty \cap \bigcap_{a\in A}\{\Sigma,\, i_a\} \cap \bigcap_{a\in A}\{\Sigma,\, s_a\}$$

Remains to check when A is a characteristic set of $[A]:h_A^\infty$ and therefore when

$$q \in [A]:h_A^\infty \quad - \quad q \longrightarrow_A 0.$$

According to Corollary F.2.4 this happens whenever A is a characteristic set of $(A):h_A^\infty$. We thus only have to check that no non-zero element of $(A):h_A^\infty$ is reduced w.r.t. A. We have seen how to proceed with a Gröbner basis technique in the previous section.

Let G be a Gröbner basis of $(A):h_A^\infty$ in $\mathcal{F}[\Theta_A Y]$ according to a term order induced by the ranking on $\mathcal{F}\{Y\}$. $(A):h_A^\infty$ has a non-zero element reduced w.r.t. A if and only if G has such an element. We shall call **Reduced-Element** a procedure which takes in entry a coherent auto-reduced set and returns such an element when it exists and zero otherwise.

A decomposition of $\{\Sigma\}$ into regular differential ideal consists in computing a finite set of auto-reduced coherent sets $A_1, \ldots, A_r$ such that

- $\{\Sigma\} = \bigcap_{i=1}^{r} [A_i]:h_{A_i}^\infty$,
- A_i is a characteristic set of $R_i = [A_i]:h_{A_i}^\infty$. This implies

$$q \in R_i - q \longrightarrow_{A_i} 0.$$

To achieve such a decomposition, we can proceed with the algorithm Ritt-Decomposition of the previous section, where we replace the procedure Ritt-Tower with the procedure Reduced-Element described above.

F.4.2 Algorithm: **Regular-Decomposition**

INPUT: Σ, a finite set

OUTPUT: $U = A_1, \ldots, A_r$, a finite sequence of characteristic sets of regular ideals such that $\{\Sigma\} = \bigcap_{i=1}^{r} [A_i]:h_{A_i}^\infty$

$A :=$ Coherent-Auto-Reduced (Σ) ;

$q :=$ Reduced-element (A)

If $q = 0$ *# i.e. A is a characteristic set of $(A):h_A^\infty$*

then $U = A$, Regular-Decomposition $(\{\Sigma, s_a\})_{a\in A}$, Regular-Decomposition $(\{\Sigma, i_a\})_{a\in A}$;

else $U =$ Regular-Decomposition $(\{\Sigma, q\})$

fi;

end;

A great many of improvements should be brought to this algorithm to give the Rosenfeld-Gröbner algorithm . We can only invite the reader to read about it in [Bou97] which is presently in preparation.

An immediate improvement we can think of is to extract more information of the Gröbner basis we compute. More precisely, once we have computed

$$A = \text{Coherent-Auto-Reduced } (\Sigma)$$

we computed a Gröbner basis G of $(A) : h_A^\infty$ to determine if there were elements in $(A) : h_A^\infty$ reduced w.r.t. A. From G we may in fact extract an auto-reduced set C such that

- C is a characteristic set of $[C] : h_C^\infty$
- $[C] : h_C^\infty = [A] : h_A^\infty$

on condition its initials and separants are not zero divisors modulo $(A) : h_A^\infty$.

A similar criterion of *invertibility* of the initials and separants also appear in [KRHM]. The interesting part of the presentation given therein is that the computations are lead with linear algebra instead of Gröbner bases techniques.

The exposition of next sections will actually be supported by the the Rosenfeld-Gröbner decomposition and therefore we will speak of Rosenfeld-Gröbner decompositions instead of Regular decompositions. The implementations will be done with the *diffalg* package which implements the Rosenfeld-Gröbner algorithm and several facilities for handling algebraic differential equations. The package is available on Maple V.3 and will be in the main library of Maple V.5.

Part III

Algebraic differential equations

G Essential components of a differential polynomial

None of the decompositions we have presented in the last section is minimal. In both cases, a component may contain other ones. In the Rosenfeld-Gröbner decomposition, it may happen that only some essential components of a regular component are redundant.

Determining when a prime or regular differential ideal given by its characteristic set is contained in another one is an open problem. It is even a problem tantamount to the problem of computing differential bases of these differential ideals.

We shall present here an algorithm which determines the minimal decomposition for the radical differential ideal generated by a single differential polynomial: from a Rosenfeld-Gröbner decomposition, we will extract the essential components. We do not though solve the inclusion problem; the foundation of the algorithm lies in the Low power theorem.

Consider p and a differential polynomials, a being irreducible and s_a being the separant of a. The Low power theorem provides a necessary and sufficient condition for $[a] : s_a^\infty$ to be an essential prime component of $\{p\}$.

The criterion lies on the degree of the differential polynomial p. It is beautifully simple and algorithmic in essence. It is quite amazing that the early intuitions of the French school can be formulated in such an algebraic way. Even more surprising is that Ritt's early proof [Rit36], for ordinary differential polynomial in one differential indeterminate, would use essentially complex analysis tools, such as a Painlevé transformation. As Ritt put it "this would suggest a search for analogies between critical point problem and the problem of singular solutions".

Though this proof is precious for the understanding of the analytic relations of the singular solutions with the general solution, we will stick to an algebraic exposition. The tremendous advantage of the algebraic way is that it readily gives the generalization for differential polynomials in more than one differential indeterminate and, furthermore, to partial differential equations. H.Levi, for the sufficiency, and A.Hillman, for the necessity, took the lead in the proofs.

G.1 The general component

The algebraic definitions of the general and particular solutions of an irreducible differential polynomial are due J.F.Ritt [Rit30, part II].

Consider a differential polynomial p in $\mathcal{F}\{Y\}$. In the following sections we will consider that $\mathcal{F}\{Y\}$ is endowed with a ranking and we will note u_p the leader and $s_p = \frac{\partial p}{\partial u_p}$ the separant of p.

We recall from Section E.2 that a zero of a set of differential polynomials is an element in an integral over-ring of $\mathcal{F}$ which makes vanish all these differential polynomials.

With this in mind, the *singular zeros* are the common zeros of p and s_p and therefore of the radical differential ideal $\{p, s_p\}$. On the other hand, the *non-singular zeros* are quite naturally part of the so called *general solution.*

Now, recall from Property E.4.6 that

$$\{p\} = \{p\} : s_p \ \cap \{p, s_p\}.$$

As $\{p\} : s_p$ does not contain s_p, the non-singular zeros must be zeros of $\{p\} : s_p$. The properties of this radical differential ideal can be studied through the following lemma [Kol73, I.11] which is similar to Rosenfeld lemma:

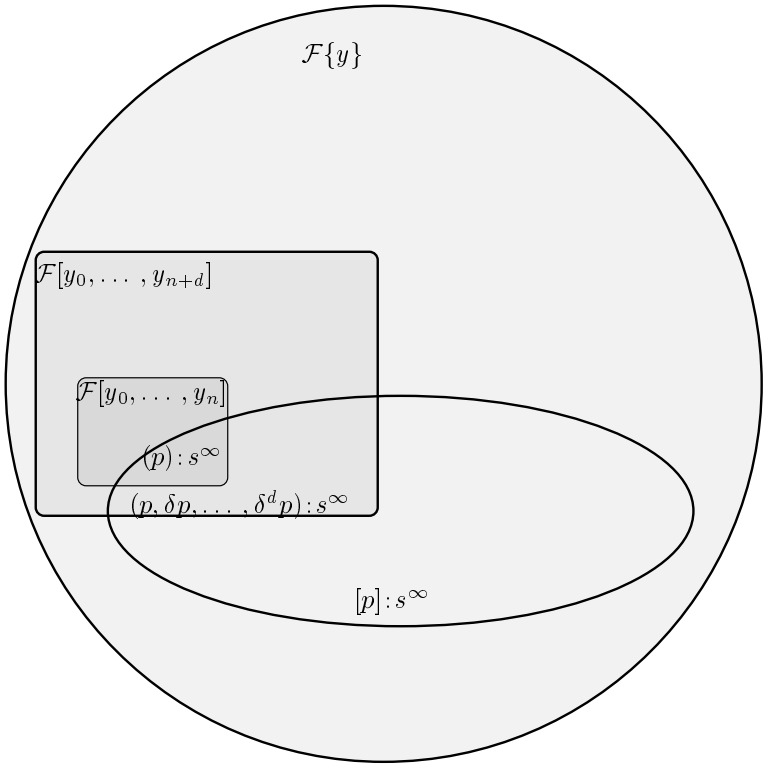
G.1.1 LEMMA: If $q \in [p] : s_p^\infty$ and v denotes the highest derivative of u_p present in $p\,q$ then $q \in (\Theta_v p) : s_p^\infty$.

This implies that for any derivatives v of u_p, $[p] : s_p^\infty \cap \mathcal{F}[\Theta_v Y] = (\Theta_v p) : s_p^\infty$.

ILLUSTRATION: consider an ordinary differential polynomial ring in one differential indeterminate $\mathcal{F}\{y\}$. We shall note $y_i = \delta^i y$. Let p be a differential polynomial of order n.

Assume q is a differential polynomial that belongs to $[p] : s_p^\infty$. If its order is not more than $n + d$, q belongs to $(p, \delta p, \ldots \delta^d p) : s_p^\infty$.

In fact, the intersection of $[p] : s_p^\infty$ with $\mathcal{F}[y_0, y_1, \ldots, y_n]$ is exactly $(p) : s_p^\infty$. And likewise, the intersection of $[p] : s_p^\infty$ with $\mathcal{F}[y_0, y_1, \ldots, y_{n+d}]$, for any integer $d \geq 0$, is $(p, \delta p, \ldots \delta^d p) : s_p^\infty$.



Besides, as s_p contains the multiple factors of p, $(p) : s_p^\infty$ is a radical ideal. What can we conclude on $[p] : s_p^\infty$, then?

Take a differential polynomial q such that for a positive integer α, q^α belongs to $[p] : s_p^\infty$. Let $\bar{q}$ be the partial differential remainder of q w.r.t. p.

$$\exists \beta \in \mathbb{N} \quad \text{such that } s_p^\beta \, q \equiv \bar{q} \mod [p].$$

Thus $\bar{q}^\alpha$ belongs to $[p] : s_p^\infty$ and is partially reduced w.r.t. p. In virtue of Lemma G.1.1, $\bar{q}^\alpha$ belongs to $(p) : s_p^\infty$. It follows that $\bar{q}$ also belongs to $(p) : s_p^\infty$, since this ideal is radical, and therefore q belongs to $[p] : s_p^\infty$.

G.1.2 Proposition: For any differential polynomial p of $\mathcal{F}\{Y\}$

- $[p] : s_p^\infty$ is a radical differential ideal and is thus equal to $\{p\} : s_p$.

$$\forall p \in \mathcal{F}\{Y\} \; [p] : s_p^\infty = \{p\} : s_p$$

- For any derivative v of u_p, $(\Theta_v p) : s_p^\infty$ is a radical ideal.

The second property comes in a straightforward way from the fact that

$$[p] : s_p^\infty \cap \mathcal{F}[\Theta_v Y] = (\Theta_v p) : s_p^\infty.$$

Irreducible differential polynomial

We are assuming in this paragraph that p is an irreducible differential polynomial. Then $(p):s_p^\infty = (p)$ is a prime ideal and a polynomial belongs to it if and only if it is divisible by p.

Assume that a pair of differential polynomials q, q' is such that $q\,q' \in [p]:s_p^\infty$ and let $\bar{q}$, $\bar{q}'$ be their partial remainder w.r.t. p.

$$\exists \beta, \beta' \text{ such that } s_p^\beta\, q \;\equiv\; \bar{q} \mod [p] \quad \text{and} \quad s_p^{\beta'}\, q' \;\equiv\; \bar{q}' \mod [p]$$

Then

$$s_p^{\beta'+\beta}\, q\, q' \;\equiv\; \bar{q}\,\bar{q}' \mod [p]$$

and therefore $\bar{q}\,\bar{q}'$ is a differential polynomial that belongs to $[p]:s_p^\infty$ and which is partially reduced w.r.t. p. Thus, by Lemma G.1.1, $\bar{q}\,\bar{q}'$ belongs to $(p):s_p^\infty = (p)$. This is a prime ideal and thus either $\bar{q}$ or $\bar{q}'$ belongs to it. It then follows that either q or q' belongs to $[p]:s_p^\infty$.

G.1.3 Proposition: If p is an irreducible differential polynomial of $\mathcal{F}\{Y\}$ then

- $[p]:s_p^\infty$ is a prime differential ideal.
- If q is a differential polynomial of $[p]:s_p^\infty$ which is partially reduced w.r.t. p then q must be divisible by p.
- For any derivative v of $\mathcal{F}\{Y\}$, $(\Theta_v p):s_p^\infty$ is a prime ideal.

As a consequence, $\{p\}:s_p = [p]:s_p^\infty$ contains no non-zero differential polynomial reduced w.r.t. p. On the contrary, the radical differential ideal $\{p, s_p\}$ contains such an element. Therefore, $\{p\}:s_p$ contains no essential component of $\{p, s_p\}$. It must be an essential component of $\{p\}$. This points the way for the definition of the general component.

G.1.4 Definition: Let p be an irreducible differential polynomial and note s_p its separant.

(G).The *general component* of p is the only essential component of $\{p\}$ which does not contain s_p:

$$\mathcal{G}_p = \{p\}:s_p.$$

(S).A *singular component* of p is a prime differential ideal which contains $\{p, s_p\}$. The *essential singular components* are the singular components which are present in the minimal decomposition of $\{p\}$.

Regular differential polynomials

If a regular ideal has a characteristic set consisting of a single differential polynomial, this latter satisfies the following definition.

G.1.5 DEFINITION: A differential polynomial p of $\mathcal{F}\{Y\}$ is *regular* provided p is square free and has no factor independent of its leader.

A regular differential polynomial p has no common factor with its separant. Thus $(p) : s_p^\infty = (p)$. By Lemma G.1.1 any differential polynomial in $[p] : s_p^\infty$ partially reduced with respect to p must be in (p) or equivalently it must be divisible by p.

G.1.6 PROPOSITION: Let p be a regular differential polynomial. A differential polynomial q that belongs to

$$[p] : s_p^\infty \ = \ \{p\} : s_p$$

and is partially reduced w.r.t. p must be divisible by p.

Furthermore we would like to extend the notion of general component to regular differential polynomials.

G.1.7 PROPOSITION: Assume the irreducible factors of a regular differential polynomial p are

$$p = \prod_{i=1}^{r} p_i.$$

Let s_p be the separant of p and s_i be the separant of p_i. Then

$$\{p\} : s_p = \bigcap_{i=1}^{r} \{p_i\} : s_i$$

is a minimal decomposition of $\{p\} : s_p$ and each $\{p_i\} : s_i$ is an essential prime component of $\{p\}$.

PROOF: Note first that for any pair p_i, p_j with $i \neq j$, p_j is partially reduced w.r.t. p_i and not divisible by p_i. Therefore, p_j does not belong to the prime differential ideal $\{p_i\} : s_i$ for $j \neq i$. Thus, none of the $\{p_i\} : s_i$ contains another one.

Owing to property E.1.9

$$\{p\} : s_p \ = \ \left\{ \prod_{i=1}^{r} p_i \right\} : s_p \ = \ \bigcap_{i=1}^{r} \{p_i\} : s_p.$$

It remains to show that

$$\{p_i\} : s_p = \{p_i\} : s_i.$$

Let $q \in \{p_i\} : s_p$. This means that $s_p\, q \in \{p_i\}$. The only term in

$$s_p\, q = \left(\sum_{k=1}^{r} s_k \prod_{j \neq k} p_j \right) q$$

which is not trivially in $\{p_i\}$ is $s_i \left(\prod_{j \neq i} p_j \right) q$. Therefore

$$\left(\prod_{j \neq i} p_j \right) \; q \; \in \; \{p_i\} : s_i$$

and since p_j, for $j \neq i$, does not belong to the prime differential ideal $\{p_i\} : s_i$, $q \in \{p_i\} : s_i$. We have shown that $\{p_i\} : s_p \subset \{p_i\} : s_i$ and the convert inclusion is easy to see.

Recall from Proposition E.4.6 that

$$\{p\} \; = \; \{p\} : s_p \; \cap \; \{p, s_p\}.$$

Any component of $\{p, s_p\}$ contains an element free of the leader of p. Thus no component of $\{p, s_p\}$ can be contained in $\{p_i\} : s_i$. Therefore each $\{p_i\} : s_i$ is an essential prime component of $\{p\}$. □

We have

$$\begin{aligned} \{p, s_p\} &= \left\{ \prod_{i=1}^{r} p_i, \sum_{k=1}^{r} s_k \prod_{j \neq k} p_j \right\} = \bigcap_{i=1}^{r} \left\{ p_i, s_i \prod_{j \neq i} p_j \right\} \\ &= \left(\bigcap_{i=1}^{r} \{p_i, s_i\} \right) \cap \left(\bigcap_{i=1}^{r} \{p_i, p_j\} \right) \end{aligned}$$

The common zeros of two factors of p can be considered as singular zeros. But $\{p_i\} : s_i \cap \{p_i, s_i\} = \{p_i\} \subset \{p_i, p_j\}$ and therefore none of the prime components of $\{p_i, p_j\}$ is essential in the decomposition of $\{p\}$. We can write:

$$\{p\} = \bigcap_{i=1}^{r} \left(\{p_i\} : s_i \cap \{p_i, s_i\} \right)$$

But again, some essential components of the $\{p_i, s_i\}$ can be redundant in the decomposition of $\{p\}$. They may contain $\{p_i\} : s_i$ but also $\{p_j\} : s_j$ for a $j \neq i$.

Any differential polynomials

As s_p contains the factors independent of u_p and the multiple factors of p, it is delicate to define the general and singular solutions of any differential polynomial. Nonetheless, the COMPONENT THEOREM [Kol73, IV.14] ensures a specific structure to the minimal decomposition of $\{p\}$.

G.1.8 THEOREM: Let p be a nonzero differential polynomial in $\mathcal{F}\{Y\}$. If P is an essential component of $\{p\}$, there exists an irreducible differential polynomial $a \in \mathcal{F}\{Y\}$ such that P is the general component of a : $P = \mathcal{G}_a = \{a\} : s_a = [a] : s_a^\infty$.

G.1.9 EXAMPLE: Consider the differential polynomial in $\mathbb{Q}(x,y)\{u\}$ endowed with the derivations according to x and y,

$$p = u - xu_x^2 - u_y^2.$$

For a ranking where $u_x > u_y$, the Rosenfeld-Gröbner decomposition is

$$\{p\} = \mathcal{G}_p \cap [u_x, -u + u_y^2] \cap [u].$$

According to Theorem F.4.1 and Theorem G.1.8, we can assert that none of the components of the regular differential ideal $[u_x, -u + u_y^2]$ appears in the minimal decomposition of $\{p\}$. We will get this latter by checking whether $[u]$ is an essential component or not.

G.2 The preparation process

Assume p is contained in the general component of an irreducible differential polynomial a. The Low power theorem provides a necessary and sufficient condition for $\mathcal{G}_a$ to be an essential component of $\{p\}$. The criterion lies on the manner a makes itself visible in the algebraic structure of p. This structure is revealed by writing p as a differential polynomial in a.

If m is a differential monomial in a differential polynomial ring $\mathcal{R}\{z\}$ with coefficients in a differential ring $\mathcal{R}$[1]

$$m \;=\; \prod_{i=1}^{r} \theta_i\, z,$$

we shall write

$$m\,(a) \;=\; \prod_{i=1}^{r} \theta_i\, a$$

[1] We will have to consider most of the time $\mathcal{R} = \mathcal{F}\{Y\} = FY$

G.2.1 DEFINITION: Let p and a be differential polynomials, a irreducible. A preparation equation of p w.r.t. a is an equation

$$c_{-1}\, p = \sum_{\gamma=0}^{l} c_\gamma\, m_\gamma(a) \tag{1}$$

where $m_0, \ldots, m_l$ are distinct differential monomials and $c_{-1}, c_0, \ldots, c_l$ are differential polynomials not contained in $\mathcal{G}_a$

The existence and computability of such a preparation equation is proved by the inductive argument below.

Assume p is partially reduced w.r.t. a. A preparation equation is given by a a-adic development of p:

$$p = c_0 + c_1\, a + c_2\, a^2 + \ldots + c_l\, a^l,$$

where the c_i are also partially reduced w.r.t. a but not divisible by a. According to Proposition G.1.3, they are not in $\mathcal{G}_a$.

Otherwise, p involves a highest ranking proper derivative v of the leader u_a of a. Assume we know how to proceed for any derivative of u_a of rank strictly less than v. Let θ be the derivation operator such that $v = \theta u_a$. Then $\theta a = s_a v + t$.

Let e be the degree of p in v. In the (θa)-adic expansion of $s_a^e\, p$,

$$s_a^e\, p = c_0 + c_1\, (\theta a) + c_2\, (\theta a)^2 + \ldots + c_l\, (\theta a)^l,$$

the coefficients c_i involve only derivatives of u_a of strictly lower rank than v, and s_a does not belong to $\mathcal{G}_a$. A preparation equation of

$$c_0 + c_1(\theta a) + c_2(\theta a)^2 + \ldots + c_l(\theta a)^l$$

will immediately give a preparation equation for p.

For a proper derivation operator θ, $\theta\, a$ is linear in $\theta\, u_a$. Indeed $\theta a = s_a\, \theta u_a + t$, where t has no derivatives of higher or equal rank to θu_a. Therefore, when p is not partially reduced by a and $v = \theta\, u_a$ is the highest ranking proper derivative of u_a in p, we can replace the computation of the (θa)-adic expansion of p by the two following operations

- substitute in p $\qquad v = \theta\, u_a \quad$ by $\quad \dfrac{\theta\, a - t}{s}$
- clear out fraction; c_{-1} will be the denominator of the expression obtained.

Furthermore the computation of the a-adic expansion can be improved with a divide and conquer technique as can be done for computing generalized Taylor series [BP94, I.3].

The basic operations like finding the highest derivative of u_a in p can be performed with the *diffalg* package. We just give the specification of the algorithm we have implemented in MapleV.3.

G.2.2 ALGORITHM: **Preparation-Equation**

INPUT: p and a differential polynomials of $\mathcal{F}\{Y\}$, a is irreducible

OUTPUT:

- A differential polynomial in $(\mathcal{F}\{Y\})\{z\}$ $prep = \sum_{\gamma=0}^{l} c_\gamma m_\gamma$ where m_γ are differential monomials in z and c_γ are differential polynomials in $\mathcal{F}\{Y\}$ partially reduced w.r.t. a but not divisible by a.
- A differential polynomial c_{-1} partially reduced w.r.t. a but not divisible by a.

Let us just see on an example how it works.

G.2.3 EXAMPLE: In the ordinary differential polynomial ring $\mathbb{Q}\{y\}$, let

$$p = 4\,y_1^2\,y_2^2 - 16\,y_1^2\,y_2 + 15\,y_1^2 + 4\,y_0.$$

The preparation equation of p with respect to $a = y_0$ is trivial:

$$p = 4\,z_1^2\,z_2^2 - 16\,z_1^2\,z_2 + 15\,z_1^2 + 4\,z_0.$$

Let $a = y_1^2 - 4\,y_0$; y_1 is its leader: $u_a = y_1$. The highest derivative of y_1 in p is $y_2 = \delta y_1 = \delta u_a$. We have

$$\delta a \;=\; 2\,y_1\,y_2 - 4\,y_1.$$

In p we make the substitution

$$y_2 \longrightarrow \frac{\delta z + 4\,y_1}{2\,y_1}.$$

This results in

$$p = z_1^2 - y_1^2 + 4\,y_0, \quad \text{where we have noted } z_1 = \delta z$$

Written like that, p is partially reduced with respect to a. The remainder and the quotient of the pseudo-division of p' by a according to $u_a = y_1$ are respectively z_1^2 and -1:

$$p = -1.z_0 + z_1^2$$

This is the result of the above algorithm. A preparation equation of p with respect to $a = y_1^2 - 4\,y_0$ is thus

$$p = (\delta a)^2 - a.$$

Let ρ be the minimal degree of the monomials m_γ in the preparation equation (1) of p w.r.t. a. If we denote the differential monomials m_γ of degree ρ by $m'_1, \ldots, m'_l$, then the preparation equation (1) yields a *preparation congruence* of p w.r.t. a

$$c_{-1}\, p \;\equiv\; \sum_{\gamma=0}^{l'} c'_\gamma\, m'_\gamma(a) \mod [a]^{\rho+1} \tag{2}$$

We shall call **Preparation-Congruence** a procedure which computes it.

Note that the preparation equation of p w.r.t. a is not unique. Nonetheless, ρ and the set of monomials m'_γ depends only on p and a [Hil43].

G.3 The Low power theorem

The Low power theorem is one of the most sophisticated theorem in differential algebra. J.F.Ritt first showed the theorem for ordinary algebraic differential equations in [Rit36]. The sufficiency would use "a transformation belonging to the class of differential equations whose solutions have fixed critical points". H. Levi brought a purely algebraic proof based on the study of the ideal $[z^p]$ ([Lev42] and [Lev45] for partial differential equations). Besides, the original necessity proof [Rit36] requires the construction of a solution into power series of a constant according to a *polygon process*. A.Hillman uses this process in a more algebraic way to show the *Leading coefficient theorem* [HM62] . E.Kolchin's presentation uses this latter theorem for the necessity proof. He introduces the notion of domination, which allows to generalize Levi's lemma, to prove the sufficiency [Kol73, IV].

Albeit the difficulty of the proofs, the statement of the theorem is very simple. When a differential polynomial p of $\mathcal{F}\{y_1, \ldots, y_n\}$ is contained in a $\{y_i\}$, that is, when p vanishes for $y_i = 0$, then $\{y_i\}$ is an essential prime component of $\{p\}$ if and only if the lowest degree terms of p contains no proper derivatives of y_i.

Now when p is contained in the general component of an irreducible differential polynomial a, then the criterion is just the same, but applied on the preparation equation of p w.r.t. a.

G.3.1 THEOREM: Let p and a be differential polynomials, a irreducible. Assume

$$c_{-1}\, p \;\equiv\; \sum_{\gamma=0}^{l'} c'_\gamma\, m'_\gamma(a) \mod [a]^{\rho+1}$$

is a preparation congruence of p w.r.t. a. A necessary and sufficient condition for $\mathcal{G}_a$ to be an essential component of $\{p\}$ is that $\rho \geq 0$, $l' = 0$ and $m'_0(a) = a^\rho$.

Sufficiency and necessity proofs will be partially given along with the algorithms we shall develop. We give here two examples to give a for-taste of what they are made of.

G.3.2 EXAMPLE: (for the sufficiency)

Consider the ordinary differential polynomial $p = y_0 y_1 + y_2^2$. The Rosenfeld-Gröbner decomposition is

$$\{p\} = \mathcal{G}_p \cap \{y_1\} \cap \{y_0\}$$

Trivially $\{y_0\}$ can not be an essential component since $\{y_1\} \subset \{y_0\}$.

Let thus $a = y_1$. We denote by $a_0, a_1, a_2, \ldots$ the successive derivatives of a (we introduce in fact the new indeterminate a). The preparation equation of p according to a is

$$p = \mathbf{y_0}\, a_0 + a_1^2.$$

We have on purpose put the coefficient of the lowest degree monomial in a in bold font. One should indeed keep track of what happens to it in the subsequent operations.

To be in a position to show that $\mathcal{G}_a = \{y_1\}$ is an essential component of $\{p\}$, we look for a differential polynomial in $\{p\}$ which can be factored as $a_0\, d = y_1\, d$, where $d \notin \{a_0\} = \{y_1\}$.

Consider the derivatives of p:

$$\begin{aligned} \delta p &= \mathbf{y_0}\, a_1 + y_1\, a_0 + 2\, a_1\, a_2 \\ \delta^2 p &= \mathbf{y_0}\, a_2 + 2\, y_1\, a_1 + y_2\, a_2^2 - 2 a_1\, a_3 \end{aligned}$$

We can write a system of congruences

$$\begin{pmatrix} \mathbf{y_0} & a_1 & 0 \\ y_1 & \mathbf{y_0} + 2a_2 & 0 \\ y_2 & 2y_1 + 2a_3 & \mathbf{y_0} + 2a_2 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} \equiv 0 \mod (p, \delta p, \delta^2 p) \qquad (1)$$

The determinant of this system is

$$d = \mathbf{y_0}^3 + 4y_0^2 a_2 - y_0 y_1 a_1 + 4 y_0 a_2^2 = \mathbf{y_0}^3 + r$$

where r is obviously a polynomial in $[a]$. Therefore, by Cramer's rule

$$d\, a_0 = (\mathbf{y_0}^3 + r)\, a_0 \equiv 0 \mod (p, \delta p, \delta^2 p).$$

Thus $a_0\, d \in \{p\}$ is a polynomial as the one we looked for.

Assume $\mathcal{G}_a = \{y_1\}$ is not a essential component of $\{p\}$. Then $\mathcal{G}_p$ must be included in $\{y_1\}$. Now $\mathcal{G}_p$ can not contain $a = y_1$ since y_1 is reduced w.r.t. p. Therefore $(\mathbf{y_0}^3 + r)\, a_0 \in \{p\} \subset \mathcal{G}_p$ implies that $\mathbf{y_0}^3 + r \in \mathcal{G}_p \subset \{y_1\}$. As $r \in \{y_1\}$, we are driven to the contradiction $\mathbf{y_0} \in \{y_1\}$. Thus $\mathcal{G}_a$ is an essential component.

G.3.3 EXAMPLE: (for the necessity)

Consider the differential polynomial in $\mathbb{Q}(x)\{y\}$

$$p = x^2y_1 - x^2y_0 + x + 1 + (x^2y_2 + 2xy_1 - x^2y_1 - 2xy_0 + 1)^2.$$

$\nu(x) = \frac{1}{x} \in \mathbb{Q}(x)$ is a singular zero of p: $\nu(x)$ is the general solution of $a = xy_0 - 1$ and $p \in \mathcal{G}_a = \{a\}$.

The preparation congruence of p w.r.t. a is

$$p \equiv (x-1)a + x\delta a \mod [a]^2.$$

It contains a derivative of a. To prove that $\mathcal{G}_a$ is not an essential component of p, we shall exhibit an irreducible differential polynomial b such that

$$\{p\} \subset \mathcal{G}_b \subset \mathcal{G}_a.$$

Such a b must therefore be reducible by a.

In other words, we shall exhibit another zero ν' of p in which ν is *embedded*; That b is reducible by a suggests that this zero shall depend on at least one arbitrary constant. When specializing the constant to zero we shall obtain ν.

More precisely, we shall look for zeros of p of the the type $y(x) = \nu(x) + c\,z(x)$ where c is a transcendental constant.

To find out what z shall be, we substitute in p, y by $\nu + c\,z$, where z is a new differential indeterminate.

$$\begin{aligned} p(\nu + c\,z) &= \underbrace{p(\nu)}_{=0} + c\left(\frac{\partial p}{\partial y_2}(\nu)\,z_2 + \frac{\partial p}{\partial y_1}(\nu)\,z_1 + \frac{\partial p}{\partial y_0}(\nu)\,z_0\right) \\ &\quad + c^2\ (\text{ terms of degree 2 in } z_0,\, z_1,\, z_2) + \cdots \end{aligned}$$

A necessary condition for $\nu + cz$ to be a solution is that the coefficient of c vanishes. This coefficient is : $x^2(z_1 - z_0)$. $\nu_1(x) = e^x$ is a zero of this differential polynomial . We observe that $p(\nu'(x)) = 0$.

Let $b = x^2y_1 - x^2y_0 + x + 1$. b is irreducible and $\{b\} = \mathcal{G}_b$. $\nu'(x) = \frac{1}{x} + ce^x$ is a generic zero of $\{b\}$.

b is reduced to zero by a and thus $\{b\}$ is strictly included in $\{a\}$. Likewise p is reduced to zero by b. Thus $\{p\} \subset \{b\}$. Thus $\{a\}$ can not be an essential component of $\{p\}$.

Note that the preparation equation of p w.r.t. b is

$$p = b + b^2.$$

hence $\{b\}$ is an essential component of $\{p\}$.

More generally, when the preparation congruence of p w.r.t. a involves some derivatives of a, we can construct a zero of p of the type

$$y = \nu + \nu_1 c + \nu_2 c^{\rho_2} + \nu_3 c^{\rho_3} \ldots .$$

After the first step we presented in this example to find ν_1, we proceed with a polygon to determine in $p(\nu + c(\nu_1 + z))$ the smallest power of c and its coefficient. Then, ν_2 can be taken as any zero of this coefficient. By taking successive step, we construct the above series in fractional powers of c.

G.4 Effective algorithm and examples

Assume the Rosenfeld-Gröbner algorithm returns

$$\{p\} = \bigcap_{i=1}^{r''} [A_i] : h_{A_i}^{\infty}$$

for a given differential polynomial p in $\mathcal{F}\{Y\}$. According to theorem G.1.8 and Lemma F.4, we can cast out of this decomposition the regular components whose A_i have more than one element. We obtain a decomposition

$$\{p\} = \bigcap_{i=1}^{r'} [b_i] : s_{b_i}^{\infty} = \bigcap_{i=1}^{r'} \{b_i\} : s_{b_i}, \tag{1}$$

where the b_i are regular differential polynomials and the s_{b_i} are their respective separants.

Let a_k, $1 \leq k \leq r$, be the set of all factors of the b_i in (1), and s_k their respective separants. According to Proposition G.1.7, we have a decomposition into prime differential ideals

$$\{p\} = \bigcap_{k=1}^{r} [a_k] : s_k^{\infty} = \bigcap_{k=1}^{r} \{a_k\} : s_k = \bigcap_{k=1}^{r} \mathcal{G}_{a_k} \tag{2}$$

Any $\mathcal{G}_{a_k}$ is a possible essential component of $\{p\}$. The criterion provided by the Low power theorem is readily implemented to check if it the case.

G.4.1 Example: Recall Example G.1.9 where we considered the differential polynomial

$$p = u - x u_x^2 - u_y^2.$$

The preparation congruence of p according to u trivially is $p \equiv u \mod [u]^2$. The minimal decomposition of $\{p\}$ is therefore

$$\{p\} = \mathcal{G}_p \cap [u] = \mathcal{G}_p \cap \{u\}.$$

G.4.2 EXAMPLE: Consider the ordinary differential ring $\mathbb{Q}\{y\}$. We rewrite $\delta^i y = y_i$ for all $i \in \mathbb{N}$. Consider the differential polynomial

$$p = (y_0y_2 + y_0y_1 - 2y_1^2)^2 + (y_1 - y_0 + y_0^2)(y_1 - y_0 + 2y_0^2).$$

The Rosenfeld-Gröbner decomposition is

$$\{p\} = [p] : s_p^\infty \cap [q] : s_q^\infty \cap [y_0]$$

where $q = 2y_0^4 - 3y_0^3 + 3y_0^2y_1 + y_0^2 - 2y_0y_1 + y_1^2$.

The preparation congruence of p according to $a = y_0$ is $p \equiv (a - \delta a)^2 \mod [a]^3$. $[y_0]$ is not an essential component. Conversely, the two irreducible factors of q over $\mathbb{Q}$ are

$$q_1 = y_1 - y_0 + y_0^2 \quad \text{and} \quad q_2 = y_1 - y_0 + 2y_0^2.$$

We check that both $\mathcal{G}_{q_1}$ and $\mathcal{G}_{q_2}$ are essential components of q: the preparation congruence of p according to q_1 and q_2 are respectively

$$p \equiv -y_0^2\, q_1 \mod [q_1]^2 \quad \text{and} \quad p \equiv y_0^2\, q_2 \mod [q_1]^2.$$

The minimal decomposition of $\{p\}$ is thus:

$$\{p\} = \mathcal{G}_p \ \cap \ \mathcal{G}_{q_1} \ \cap \ \mathcal{G}_{q_2}$$

In Chapter I , we construct a Duval's type algorithm that avoids factorizations, and thus spares computations of preparation equations. This algorithm works directly with the regular differential polynomials obtained in the Rosenfeld-Gröbner decomposition, splitting them, if necessary, after gcd tests. The result is a *minimal regular decomposition*. In this example $\{p\} = \mathcal{G}_p \ \cap \ \mathcal{G}_q$ is such a minimal regular decomposition.

H Computation of differential bases

We aim now at computing the differential bases of the essential components of some differential polynomial p in a differential polynomial ring $\mathcal{F}\{Y\}$. We have thus far determined these components as the general components of irreducible differential polynomials. Therefore the problem reduces to compute the differential basis of such differential ideals.

H.1 Theoretical process

Let p be an irreducible differential polynomial [1]. Consider a sequence $(u_i)_{i\in\mathbb{N}}$ of derivatives of its leader u_p that is strictly increasing according to a chosen ranking.

According to Lemma F.2.3,

$$\mathcal{G}_p \cap \mathcal{F}[\Theta_{u_i} Y] = (\Theta_{u_i} p) : s_p^\infty,$$

where $(\Theta_{u_i} p)$ is the ideal generated by $\Theta_{u_i} p$ in $\mathcal{F}[\Theta_{u_i} Y]$.

Let the radical differential ideal generated by this ideal in $\mathcal{F}\{Y\}$ be noted $\mathcal{G}_p^i$:

$$\mathcal{G}_p^i = \left\{ (\Theta_{u_i} p) : s_p^\infty \right\}.$$

In other words, if G_i is a basis of $(\Theta_{u_i} p) : s_p^\infty$ in $\mathcal{F}[\Theta_{u_i} Y]$, G_i is a differential basis of $\mathcal{G}_p^i$,

$$\mathcal{G}_p^i = \{G_i\}.$$

Obviously, for any natural integer i, $\mathcal{G}_p^i \subset \mathcal{G}_p$.

The sequence $(u_i)_{i\in\mathbb{N}}$ being strictly increasing,

$$\Theta_{u_i} p \subset \Theta_{u_{i+1}} p$$

[1] This process is also valid to compute a basis of $\{p\} : s$ for any differential polynomial.

and therefore

$$\mathcal{G}_p^0 \subset \mathcal{G}_p^1 \subset \cdots \subset \mathcal{G}_p^i \subset \cdots .$$

As $\mathcal{F}\{Y\}$ is nœtherian w.r.t to its radical differential ideal, this increasing sequence of radical differential ideals is stationary: there exists $\tau \in \mathbb{N}$ such that for any $i \geq \tau$, $\mathcal{G}_p^i = \mathcal{G}_p^\tau$. We claim that

$$\mathcal{G}_p^\tau = \mathcal{G}_p.$$

PROOF: Assume it is not the case.

There exists a non-zero differential polynomial $q \in \mathcal{G}_p \backslash \mathcal{G}_p^\tau$. Thus q is not reduced w.r.t. p; Let v be the highest derivative of u_p occurring in q. By Lemma F.2.3 $q \in (\Theta_v p) : s_p^\infty$.

Chose now $l \in \mathbb{N}$ such that u_l is greater than v: $\Theta_v p$ is a subset of $\Theta_{u_l} p$. Consequently, q is in $(\Theta_{u_l} p) : s_p^\infty$ and thus in $\mathcal{G}_p^l$. This brings out a contradiction since $\mathcal{G}_p^l \subset \mathcal{G}_p^\tau$. □

If the ranking is sequential, $\mathcal{F}[\Theta_{u_\tau} Y]$ is nœtherian w.r.t. its ideals. If $\mathcal{F}$ is computable, we may even compute a (Gröbner) basis of $(\Theta_{u_\tau} p) : s_p^\infty$ [BW93]. This summarizes into the following proposition[2].

H.1.1 PROPOSITION: Consider a computable field $\mathcal{F}$ and a sequential[3] ranking on $\mathcal{F}\{Y\}$.

Let p be an irreducible differential polynomial of $\mathcal{F}\{Y\}$, u_p its leader and s_p its separant.

Let $(u_i)_{i \in \mathbb{N}}$ be a strictly increasing sequence of derivatives of u_p.

- For any τ we can compute a finite basis G_τ of $\mathcal{G}_p^\tau (\Theta_{u_\tau} p) : s_p^\infty$.
- If τ is big enough, $\mathcal{G}_p^\tau = \mathcal{G}_p$, that is G_τ is a differential basis of $\mathcal{G}_p$.

What is left to determine is how much big τ should be. We will make clear in Section J.1 that this problem is tentamount to the problem of determining the inclusion of $\mathcal{G}_p$ in a prime differential ideal given by its characteristic set.

H.2 A bound to the number of derivations?

Consider an orderly[4] ranking on $\mathcal{F}\{Y\}$. Such a ranking is sequential.

[2] compare it with the theoretical decomposition process proposed by Ritt ([Rit66, V.28] or [Kol73, IV.9]).

[3] recall from Section F.1 that a ranking is sequential if $\Theta_v Y$ is finite for any derivative v of $\mathcal{F}\{Y\}$.

[4] Recall from Section F.1 that a ranking on $\mathcal{F}\{y_1, \ldots, y_n\}$ is orderly if ord $\theta >$ ord $\theta' \Rightarrow \theta y_i > \theta' y_j$, for $\theta, \theta' \in \Theta$ and for any i, j, $1 \leq i, j \leq n$.

Let p be an irreducible differential polynomial . We shall consider the following strictly increasing sequence of derivatives of u_p: for $i \in \mathbb{N}$, u_i will be the highest derivative of u_p of order i and Θ_{u_i} is shorten in Θ_i.

We look for the bound of order of derivations to be made to be in a position to compute the differential basis of the general component of an irreducible differential polynomial p.

For a first order differential polynomial such a bound can be read directly on the differential polynomial p [Coh76] and the process is completed (see Section N.1). We shall see that a similar bound can be found for higher order ordinary and partial differential polynomials. But do we have as strong a conclusion as in the simplest case?

The answer to that question will be found in Theorem H.3.1. But before, to bring out the bound, we shall study Levi's lemma. This lemma relies on the study of the monomials of a differential ideal $[z^\rho]$ of a differential ring $\mathcal{R}\{z\}$[5].

The monomials of $[z^\rho]$

The criterion for a monomial in z to belong to $[z^\rho]$ is the core of the proof of Levi's lemma and requires a number of pages to be shown. It starts with the simple observation:

H.2.1 LEMMA: Let a and b be elements of a differential ring. Let θ be a derivative operator of order ρ. Then $a^{\rho+1}\,\theta b$ can be written as a linear combination of $(\theta'(ab))_{\theta'|\theta}$ with homogeneous coefficient of degree ρ in a and its derivatives.

PROOF: The result is trivial for $\rho = 0$. Assume this is true for all integer strictly less than a $\rho > 0$. A derivative operator of order ρ can be written as $\theta = \delta\theta_1$ where $\delta \in \Delta$ and θ_1 is a derivation operator of order $\rho - 1$. Now

$$a^{\rho+1}\,\theta b = a\,\delta(a^\rho\,\theta_1 b) - \rho\,(a^\rho\theta_1 b)\,\delta a.$$

The inductive hypothesis leads thus to the desired result. □

H.2.2 DEFINITION: For any non zero natural integers μ, κ, ρ we define two functions ϵ and ω as follow:

- $\epsilon(\mu, \kappa, 1) = 1$
  and for $\rho > 1$

$$\epsilon(\mu, \kappa, \rho) = (\rho - 1)\frac{(\mu+1)\ldots(\mu+r)}{r!} = (\rho - 1)\begin{pmatrix} \mu + r \\ r \end{pmatrix}$$

[5] We want to point out that $\mathcal{R}$ will be often interpreted as $\mathcal{R} = \mathcal{F}\{Y\}$.

where r is an integer greater or equal to $\dfrac{\kappa(\mu+1)}{\mu}$.

- $\omega(\mu,\kappa,\rho) = \kappa\,\epsilon(\mu,\kappa,\rho)$

Recall also from Section E.2 the definition of the degree and the weight of a differential monomial.

H.2.3 LEMMA: Consider a differential polynomial ring $\mathcal{R}\{z\}$ endowed with μ derivation operators.

Given $\kappa,\ \rho\ \in \mathbb{N}$, any differential monomial m in z of degree equal to $\epsilon(\mu,\kappa,\rho)$ and weight lower or equal to $\omega(\mu,\kappa,\rho)$ is in $[z^\rho]$

This was proved by H. Levy in [Lev45].

In the ordinary differential case ($\mu = 1$), we can in fact take

$$\epsilon(1,\kappa,\rho) = \kappa(\rho-1)+1 \quad \text{and} \quad \omega(1,\kappa,\rho) = (\kappa-1)\,\epsilon(1,\kappa,\rho).$$

This is given in [Lev42], where was first given an algebraic proof for the sufficiency of the Low power theorem.

Another generalized pair of functions ϵ and ω is brought by Kolchin [Kol73, I.7] in a comparatively simpler way. They are nonetheless bigger, which will be annoying in the use we shall do of these functions.

Levi's lemma

H.2.4 LEMMA: Let q be a differential polynomial in $\mathcal{R}\{u_0,\ldots,u_l,\ z\}$ of the form

$$q = u_0 z^\rho + \sum_{\gamma=1}^{l} u_\gamma m_\gamma$$

where $\rho \in \mathbb{N}^*$ and $m_1,\ldots,m_l$ are differential monomials in z of total degree strictly greater than ρ. If κ is the maximum weight of the m_γ, there exists $d \in \mathbb{N}^*$ such that for $\epsilon = \epsilon(\mu,\kappa,\rho)$ and $\omega = \omega(\mu,\kappa,\rho)$

$$z^\epsilon(u_0^d + r) \in (\Theta_\omega q)$$

PROOF: (taken from [Kol73, IV.11])

Consider a monomial g of $\mathcal{R}\{z\}$ of degree ϵ and weight less than ω. According to lemma H.2.3, $g \in [z^\rho]$.

As $\mathcal{R}\{z\}$ is a graded algebra according to the degree and according to the weight, we can write:

$$g = \sum_{\text{ord } \theta \leq \text{wt } g} a_\theta \, \theta(z^\rho) \tag{1}$$

where a_θ is homogeneous of degree $\deg g - \rho$ and isobaric of weight wt $g -$ ord θ.

According to lemma H.2.1, we may write

$$u_0^{1+\text{ord}\theta} \, \theta(z^\rho) = \sum_{\theta_1 | \theta} b_\theta^{\theta_1} \, \theta_1(u_0 z^\rho).$$

where $b_\theta^{\theta_1} \in \mathcal{R}'\{z, u_0\}$ is homogeneous of degree ord θ. Therefore

$$\begin{aligned} u_0^{1+\omega} \, g &= \textstyle\sum_{\text{ord } \theta \leq \text{wt} g} u_0^{\omega - \text{ord } \theta} \, a_\theta \, u_0^{\text{ord } \theta + 1} \, \theta(z^\rho) \\ &= \textstyle\sum_{\text{ord } \theta \leq \text{wt} g} u_0^{\omega - \text{ord } \theta} \, a_\theta \sum_{\theta_1 | \theta} b_\theta^{\theta_1} \, \underline{\theta_1(u_0 z^\rho)} \end{aligned}$$

Let us rewrite $\theta_1(u_0 z^\rho)$ with Leibniz rule:

$$\theta_1(u_0 z^\rho) \equiv - \sum_{\gamma=1}^{l} \sum_{\theta_2 \theta_3 = \theta_1} c_{\theta_2}^{\theta_3} \, \theta_2(u_\gamma) \, \theta_3(m_\gamma) \mod (\theta_1 q)$$

where the $c_{\theta_2}^{\theta_3}$ are integers. We thus have

$$u_0^{1+\omega} g \equiv - \sum_{\substack{\gamma = 1 \ldots l, \\ \text{ord } \theta \leq \text{wt} g \\ \theta_1 | \theta, \, \theta_2 \theta_3 = \theta_1}} u_0^{\omega - \text{ord } \theta} \, a_\theta \, b_\theta^{\theta_1} \, c_{\theta_2}^{\theta_3} \, \theta_2(u_\gamma) \, \theta_3(m_\gamma) \mod (\Theta_\omega q) \tag{2}$$

where only the products $a_\theta \, \theta_3(m_\gamma)$ involves derivatives of z.

Furthermore the polynomials $a_\theta \, \theta_3(m_\gamma)$ are homogeneous of degree

$$\deg a_\theta + \deg m_\gamma \geq \deg g - \rho + \rho + 1 \geq \epsilon + 1$$

and isobaric of weight

$$\text{wt } a_\theta + \text{wt } m_\gamma + \text{ord } \theta_3 \leq \text{wt } g - \text{ord } \theta + \kappa + \text{ord } \theta_3 \leq \omega + \kappa$$

since ord $\theta_3 -$ ord $\theta \leq 0$.

Consider f a monomial of $a_\theta \, \theta_3(m_\gamma)$. We claim it is a multiple of a monomial of $\mathcal{R}\{z\}$ of weight less than or equal to ω and degree ϵ.

Indeed either every derivatives of z in f is of order less than κ and any product of ϵ of them will do, or, there is one of the derivatives the order of which is greater than κ and we take the product of the others.

Enumerate the monomials of $\mathcal{R}\{z\}$ of degree ϵ and weight less than or equal to ω: $g_1, \ldots, g_h$. From (2), for any $1 \leq i \leq h$

$$u_0^{1+\omega} g_i \equiv \sum_{j=1}^{h} v_{ij}\, g_j \mod (\Theta_\omega q) \tag{3}$$

where v_{ij} are differential polynomials in $[z]$.

We eventually have a linear system of congruences:

$$\begin{pmatrix} u_o^{1+\omega} - v_{11} & -v_{12} & \cdots & \cdots & -v_{1h} \\ -v_{21} & u_o^{1+\omega} - v_{22} & \cdots & \cdots & -v_{2h} \\ \vdots & \ddots & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & \vdots \\ -v_{h1} & -v_{h2} & \cdots & \cdots & u_o^{1+\omega} - v_{hh} \end{pmatrix} \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ \vdots \\ \vdots \\ g_h \end{pmatrix} \equiv 0 \mod (\Theta_\omega q)$$

The determinant of this system is a polynomial $u_0^d + r$ where $d = h(1+\omega)$, $r \in [z]$ and $\deg_{u_0} r < d$.

z^ϵ being one of the g_i, by Cramer's rule.

$$z^\epsilon (u_0^d + r) \equiv 0 \mod (\Theta_\omega q).$$

□

Identifying the hypothesis of the preceding lemma with a preparation equation of some differential polynomial p w.r.t. an irreducible differential polynomial a, we obtain the following corollary:

H.2.5 COROLLARY: Assume that a preparation equation of some differential polynomial p w.r.t. an irreducible differential polynomial a in $\mathcal{F}\{Y\}$ is

$$c_{-1}\, p = c_0\, a^\rho + \sum_{\gamma=1}^{l} c_\gamma\, m_\gamma(a)$$

where the degrees of the monomials m_γ, $1 \leq \gamma \leq l$, are strictly greater than ρ.

If κ is the maximum weight of the monomials m_γ, there exists an integer d and a differential polynomial $r \in [a]$ such that for $\epsilon = \epsilon(\mu, \kappa, \rho)$ and $\omega = \omega(\mu, \kappa, \rho)$

$$a^\epsilon\, (c_0^d + r) \in (\Theta_\omega p)$$

PROOF: It suffices to substitute a to z and c_γ to u_γ, $0 \leq \gamma \leq l$, to assert that, according to Lemma H.2, there exists $d \in \mathbb{N}^*$ and $r \in [a]$ such that

$$a^\epsilon\, (c_0^d + r) \in (\Theta_\omega (c_{-1} p)) \subset (\Theta_\omega p).$$

□

Note that this shows the sufficiency condition of the Low power theorem.

Assume the preparation equation of p w.r.t. the irreducible differential polynomial a satisfies the hypotheses of the previous corollary.

Assume then for contradiction that $\mathcal{G}_a$ is not an essential component of $\{p\}$. There exists a prime differential ideal P which is strictly contained in $\mathcal{G}_a$ and such that $\{p\} \subset P$.

P can not contain a. Otherwise it would contain an essential component of a, contradicting the fact that $P \subset \mathcal{G}_a$ since $\mathcal{G}_a$ certainly is an essential component of $\{a\}$.

Hence

$$a^\epsilon(c_0^d + r) \in \{p\} \subset P$$

and thus

$$c_0^d + r \in P \subset \mathcal{G}_a.$$

As $r \in [a] \subset \mathcal{G}_a$, this would imply that $c_0 \in \mathcal{G}_a$. This is in contradiction with the definition of a preparation equation.

The same argument is used to show the somewhat generalized result of next section.

H.3 Another way against the Ritt problem

Recall from Section H.1 that for an integer k and an irreducible differential polynomial p we note

$$\mathcal{G}_p^k \;=\; \left\{ (\Theta_k p) : s_p^\infty \right\}$$

H.3.1 THEOREM: Assume that the minimal decomposition of a given irreducible differential polynomial p is

$$\{p\} = \bigcap_{i=0}^{r} \mathcal{G}_{a_i}, \qquad \text{where } a_0 = p.$$

The preparation congruences of p according to each a_i, $1 \leq i \leq r$, can be written

$$s_i^{\alpha_i}\, p \;\equiv\; c_i\, a_i^{\rho_i} \mod [a_i]^{\rho_i+1}, \;\; \rho_i \geq 1.$$

Let κ_i be the maximum weight of the monomials in the underlying preparation equations and let

$$\omega = \max_{i=1}^{r} \omega(\mu, \rho_i, \kappa_i).$$

Then

- $\mathcal{G}_p^\omega$ is contained in no other essential component of $\{p\}$ than $\mathcal{G}_p$.
- $\mathcal{G}_p$ is an essential component of $\mathcal{G}_p^\omega$.
- If P is another essential component of $\mathcal{G}_p^\omega$, there exists i, $1 \leq i \leq r$ such that $\{\mathcal{G}_{a_i}, c_i\}$ is included in P.

PROOF:

- According to Corollary H.2.5 and the preparation equation of p w.r.t. a_i, $i \geq 1$, we conclude that there exists an integer d_i and a differential polynomial r_i which lies in $[a_i]$ such that

$$a^{\epsilon_i}\,(c_i^d + r_i) \in (\Theta_{\omega_i} p) \subset (\Theta_\omega p) \subset (\Theta_\omega p) : s_p^\infty,$$

  where $\omega_i = \omega(\mu, \rho_i, \kappa_i)$ and $\epsilon_i = \epsilon(\mu, \rho_i, \kappa_i)$.

  We want to show that $(c_i^d + r_i)$ is in $\mathcal{G}_p^\omega$ but not in $\mathcal{G}_{a_i}$.

  First, since $\mathcal{G}_{a_i}$ is an essential component, $a_i \notin \mathcal{G}_p$ and consequently $a_i \notin (\Theta_\omega p) : s^\infty$. In virtue of Lemma F.2.3 $(\Theta_\omega p) : s^\infty$ is prime. Therefore

$$(c_i^d + r_i) \in (\Theta_\omega p) : s$$

  and thus

$$(c_i^{d_i} + r_i) \in \mathcal{G}_p^\omega.$$

  Now, $r_i \in [a_i] \subset \mathcal{G}_{a_i}$ but $c_i \notin \mathcal{G}_{a_i}$. Consequently $(c_i^{d_i} + r_i) \notin \mathcal{G}_{a_i}$. Thus, for $i = 1, \ldots, r$, $\mathcal{G}_p^\omega$ contains an element which does not belong to $\mathcal{G}_{a_i}$.

- According to property E.4.6

$$\mathcal{G}_p^\omega = \mathcal{G}_p^\omega : s \cap \{\mathcal{G}_p^\omega, s\} \quad \text{and} \quad \mathcal{G}_p^\omega : s = \mathcal{G}_p.$$

  Any component of $\{\mathcal{G}_p^\omega, s\}$ contains a non-zero differential polynomial reduced w.r.t. p and therefore can not be contained in $\mathcal{G}_p$: $\mathcal{G}_p$ is an essential component of $\mathcal{G}_p^\omega$.

  As $\{p\} \subset \mathcal{G}_p^\omega$, any essential component P of $\mathcal{G}_p^\omega$ contains an essential component of $\{p\}$, say $\mathcal{G}_{a_i}$. If $i \geq 1$, as $c_i^{d_i} + r_i \in \mathcal{G}_p^\omega \subset P$ and $r_i \in [a_i] \subset \mathcal{G}_{a_i} \subset P$, P contains c_i.

□

In the simplest case where p is a first order ordinary differential polynomial, the singular components are algebraic: $a_1, \ldots, a_r$ are of order zero. Therefore the corresponding $\{\mathcal{G}_{a_i}, c_i\}$ contain an element in the ground field $\mathcal{F}$. Consequently $\mathcal{G}_p^\omega$ has no other component than $\mathcal{G}_p$. This means that a basis of $(\Theta_\omega p) : s_p^\infty$ is a differential basis of the general component $\mathcal{G}_p$ of p. This unfortunately does not generalize as is set forth in Example H.3.3.

H.3.2 EXAMPLE: Consider the differential polynomial

$$p = y_0 y_1 + y_2^2 \in \mathbb{Q}\{y\}.$$

We already looked at this differential polynomial in the first example of Section D.2. The Rosenfeld-Gröbner algorithm returns $\{p\} = \mathcal{G}_p \cap [y_1] \cap [y_0]$. Trivially $[y_1]$ is included in $[y_0]$, which therefore is not an essential component.

Besides a preparation equation of p according to $a = y_1$ is:

$$p = y_0 a + (\delta a)^2.$$

In virtue of the Low power theorem $[y_1]$ is an essential component and the ω of Theorem H.3.1 is $\omega = 1$.

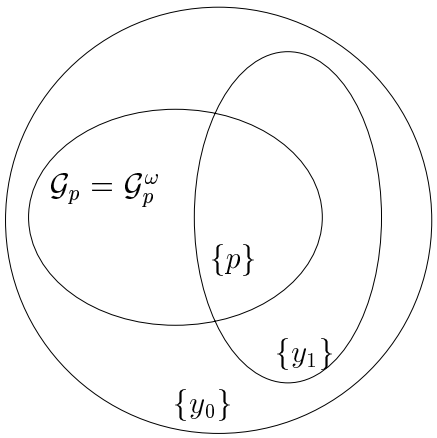
Some computations lead to

$$\mathcal{G}_p^\omega = \{2\, y_0\, y_3 - y_1\, y_2 + y_0^2,\ y_2\, y_3 + y_0\, y_2 + y_1^2,\ p\}.$$

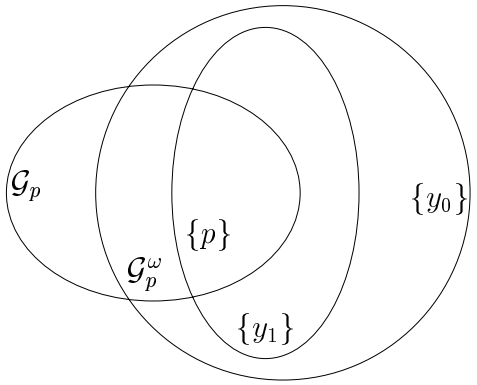
The Rosenfeld-Gröbner decomposition of $\mathcal{G}_p^\omega$ consists of two regular components:

$$\mathcal{G}_p^1 = \mathcal{G}_p \cap \{y_0\}. \tag{1}$$

But fortunately $\mathcal{G}_p \subset \{y_0\}$ [Kol73, IV.15, theorem 7] and therefore $\mathcal{G}_p^\omega = \mathcal{G}_p$. We thus managed to compute a differential basis of the general component of p.



$p = y_0 y_1 + y_2^2$



$q = y_0 y_1 + y_2^3$

H.3.3 EXAMPLE: Consider now the very similar differential polynomial we have also encountered in Section D.2.

$$q = y_0 y_1 + y_2^3.$$

As previously, $\{q\} = \mathcal{G}_q \cap \{y_1\}$ is the minimal decomposition and the ω of Theorem H.3.1 is $\omega = 2$.

The result of the computation is quite cumbersome, but the Rosenfeld-Gröbner decomposition of $\mathcal{G}_q^\omega$ is just the same as (1). Unfortunately now $\mathcal{G}_q$ is not included in $\{y_0\}$ [Lev42, §38]. Thus $\mathcal{G}_p^\omega \neq \mathcal{G}_p$.

Deciding whether the general component of differential polynomial contains the general component of another has been named after J.Ritt. This latter phrased this inclusion problem when investigating the analytic relation of the singular solutions to the general solution of ordinary differential equation in one differential indeterminate, as was explained in the first part of this memoir. The problem is to determine which essential components of a differential polynomial are contained in a non-essential singular component of the differential polynomial.

When considering more than one indeterminate or partial differential equations, a singular component that is not essential can have a characteristic set with more than one differential polynomial. The Ritt problem is then to determine if a prime differential ideal given by one of its characteristic set contains the general component of an irreducible differential polynomial.

This problem obviously extends to the problem of inclusion of two prime differential ideals given by their characteristic sets.

Here follow two trivial consequences of Lemma H.3.1 which provide sufficient conditions for $\mathcal{G}_p^\omega$ to be equal to $\mathcal{G}_p$. When this happen, a basis of $(\Theta_\omega p) : s^\infty$ is a differential basis of the general component of p.

H.3.4 Proposition: Consider a differential polynomial p in a differential polynomial ring $\mathcal{F}\{Y\}$. If for any essential component $\mathcal{G}_a$ of $\{p\}$ the preparation congruence of p according to a can be written $s_a\, p \equiv c\, a^\rho \mod [a]^{\rho+1}$, where c is in the ground field $\mathcal{F}$, then $\mathcal{G}_p^\omega = \mathcal{G}_p$.

H.3.5 Proposition: If a prime or regular decomposition of $\mathcal{G}_p^\omega$ has only one component, it must be $\mathcal{G}_p$ and thus $\mathcal{G}_p^\omega = \mathcal{G}_p$.

H.3.6 Example: Consider

$$p = (1 + x^2)\, y_2^2 - (2xy_1 + \frac{1}{2}x^2)\, y_2 + y_1^2 + xy_1 - y_0.$$

The Rosenfeld-Gröbner decomposition is

$$\{p\} = [p] : s_p^\infty \cap [q] : s_q^\infty = \mathcal{G}_p \cap \mathcal{G}_q \tag{2}$$

where q is the irreducible differential polynomial

$$q = y_1^2 + (x + \frac{1}{2}x^3)\, y_1 - (x^2 - 1)\, y_0 - \frac{1}{16}x^4.$$

The preparation equation of p w.r.t. q is:

$$\begin{aligned}\left(64\,(4\,y_1^2+x^3+2x)^2\right)\,p &= -4\,(x^4+4\,x^2+16\,y_0)\,q \\ &\quad +4\,q^2+(1+x^2)\,(\delta\,q)^2-4\,x\,q\,\delta q.\end{aligned}$$

Therefore (2) is a minimal decomposition of $\{p\}$. The ω of Theorem H.3.1 is $\omega = 1$.

We now look for the differential bases of the essential components. Computing a Gröbner basis of $(p, \delta p) : s_p^\infty$ gives a differential basis of $\mathcal{G}_p^\omega$,

$$\mathcal{G}_p^\omega = \{y_3, p\}.$$

The Rosenfeld-Gröbner decomposition of $\{y_3, p\}$ has only one component. Thus by Lemma H.3.5, $\mathcal{G}_p = \mathcal{G}_p^\omega = \{y_3, p\}$.

Note the integration heuristic there obtained: as $y_3 \in \mathcal{G}_p$, the general solution is a polynomial of degree two. Replacing such a polynomial with unknown coefficients in p, we find out that it shall be

$$\bar{y}(x) = c\,x^2 + b\,x + 4\,c^2 + b^2, \quad \text{where } c \text{ and } b \text{ are arbitrary constants.}$$

We want now a differential basis of $\mathcal{G}_q$. To this aim, we proceed just as before.

The Rosenfeld-Gröbner algorithm returns

$$\{q\} = [q] : s_q^\infty \cap [a] : s_a^\infty = \mathcal{G}_q \cap \mathcal{G}_a,$$

where a is the irreducible differential polynomial

$$a = 16y_0 + x^4 + 4x^2.$$

The preparation congruence of q according to a is

$$q \equiv -16(x^2+1)\,a \mod [a]^2$$

and $\omega = 1$. By Proposition H.3.4

$$\mathcal{G}_q = \mathcal{G}_q^\omega = \{4(x^2+1)\,y_2 - 4xy_1 - x^2, q\}.$$

The general solution of q satisfies a linear differential equation of second order. Such equations are widely studied in the computer algebra community. We are thus in a position to thoroughly describe the behavior of the general solution of q.

In Chapter J we shall come back to the Ritt problem and speak about the criteria which were found to decide of it.

I Minimal regular decomposition

The purpose of this section is to avoid the factorization appearing in the algorithm of Section G.4. We shall thus work directly on the regular differential polynomials in the result of the Rosenfeld-Gröbner algorithm.

On the one hand, one could argue that factorization is efficient enough not to be supplanted. But on the other hand, an algorithm working with regular differential polynomials will spare the computation of preparation equations.

As we shall talk about it in Chapter J , the preparation equation of p according to an irreducible differential polynomial a, as well as Levi's lemma, can be generalized when replacing a by the characteristic set of a prime differential ideal. If we wish to implement, in the future, such preparation equations, we should contemplate working with characteristic sets of regular differential ideals. A necessary condition to work it out is that it already works for regular differential polynomials.

Furthermore, in the previous chapter we had the occasion to go into the sufficiency proof of the Low Power theorem. This section will provide natural occasion to go furthermore into the proof of the necessity.

I.1 Definition

Consider a differential polynomial p. We will call a_0 the regular part of p

$$a_0 = \frac{p}{\gcd(p,\, s_p)}$$

and we will assume that it is different from unity: $a_0 \neq 1$[1].

Considering Theorem G.1.8 and Theorem F.4.1, we may assume without loss

[1] if it was not the case, we just have to forget about it in the following propositions and algorithms

generality that the Rosenfeld-Gröbner decomposition of $\{p\}$ is

$$\{p\} = \bigcap_{i=0}^{r} [a_i] : s_{a_i}^{\infty}$$

where the a_i are regular differential polynomials (Definition G.1.5) and a_0 is the regular part of p.

If $a_i = \prod_{j=1}^{r_i} b_{ij}$ is a factorization of a_i into irreducible polynomials, by Proposition G.1.7 the minimal decomposition of $\{a_i\} : s_{a_i}$ is

$$[a_i] : s_{a_i}^{\infty} = \{a_i\} : s_{a_i} = \bigcap_{j=1}^{r_i} \{b_{ij}\} : s_{ij},$$

where s_{ij} is the separant of b_{ij}.

Furthermore, all the essential components of $\{a_0\} : s_{a_0}$ are essential components of $\{p\}$. Indeed,

$$\{p\} = \{p\} : s_p \cap \{p, s_p\} = \{a_0\} : s_{a_0} \cap \{p, s_p\}.$$

and therefore, the other components of $\{p\}$ contain a differential polynomial free of u_p and thus can not be contain in any essential component of $\{a_0\} : s_{a_0}$.

We could say that $\{a_0\} : s_{a_0}$ is an *essential regular component* of $\{p\}$.

I.1.1 DEFINITION: A regular decomposition of $\{p\}$, $\{p\} = \bigcap_{i=0}^{r} [a_i] : s_i^{\infty}$, is minimal if the a_i are pairwise relatively prime and all the essential components of the $\{a_i\} : s_i^{\infty}$ are essential for $\{p\}$.

The condition that the a_i are relatively prime is necessary if we do not want an essential component to be repeated twice.

Preparation equation

It is no problem to extend the definition of the preparation equation and congruence to regular differential polynomial.

I.1.2 DEFINITION: Let p and a be differential polynomials, a regular. A preparation equation of p w.r.t. a is an equation

$$c_{-1}\, p = \sum_{\gamma=0}^{l} c_\gamma m_\gamma(a) \tag{1}$$

where $m_0, \ldots, m_l$ are distinct differential monomials, $c_0, \ldots, c_l$ are differential polynomials not contained in $\{a\} : s_a$ and c_{-1} does not devide zero modulo $\{a\} : {s_a}^2$.

Let ρ be the minimal degree of the monomials m_γ in 1. If we denote the differential monomials m_γ of degree ρ by $m'_1, \ldots, m'_l$, then (1) yields a *preparation congruence* of p w.r.t. a

$$c_{-1}\, p \;\equiv\; \sum_{\gamma=0}^{l'} c'_\gamma\, m'_\gamma(a) \mod [a]^{\rho+1} \tag{2}$$

Furthermore, the algorithm to compute such a preparation equation is just the same. Indeed,

- just as for irreducible differential polynomials, c partially reduced w.r.t. a belongs to $\{a\} : s_a$ if and only iff it is divisible by a (Proposition G.1.6).
- s_a belongs to no essential component of $\{a\} : s_a$.

In the two next sections we are going to see how we can determine which factors of a regular differential polynomial a define an essential component of $\{p\}$ and which do not. This determination can be made on the preparation equation of p w.r.t. a. The two criteria exposed are proved respectively in a similar way than the sufficiency and the necessity of the Low power theorem. They lead to a *lazy* algorithm for computing a minimal regular decomposition.

I.2 Sufficiency

I.2.1 THEOREM: Let p be a differential polynomial and a a regular differential polynomial in $\mathcal{F}\{Y\}$. Assume a preparation congruence of p according to a is

$$c_{-1}\, p \;\equiv\; c\, a^\rho \mod [a]^{\rho+1},$$

where c is partially reduced w.r.t. a.

Let $a'' = \gcd(a, c)$ and $a' = \dfrac{a}{a''}$. Then any essential component of $\{a'\} : s_{a'}$ is essential for p. In other words, $\{a'\} : s_{a'}$ is an essential regular component of p.

PROOF: Let b be an irreducible factor of a.

As c is partially reduced w.r.t. b, recall from Proposition G.1.3 that c belongs $\mathcal{G}_b$ if and only if it is divisible by b. We shall show that if $\mathcal{G}_b$ does not contain c it is

[2] that means it does not belong to any essential component of $\{a\} : s_a$

an essential component of $\{p\}$. This will therefore be the case for any irreducible factors of a'.

Assume $\mathcal{G}_b$ is not an essential component of $\{p\}$. There thus exists an essential component P of $\{p\}$ which is strictly included in $\mathcal{G}_b$. Such a P can not contain a, since otherwise it would contain an essential component of a.

According to Levi's lemma (Corollary H.2.5), there exists $\epsilon, d \in \mathbb{N}^*$ and $r \in [a]$ such that

$$a^\epsilon (c^d + r) \in \{p\} \subset P.$$

P being prime, $c^d + r \in P \subset \mathcal{G}_b$.

As we have $r \in [a] \subset \mathcal{G}_b$, we are brought to the conclusion that $c \in \mathcal{G}_b$. □

I.3 Necessity

The polygon process we mentioned in Example G.3.3 can be encapsulated in the Leading coefficient theorem, the most generalized version of which is due to A.Hillman [Hil52], [HM62] (see also [Kol73, IV.10]).

I.3.1 THEOREM: Let p and q be two nonzero differential polynomials of $\mathcal{F}\{Y\}$ such that $q \in \{p\}$. Let $\bar{p}$ and $\bar{q}$ be respectively the sum of the terms of lowest degree in p and q. Then $\bar{q} \in \{\bar{p}\}$.

With this in mind, we show that if the preparation congruence of p w.r.t. a regular differential polynomial a involves proper derivatives of a then, at least one of the essential component of $\{a\} : s_a$ is not essential for $\{p\}$.

I.3.2 THEOREM: Let p be a nonzero differential polynomial of $\mathcal{F}\{Y\}$ and a a regular differential polynomial. Consider a preparation congruence of p w.r.t. a

$$s_a^\alpha \, p \;\equiv\; c_0 \, a^\rho + \sum_{\gamma=1}^{l} c_\gamma \, m_\gamma(a) \mod [a]^{\rho+1}$$

where the c_γ, $0 \leq \gamma \leq r$, are partially reduced w.r.t. a; c_0 may be zero, but we assume that none of the $c_1, \ldots, c_l$ is.

Let

$$a' = \gcd(a, c_1, \ldots, c_l) \quad \text{and} \quad a'' = \frac{a}{a'}.$$

Then, no essential component of $\{a''\} : s_{a''}$ is an essential component of p.

PROOF: (similar to [Kol73, IV.15])

Let $b_0, \ldots, b_\beta$ be the irreducible factors of a. Let $s_0, \ldots, s_\beta$ be their respective separants:

$$s_a = \sum_{j=0}^{\beta} s_j \prod_{i \neq j} b_i$$

We can assume that b_0 is an irreducible factor of a''.

Consider all the essential components of $\{p\}$ which are contained in $\mathcal{G}_{b_0}$. They are the general components of some differential polynomial $r_1, \ldots, r_\kappa$.

If $\mathcal{G}_{b_0}$ were an essential component, κ would be equal to one and r_1 would be equal to b_0.

We are in fact going to show that it can not be so because one of the r_i involves a proper derivative of u_a and thus $\mathcal{G}_{r_i}$ is strictly contained in $\mathcal{G}_b$.

Let r_0 be a differential polynomial which does not belong to $\mathcal{G}_{b_0}$ but which belongs to all the components of $\{p\}$ not contained in $\mathcal{G}_{b_0}$. Thus $r_0\, r_1 \ldots r_\kappa \in \{p\}$.

Let ν be a generic zero of $\mathcal{G}_{b_0}$ in an extension field $\mathcal{F}'$ of $\mathcal{F}$. A differential polynomial q vanishes on ν iff it belongs to $\mathcal{G}_{b_0}$. Thus

$$s_a(\nu) = s_0(\nu) \prod_{i \neq j} b_i(\nu) \neq 0.$$

For a differential polynomial q in $\mathcal{F}\{Y\}$ we note $\bar{q}$ the sum of the terms of lowest degree in $q(\nu + y)$. Note that $\overline{q\, r} = \bar{q}\, \bar{r}$, for any $q, r \in \mathcal{F}\{Y\}$. As

$$a(\nu + y) = s_a(\nu)\, u_a + \text{ first degree terms of lower rank } + \text{ higher degree terms .}$$

$\bar{a}$ has degree one and u_a as leader.

Now, if

$$q = c_0\, a^\rho + \sum_{\gamma=1}^{l} c_\gamma\, m_\gamma(a)$$

then

$$\bar{q} = c_0(\nu)\, \bar{a}^\rho + \sum_{\gamma=1}^{l} c_\gamma(\nu)\, m_\gamma(\bar{a}),$$

where $c_\gamma(\nu) \neq 0$ for at least one γ, $1 \leq \gamma \leq l$. Among the derivatives of $\bar{a}$ effectively present in the monomials of the right hand side, let $\theta\bar{a}$ be such that θu_a has the highest rank. Let $\bar{q}_0$ be an irreducible factor of $\bar{q}$ which contains $\theta\bar{a}$.

We are now in a position to conclude thanks to the Leading coefficient theorem:

$$r_0\, r_1 \ldots r_\kappa \in \{p\} \;\Rightarrow\; \bar{r}_0\, \bar{r}_1 \ldots \bar{r}_\kappa \in \{\bar{p}\},$$

where $\bar{r_0} = r_0(\nu) \in \mathcal{F}'$ and for $i \geq 1$, $\bar{r_i}$ is of positive degree.

As

$$s_a^{\alpha}\, p \;\equiv\; q \mod [a]^{\rho+1},$$

$\bar{s_a}^{\alpha}\, \bar{p} = \bar{q}$, where $\bar{s_a} = s_a(\nu)$ is a nonzero element of $\mathcal{F}'$. Thus

$$\{\bar{p}\} = \{\bar{q}\} \subset \mathcal{G}_{\bar{q}_0}.$$

Consequently, $\mathcal{G}_{\bar{q}_0}$ being a prime differential ideal, there exists a i, $1 \leq i \leq \kappa$ such that $r_i \in \mathcal{G}_{\bar{q}_0}$. Therefore, r_i can not be reduced w.r.t. $\bar{q}_0$: it must contain a derivative of θu_a, and therefore a proper derivative of u_a. That is what we looked for. □

I.4 Algorithm

We collect the results presented above in an algorithm to determine a minimal regular decomposition of a differential polynomial p:

$$\{p\} = \bigcap_{i=0}^{r} \{a_i\} : s_{a_i}.$$

where a_0 is the regular part of p.

We call **single-dp** a procedure which takes as entry a Rosenfeld-Gröbner decomposition, cast out the regular components the characteristic sets of which contain more than one differential polynomial, and returns the list of the differential polynomials which are the characteristic sets of the other regular components.

Then the complete algorithm to compute a minimal regular decomposition of $\{p\}$ can be written:

I.4.1 Algorithm: **Minimal Regular Decomposition**

Input: p a differential polynomial in $\mathcal{F}\{Y\}$

Output: $MiniReg = a_0, a_1, \ldots, a_r$ such that $p = \bigcap_{i=0}^{r} \{a_i\} : s_{a_i}$ is a minimal regular decomposition of p.

$RG :=$ **single-dp** (**Rosenfeld-Gröbner** $(\{p\}\ ,\ \mathcal{F}\{Y\}\ )$);

#make the RG[i] relatively prime

For $1 < i < j \leq$nops(RG) do

if leader $(RG[i],\ \mathcal{F}\{Y\})$ = leader $(RG[j],\ \mathcal{F}\{Y\})$

then $RG[i] := \dfrac{RG[i]}{\gcd(RG[i], RG[j])}$

$MiniReg := RG[1]$; *# the regular part of p*

For each differential polynomial a in RG, $RG[1]$ excepted, do

$MiniReg := MiniReg$, **Essential-Part** $(p,\ a)$;

od;

end;

I.4.2 ALGORITHM: **Essential-part**

INPUT: p a differential polynomial and a a regular differential polynomial.

OUTPUT: $B = b_1, \ldots, b_r$ such that

- b_i divides a,
- $\{b_i\} : s_{b_i}$ is an essential regular component of $\{p\}$

If $a = 1$ then return $\emptyset$

$prep :=$ **Preparation-Congruence**$(p,\ a)$;

if $prep = c\, a^\rho$

then

$a'' := \gcd(c, a)$;

$a' := \frac{a}{a''}$;

$B :=\ a'$, **Essential-Part**$(p,\ a'')$.

else *# $prep = [c_0 a^\rho +] \sum_{\gamma=1}^{l} c_\gamma m_\gamma(a)$*

$a' := \gcd(c_1, \ldots, c_l, a)$;

$a'' := \dfrac{a}{a'}$.

$B :=$ **Essential-Part**$(\ p,\ a')$.

fi;

end;

I.4.3 EXAMPLE: Recall Example G.4.2 where we considered the differential polynomial

$$p = (y_0 y_2 + y_0 y_1 - 2y_1^2)^2 + (y_1 - y_0 + y_0^2)(y_1 - y_0 + 2y_0^2).$$

A preparation congruence of p according to

$$q = 2y_0^4 - 3y_0^3 + 3y_0^2 y_1 + y_0^2 - 2y_0 y_1 + y_1^2$$

is

$$s_q\, p \equiv y_0^4\, q \mod [q]^2,$$

where $s_q = 3\,y_0^2 - 2\,y_0 + 2\,y_1$ is the separant of q. We have $\gcd(y_0^4, q) = 1$ and therefore $\mathcal{G}_q$ is an essential regular component.

This differential polynomial is actually a particular case of an example given by Ritt [Rit66, 3.26]

$$f_m = (y_0 y_2 + y_0 y_1 - 2y_1^2)^2 + \prod_{j=1}^{m} (y_1 - y_0 + j y_0^2)$$

The general components of the differential polynomials $y_1 - y_0 + j y_0^2$ are all essential.

J Back to the Ritt Problem

J.1 Computing differential bases

In Section H.1 we presented a theoretical process to determine a basis of the general component of an irreducible differential polynomial p in $\mathcal{F}\{Y\}$, endowed with a sequential ranking.

We specialised then this ranking to be orderly and we have denoted $\Theta_\tau p$ the set of derivatives of p of order less or equal to τ.

We then know that for a sufficiently big τ

$$\mathcal{G}_p^\tau = \left\{(\Theta_\tau p) : s_p^\infty\right\}.$$

is equal to the general component $\mathcal{G}_p$ of p. Such a τ may be characterized by the fact that $\mathcal{G}_p^\tau$ has only one component. But there is no known way to decide of this problem, since the decomposition algorithm applied on a set of differential polynomial do not return a minimal decomposition.

In Chapter G we have presented an algorithm which determines the essential components of $\{p\}$:

From a decomposition into prime or regular differential ideals of $\{p\}$, we determine a finite set of irreducible differential polynomials $a_0, a_1, \ldots, a_r$ such that $a_0 = p$ and

$$\{p\} = \bigcap_{i=0}^{r} \mathcal{G}_{a_i}.$$

For each a_i we compute a preparation equation of p w.r.t. a_i. We can read out of this preparation equation whether $\mathcal{G}_{a_i}$ is an essential component of p. The necessary and sufficient condition is given by the Low power theorem, Theorem G.3.1.

If it is the case, according to Corollary H.2.5 we can also determine from the preparation equation an integer ω_i such that $\mathcal{G}_p^{\omega_i}$ is not included in $\mathcal{G}_{a_i}$.

So that if

$$\omega = \max_{i=1}^{r} \omega_i$$

$\mathcal{G}_p^\omega$ is contained in no essential components of $\{p\}$ except for $\mathcal{G}_p$.

We could have proceeded otherwise by splitting more obviously the two processes. The first step is to determine the essential components $\mathcal{G}_{a_0}, \ldots, \mathcal{G}_{a_r}$ od $\{p\}$.

By a reduction algorithm, you may determine if a given differential polynomial in $\mathcal{F}\{Y\}$ belongs to one of the $\mathcal{G}_{a_i}$. A finite basis of $(\Theta_k p) : s_p^\infty$ provides a differential basis of $\mathcal{G}_p^k$. It is therefore possible to check whether $\mathcal{G}_p^k$ is included in the essential singular components of $\{p\}$.

By computing successively $\mathcal{G}_p^1$, $\mathcal{G}_p^2$, ..., we can thus determine ω' such that $\mathcal{G}_p^{\omega'}$ is also contained in no singular essential component of p.

This iterative process shall be used in practice. Indeed the bound found gets less tight as the number of derivations of the ring and the minimal degree or the maximal weight (ρ and κ) of the preparation equation increase.

J.1.1 Example: Consider, in the ordinary differential ring $\mathbb{Q}\{y\}$, the differential polynomial

$$p \ = y_1\, y_2^2 - y_0$$

The Rosenfeld-Gröbner decomposition is

$$\{p\} \ = \ \mathcal{G}_p \cap \{y_0\}.$$

The preparation equation of p w.r.t. to y_0 is trivial. $\{y_0\}$ is an essential component and the ω of Theorem H.3.1 is $\omega = 3$.
Nontheless

$$\mathcal{G}_p^1 = \left\{ y_1\, y_3 + 2\, y_2^2 - 1,\ y_0\, y_3 + 2\, y_1\, y_2^3 - y_1\, y_2,\ y_1\, y_2^2 - y_0 \right\}$$

and thus $\mathcal{G}_p^1$ is not contained in $\{y_0\}$, the only essential singular component.
It is no real surprise then than the iterative process, even if it requires several membership tests, is nearly four times faster that the direct process, which consists in determining ω first. (This is computed on MapleV.3 with the *Diffalg* package.)

J.1.2 Example: Consider the partial differential ring $\mathbb{Q}(x, y)\{u\}$ endowed with the derivations δ_x and δ_y. Let

$$p \ = \ (\delta_x u)^2 + (\delta_y u)^2 - x\,(\delta_x u) - y\,(\delta_y u) + u.$$

The minimal decomposition of $\{p\}$ is

$$\{p\} \ = \ \mathcal{G}_p \ \cap \ \{4\,u - x^2 - y^2\}$$

and the ω of Theorem H.3.1 is $\omega = 4$. But computing $(\Theta_4 p) : s_p^\infty$ can not be achieved with the actual implementation

Nonetheless, already $\mathcal{G}_p^1$ is not contained in the singular component. (In fact $\mathcal{G}_p^1 = \mathcal{G}_p$ already).

To compute the successive $\mathcal{G}_p^k$, we have thus far used a classical algorithm (presented in Section K) to compute the saturation ideals involved. We should think of refining this algorithm owing to the special shape of $\Theta_i p$. Indeed, we can nonetheless not always manage the result with the classical algorithm.

J.1.3 EXAMPLE: In the ordinary differential ring $\mathbb{Q}\{y\}$, consider

$$p = y_0^2 + y_2^3$$

The ω of Theorem H.3.1 is 35 but unfortunately neither process succeeds.

When dealing with partial differential polynomials, computing all the derivatives of order less or equal to 35 would already be "difficult".

Let us bypass these computationnal limitations and assume that, by one way or the other, we have determined an ω such that $\mathcal{G}_p^\omega$ is included in no singular essential components. We already gave in Section H.3 two simple criterions to determine if $\mathcal{G}_p^\omega = \mathcal{G}_p$. As was exhibited in Example H.3.3, this is not always the case.

$$\mathcal{G}_p^\omega = \mathcal{G}_p^\omega : s \ \cap \ \{\mathcal{G}_p^\omega, s\} = \mathcal{G}_p \cap \{\mathcal{G}_p^\omega, s\},$$

Therefore if $\mathcal{G}_p^\omega$ has other essential components than $\mathcal{G}_p$, they are non-essential singular components of p. Assume that $\{\mathcal{G}_p^\omega, s\}$ is a proper differential ideal and that

$$\{\mathcal{G}_p^\omega, s\} \ = \bigcap_{i=1}^{r} [A_i] : h_{A_i}^\infty$$

is a decomposition into prime differential ideals.

If all these components contain $\mathcal{G}_p$ then $\mathcal{G}_p^\omega = \mathcal{G}_p$ and we have completed a differential basis of the general component of p. Now, if there is one of the $[A_i] : h_{A_i}^\infty$ which does not contain $\mathcal{G}_p$, we compute the successive $\mathcal{G}_p^k$ for $k > \omega$ until $\mathcal{G}_p^k \not\subset [A_i] : h_{A_i}^\infty$.

Therefore, to be in a position to compute the differential basis of the general component of p, the crucial point is to determine if a singular component contains the general component. This proposition extend to the general case: the problem of determining a differential basis of a prime ideal givent by its characteristic set is equivalent to the problem of determining the inclusion of two ideals given by their characterisitc sets (see [PG97]).

J.1.4 EXAMPLE: In Example H.3.3 we considered the differential polynomial

$$q = y_0 \, y_1 + y_2^3.$$

We determined $\omega = 2 : \mathcal{G}_q^2$ is not contained in $\{y_1\}$ which is the only essential singular component. We then claimed that

$$\mathcal{G}_q^\omega = \mathcal{G}_q \ \cap \ \{y_0\}$$

was a minimal decomposition of $\mathcal{G}_q^\omega$.

According to Proposition H.1.1, there nonetheless exists $\omega' > \omega$ such that $\mathcal{G}_q^{\omega'} = \mathcal{G}_q$. Let us compute the differential bases of the successive $\mathcal{G}_p^k$, for $k > \omega$.

With the Rosenfeld-Gröbner membership test applied on all the elements of the differential basis of $\mathcal{G}_p^k$, we can decide when $\mathcal{G}_p^k \not\subset \{y_0\}$. This happens for $k = 4$: $\mathcal{G}_q^4$ contains the differential polynomial

$$\begin{gathered}
-124656 - 3925376\, y_5 - 37101484\, y_5^2 - 104225832\, y_5^3 \\
-170203032\, y_5^4 - 157516488\, y_5^5 - 56687040\, y_5^6 \\
+3065944\, y_4\, y_6 + 52499448\, y_6\, y_5\, y_4 + 1161181216\, y_6\, y_5^2\, y_4 \\
+104871024\, y_6\, y_4\, y_5^4 - 24315795\, y_6^2\, y_4^2 - 48026520\, y_6^2\, y_4^2\, y_5 \\
-64658655 y_6^2\, y_4^2\, y_5^2 + 174410112\, y_6^2\, y_4\, y_5^3 + 13286025\, y_6^3\, y_4^3.
\end{gathered}$$

Thus

$$\mathcal{G}_q^4 = \mathcal{G}_q$$

For second order ordinary differential polynomials in one differential indeterminate, J.F. Ritt has solved the problem of determining if the general component was included in a given singular component [Rit36]. In the other cases, only some criteria were secured.

J.2 Some criteria to decide of the Ritt problem

There are two main ideas to determine if a prime differential ideal, given by its characteristic set A, contains the general component of an irreducible differential polynomial p in $\mathcal{F}\{Y\}$.

For the case A contains a unique element a[1], Hillman provided a sample of criteria to prove that $[a] : s_a^\infty = \mathcal{G}_a$ contains $\mathcal{G}_p$. These are based on the Leading coefficient theorem and exposed in [Hil52].

In the case of ordinary differential polynomials, some extensions of Levi's lemma provide sufficient conditions for claiming that $\mathcal{G}_a$ does not contain $\mathcal{G}_p$.

To complete this memoir, we shall give the simplest form of the above mentionned criteria. The first one is simply obtained by specializing the proof of Theorem I.3.2.

[1]This is always the case when considering ordinary differential ring in only one differential indeterminate

J.2.1 PROPOSITION: Let p and a be irreducible differential polynomials in $\mathcal{F}\{Y\}$. Let u_a be the leader of a. In the preparation congruence of p w.r.t. a,

$$c_{-1}\, p \;\equiv\; \sum_{\gamma=0}^{l} c_\gamma\, m_\gamma(a) \mod [a]^{\rho+1},$$

consider $\theta\, a$ the factor of $m_0(a), \ldots, m_l(a)$ for which the rank of $\theta\, u_a$ is highest. If this $\theta\, u_a$ is the leader of p, then $\mathcal{G}_p \subset \mathcal{G}_a$.

PROOF: In the proof of Theorem I.3.2 we showed that if $v = \theta\, u_a$ was chosen as above, there existed an irreducible differential polynomial b which involved a derivative of v such that $\mathcal{G}_b$ was an essential component of $\{p\}$ and $\mathcal{G}_b \subset \mathcal{G}_a$. If v is the leader of p, obviously $b = p$. □

For the second criterion, we introduce the relation of *domination* [Kol73, IV.12] between two monomials.

Let m be a monomial in a differential polynomial ring $\mathcal{R}\{z\}$. For a derivative θz we note $m_{\theta\, z}$ the product of all the factors of m which are derivatives of $\theta\, z$.

J.2.2 DEFINITION: Let m and m' be two monomials in some differential polynomial ring $\mathcal{R}\{z\}$. m' dominates m if for any derivative $\theta\, z$ either

$$\deg\, m_{\theta\, z} \;<\; \deg\, m'_{\theta\, z}$$

or

$$m_{\theta\, z} = m'_{\theta\, z}$$

A light version of the Domination lemma [Kol73, IV.12, Lemma 6] can then be stated as follow.

J.2.3 LEMMA: Let p and a be two different irreducible differential polynomials of $\mathcal{F}\{y_1, \ldots, y_n\}$. Assume that the preparation equation of p according to a can be written

$$s_a^\alpha p = c_0\, m_0(a) + \sum_{\gamma=1}^{l} c_\gamma\, m_\gamma(a)$$

where $m_1, \ldots, m_l$ dominate m_0. Then there exists an integer d and a differential polynomial $r \in [a]$ such that

$$m_0(a)\,(c_0^d + r) \;\in\; \{p\}$$

and thus $\mathcal{G}_p$ is not included in $\mathcal{G}_a$.

The proof of this lemma consists of recursive calls to Levi's lemma. It is highly probable that we can extract from this proof a bound ω such that $(\Theta_\omega p) : s_p^\infty$ is not included in $\mathcal{G}_a$.

J.3 Prospects

Both of these criteria have been lifted by Kolchin to the general case where we have to determine if a prime differential ideal given by its characteristic set A contains the general component of an irreducible differential polynomial p. ([Kol65] and [Kol73, IV]). To this aim, a preparation equation according to the characteristic set of a prime differential ideal is introduced in [Kol73, I.9]. The implementation of Kolchin's criteria requires thus further investigations. We can contemplate two ways to tackle the problem.

- From a decomposition into regular differential ideals, it is possible, but costly, to obtain a decomposition into prime differential ideals through algebraic computations: that would lead to a counter part of the algorithm presented in Chapter G which relied on factorization. We then would need only to implement the criteria as they exist.
- We can also consider working directly on the regular components computed by the Rosenfeld-Gröbner algorithm. This requires, as in Chapter I , to go deeper into the proofs of the criteria.

Studying and implementing these criteria will be a natural continuation of this thesis work.

Part IV

Singular points of first order ordinary differential equations

This part is mostly independent of the previous ones. We shall focus our attention on first order differential equations.

We noted in Section H.3, that it was always possible in that case to compute a differential basis of the general solution. We want to show how this can be useful to analyze the singular points of solutions.

We shall first review the existing analysis of singular points. A geometrical approach allows a better understanding of them. The classification it generates puts light on the analytic behavior of the solutions in their neighborhood. But this analysis breaks down when there exists a singular solution.

K Notations in Algebra

K.1 Algebraic varieties

We will consider a commutative field $\mathcal{K}$ of characteristic zero and a ring of polynomial with coefficients in that field $\mathcal{K}[z_1, \ldots, z_n]$. For a subset Σ of $\mathcal{K}[z_1, \ldots, z_n]$ we define the radical of Σ as

$$\sqrt{\Sigma} = \{q \in \mathcal{K}[z_1, \ldots, z_n] \text{ such that } \exists n \in \mathbb{N}^*,\ q^n \in \Sigma\}$$

NOTATION: (Σ) and $\langle\Sigma\rangle$ will be respectively the ideal and the radical ideal generated by a subset Σ of $\mathcal{K}[z_1, \ldots, z_n]$.

$$\langle\Sigma\rangle = \sqrt{(\Sigma)} = \{q \in \mathcal{K}[z_1, \ldots, z_n] \text{ such that } \exists n \in \mathbb{N}^*,\ q^n \in (\Sigma)\}.$$

In the affine space $\mathcal{K}^n$, we define the algebraic variety of a finite set of polynomials $p_1, \ldots, p_s$ as

$$\mathcal{V}(p_1, \cdots, p_s) = \{(a_1, \cdots, a_n) \in \mathcal{K}^n \text{ such that } \ p_i(a_1, \cdots, a_n) = 0\ \forall i,\ 1 \leq i \leq s\}$$

As $\mathcal{K}[z_1, \ldots, z_n]$ is nœtherian, any of its ideal is finite, and therefore it makes sense to define the algebraic variety of an ideal; It is the algebraic variety of a basis of this ideal.

The algebraic variety of $\mathcal{K}[z_1, \ldots, z_n]$ is thus the algebraic variety of the unit polynomial. It is the empty set. Conversely, the Hilbert theorem ensures that if $\mathcal{K}$ is algebraically closed, and if I is an ideal of $\mathcal{K}[z_1, \ldots, z_n]$ then the algebraic variety of I is empty only if I contains the unit polynomial.

$$\mathcal{V}(I) = \emptyset \ \Rightarrow\ I = (\mathbf{1}) = \mathcal{K}[z_1, \cdots, z_n]$$

Let now V be a subset of $\mathcal{K}^n$. We define

$$\mathcal{I}(V) = \{p \in \mathcal{K}[z_1, \cdots, z_n] \text{ such that } \ p(a_1, \cdots, a_n) = 0 \quad \forall (a_1, \cdots, a_n) \in V\}$$

$\mathcal{I}(V)$ is a radical ideal.

The Nullstellensatz (stronger version of Hilbert theorem) ensures that whenever $\mathcal{K}$ is algebraically closed,

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$$

Therefore when $\mathcal{K}$ is closed there is a one-to-one relation between the radical ideals of $\mathcal{K}[z_1, \cdots, z_n]$ and the algebraic varieties in $\mathcal{K}^n$.[1]

K.2 Quotient ideals

K.2.1 Definition: Consider an ideal I in $\mathcal{K}[z_1, \ldots, z_n]$. For a non-empty subset S of $\mathcal{K}[z_1, \ldots, z_n]$ we define the quotient of I w.r.t. S to be

$$I : S = \{a \in \mathcal{K}[z_1, \ldots, z_n] \text{ such that } \forall s \in S \; s\,a \in I\}.$$

We immediately see that $I \subset I : S$ and that $I : S$ is an ideal which is equal to the quotient of I w.r.t. to the ideal generated by S.

$$I : S = I : (S)$$

When S consists of a single element s we simply write $I : s$.

K.2.2 Definition: For an element s of $\mathcal{K}[z_1, \ldots, z_n]$, we define the saturation of I w.r.t. s as

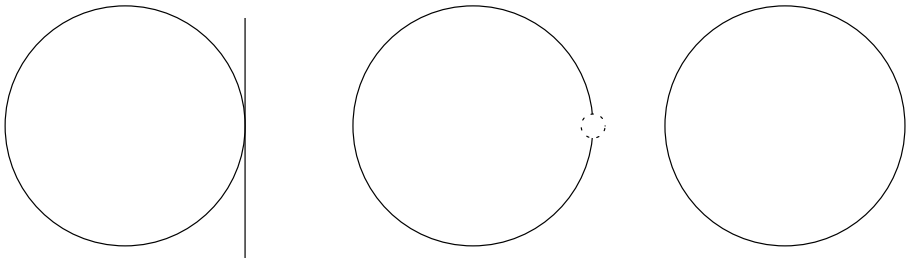
$$I : s^\infty = \bigcup_{e=0}^{\infty} I : s^e = \{a \in \mathcal{K}[z_1, \ldots, z_n] \text{ such that } \exists \alpha \in \mathbb{N} \; s^\alpha a \in I\}$$

We have $I \subset I : s \subset I : s^2 \subset \ldots I : s^\infty$. As our polynomial ring is nœtherian, there must exist a k such that $I : s^k = I : s^\infty$. When R is a radical ideal $R : s^\infty = R : s$ and therefore for any ideal I, $\sqrt{I : s^\infty} = \sqrt{I} : s$.

K.2.3 Example: In the polynomial ring $\mathbb{R}[x, y]$ consider the ideal I generated by $(x^2 + y^2 - 1)(x - 1)^2$. Let $s = (x - 1)$. Then $I : s^\infty = I : s^2$ is the ideal generated by $(x^2 + y^2 - 1)$.

$\mathcal{V}(I)$ consists of the unit circle together with one of its tangents. This tangent is precisely $\mathcal{V}(s)$. Thus $\mathcal{V}(I) - \mathcal{V}(s)$ is the unit circle excepted for a point. Eventually, $\mathcal{V}(I : s^\infty)$ is the complete unit circle. It actually is the smallest algebraic variety containing $\mathcal{V}(I) - \mathcal{V}(s)$ (the Zarisky closure of $\mathcal{V}(I) - \mathcal{V}(s)$).

[1] In differential algebra we also find this one-to-one relationship between radical differential ideals and the set of zeros of a differential system. But we can not consider this approach since there is no differential closure.



$\mathcal{V}(I)$ $\mathcal{V}(I) - \mathcal{V}(s)$ $\mathcal{V}(I:s)$

Computing saturation ideals

Assume $\mathcal{K}$ is a computable field. Typically we will choose $\mathbb{Q}$ or an algebraic extension of it.

On $\mathcal{K}[z_0 \cdots, z_m, z]$ a term order $>$ where z prevails satisfies the property $z^\alpha r > z^\beta t$ for any monomials r and t of $\mathcal{K}[z_0, \cdots, z_m]$ whenever α is greater than β.

If G' is a Gröbner basis of some ideal I of $\mathcal{K}[z_0 \cdots, z_m, z]$ according to an order where z prevails, then $G = G' \cap \mathcal{K}[z_0, \ldots, z_m]$ is a Gröbner basis of the elimination ideal of I with respect z, that is $I \cap \mathcal{K}[z_0, \ldots, z_m]$, according to the induced order.

Now the saturation of an ideal $I = (p_1, \cdots, p_k)$ w.r.t. an element s of $\mathcal{K}[z_0, \ldots, z_m]$ is the elimination ideal of $(s\ z - 1, p_1, \cdots, p_k)$ in $\mathcal{K}[z_0 \cdots, z_m, z]$ with respect to the dummy indeterminate z.

K.3 Decompositions

We have the following splitting properties of the radical ideals:

K.3.1 Proposition:

- $\langle \Sigma, ab \rangle = \langle \Sigma, a \rangle \cap \langle \Sigma, b \rangle$, for any subset Σ and elements a, b of $\mathcal{K}[z_1, \ldots z_n]$.
- $\langle \Sigma \rangle = \langle \Sigma \rangle : s \cap \langle \Sigma, s \rangle$, for any non-empty subset Σ and element s of $\mathcal{K}[z_1, \ldots z_n]$.

which entails the decomposition into prime ideals:

K.3.2 Theorem: Any radical ideal R in $\mathcal{K}[z_1, \ldots z_n]$ is a finite intersection of prime ideals

$$R = \bigcap_{i=1}^{r} P_i$$

where P_i is a prime differential ideal.

When $\mathcal{K}$ is algebraically closed, a minimal prime decomposition of a radical ideal R corresponds to the decomposition of its variety in $\mathcal{K}^n$ into irreducible varieties.

L Geometry for first order differential equations

L.1 Integral curves

We consider a differential equation of first order $p(x, y, y') = 0$ which we shall rewrite for consistency with the other parts as

$$p(x, y_0, y_1) \;=\; 0$$

In this presentation p is a polynomial in $\mathcal{K}[x, y_0, y_1]$, where $\mathcal{K}$ is a field of characteristic zero. This entitles us to describe the singular locus and other related objects as algebraic varieties. These can therefore be handled in a computer algebra system and the operations we shall describe can all be done with Gröbner bases techniques.

The function giving y_1 for a given (x, y_0) is multi-valued. Thus instead of looking at the (x, y_0)-plane we can turn our attention to the algebraic surface in $\mathcal{K}^3$

$$\mathcal{S}_p \;:\quad p(x, y_0, y_1) = 0$$

At a point where $\mathcal{S}_p$ is regular, its tangent space is the set of vectors $\xi \in \mathcal{K}^3$ such that

$$p_x \, \mathrm{d}x(\xi) + p_{y_0} \, \mathrm{d}y_0(\xi) + p_{y_1} \, \mathrm{d}y_1(\xi) = 0.$$

In most of the works on the subject, the surface $\mathcal{S}_p$ is assumed to be everywhere regular. That way, the purely differential singularities do not mix with the geometric singularities. Such an assumption is for instance made in the work of Izumiya [IY93] on the definition of the singular and general solution. We shall not make this assumption here and see where this geometric approach gets to its limits.

L.1.1 Definition: An integral curve of $p(x, y_0, y_1) = 0$ is a regular curve on the surface $\mathcal{S}_p \;:\quad p(x, y_0, y_1) = 0$ in $\mathcal{K}^3$ such that the tangent at each of its points is a zero of the one form $\mathrm{d}y_0 - y_1 \mathrm{d}x$.

The set of vectors $\xi \in \mathcal{K}^3$ such that

$$\mathrm{d}y_0(\xi) - y_1 \mathrm{d}x(\xi) = 0,$$

is called the *contact* plane at a point (x, y_0, y_1). This is the plane parallel to the y_1 axis which cuts the (x, y_0) axis along a line of slope y_1.

If an integral curve of $p(x, y_0, y_1) = 0$ goes through a regular point of $\mathcal{S}_p$, its tangent vector belongs to the intersection of the tangent plane to $\mathcal{S}_p$ and the contact plane at this point.

In other words, if γ is locally parameterized by

$$\begin{array}{rccl} \gamma: & (a,b) \in \mathbb{R} & \to & \mathcal{K}^3 \\ & t & \mapsto & (x(t), y_0(t), y_1(t)) \end{array} \tag{1}$$

the definition says

1. γ is a regular curve: $\dfrac{\mathrm{d}\gamma}{\mathrm{d}t} \neq 0 \ \ \forall t \in (a,b)$.
2. γ lives on $\mathcal{S}_p$: $p(x(t), y_0(t), y_1(t)) = 0, \ \ \forall t \in (a,b)$.
3. the tangent to γ is a zero of $\mathrm{d}y_0 - y_1\,\mathrm{d}x$: $\dfrac{\mathrm{d}y_0}{\mathrm{d}t}(t) = y_1(t)\dfrac{\mathrm{d}x}{\mathrm{d}t}(t), \ \forall t \in (a,b)$.

Note that to any continuously differentiable solution $f : x \to f(x)$, defined on an interval I, of the differential equation $p(x, y_0, y_1) = 0$, we can associate the parametric curve

$$\begin{array}{rccl} \gamma_f: & I & \to & \mathcal{K}^3 \\ & x & \mapsto & (x, f(x), f'(x)). \end{array} \tag{2}$$

which is an integral curve of $p(x, y_0, y_1) = 0$.

Conversely, consider an integral curve is given by (1). If for some $t_0 \in (a,b)$, $\dfrac{\mathrm{d}x}{\mathrm{d}t}(t_0) \neq 0$, we can write locally t as a function of x. Then y_0 and y_1 can also be seen as function of x. We have

$$\frac{\mathrm{d}y_0}{\mathrm{d}x}(x) = \frac{\mathrm{d}y_0}{\mathrm{d}t}(t(x))\frac{\mathrm{d}t}{\mathrm{d}x}(x) = \left(\frac{\mathrm{d}y_0}{\mathrm{d}t}(t(x))\right)\left(\frac{\mathrm{d}x}{\mathrm{d}t}(t(x))\right)^{-1} = y_1(x).$$

Therefore y_0 considered as a function of x is a solution of the differential equation $p(x, y_1, y_0) = 0$.

More generally, to see the connection backward between integral curves and solutions, let the projection from $\mathcal{S}_p$ to the (x, y_0)-plane be

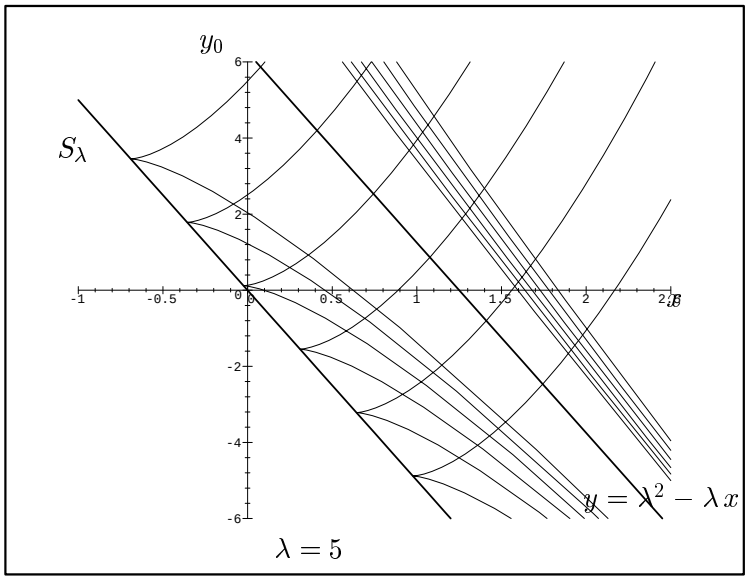
$$\begin{array}{rccl} \pi: & \mathcal{S}_p & \to & \mathcal{K}^2 \\ & (x, y_0, y_1) & \mapsto & (x, y_0). \end{array}$$

Consider a point of an integral curve with tangent ξ. Assume ξ is not parallel to the (y_0, y_1)-plane, that is $\mathrm{d}x(\xi) \neq 0$. Since ξ is a zero of $\mathrm{d}y_0 - y_1\mathrm{d}x$, the projection by π of the integral curve will have a tangent with slope y_1. The projection is thus the graph of a solution of the differential equation $p(x, y_1, y_0) = 0$. .

L.1.2 EXAMPLE: Consider the equation

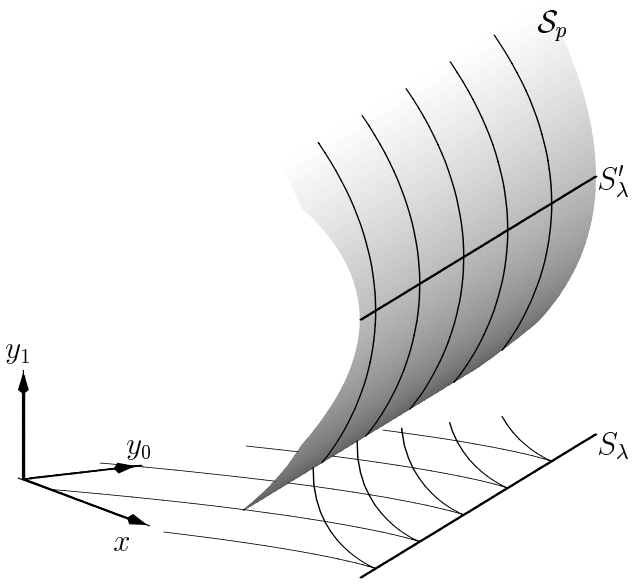
$$p(x, y_0, y_1) \;=\; y_1^2 - 4y - 4\lambda x = 0 \quad \text{where } \lambda > 0.$$

For any $x, y_0 \in \mathbb{R}^2$ such that $y_0 + \lambda x > 0$, p admits two simple real roots in y_1. There are thus two smooth solutions through each such pair x, y_0.



On the line $S_\lambda : y = -\lambda x$, p has a double root $y_1 = 0$. Two tangential solutions are issued from these points. Note also that the solutions have a moving singularity at infinity in the direction of the line $y = \lambda^2 - \lambda x$. We will not study this last type of singularity.

Instead of tracing the graphs $(x, f(x))$ of a solution of $p(x, y_0, y_1) = 0$ in $\mathbb{R}^2$, we can contemplate tracing them on the surface $\mathcal{S}_p : p(x, y_0, y_1) = 0$. We represent the graphs obtained in the neighborhood of the line $S'_\lambda : y + \lambda x = 0,\ y_1 = 0$ together with their projection on $\mathbb{R}^2$. The cusps on S_λ are unfolded. S'_λ is the set of the critical points of the projection π.



L.2 Singular points

The points in the neighborhood of which π is not diffeomorphic are the points where either $\mathcal{S}_p$ does not admit a tangent plane or the tangent plane is parallel to the y_1-axis. They are the points of $\mathcal{S}_p$ where $s = \frac{\partial p}{\partial y_1}$ vanish. We call the polynomial s the separant of p. We will also note

$$p_x = \frac{\partial p}{\partial x} \quad p_{y_0} = \frac{\partial p}{\partial y_0} \quad p_{y_1} = \frac{\partial p}{\partial y_1} = s$$

L.2.1 Definition: The singular points of the differential equation $p(x,\, y_0,\, y_1) = 0$ are the points of $\mathcal{S}_p$ for which the *separant* vanishes. They satisfy

$$p(x,\, y_0,\, y_1) = 0 \quad \text{and} \quad s(x, y_0, y_1) = \frac{\partial p}{\partial y_1}\,(x,\, y_0,\, y_1) = 0$$

Contact singular points are the singular points for which $p_x + y_1 p_{y_0}$ also vanishes. *Regular* singular points[1] are the points for which $p_x + y_1 p_{y_0}$ does not vanish.

[1] this terminology is borrowed from [Arnon] and should be distinguished from the terminology used when dealing for linear differential equations

Assume that an integral curve goes through a singular point with tangent ξ. Then at this point

$$p_{y_1} = 0, \;\; p_x \, \mathrm{d}x + p_{y_0} \, \mathrm{d}y_0 + p_{y_1} \, \mathrm{d}y_1 \; = \; 0 \quad \text{and} \quad \mathrm{d}y_0 - y_1 \, \mathrm{d}x = 0.$$

This results in

$$(p_x + y_1 \, p_{y_0}) \; \mathrm{d}x(\xi) = 0.$$

If this is a regular singular point then $\mathrm{d}x(\xi) = 0$: the integral curve can not be parameterized by x at this point.

If the point is a contact singular point, i.e. $(p_x + y_1 \, p_{y_0}) = 0$, either $\mathcal{S}_p$ has no tangent space at this point ($p_x = p_{y_0} = p_{y_1} = 0$) or the tangent space is equal to the contact plane;

Regular singular points are in fact the singularities of the projection π while the contact regular points have a more intrinsic nature. At these latter points, the possible tangents to an integral curve remain undetermined.

We call *regular* points the point which are not singular. The integral curve through this point can be parameterized by x and their projections are solutions of the differential equation $p(x, y_0, y_1) = 0$.

Points with infinite tangent

Assume that the polynomial p defining the differential equation can be written

$$p(x, y_0, y_1) = i_n(x, y_0) \, y_1^n + i_{n-1}(x, y_0) \, y_1^{n-1} + \ldots + i_0(x, y_0) \tag{1}$$

where $n > 0$ and $i_n(x, y_0)$ is different from zero. We call i_n the initial of p.

When i_n belongs to $\mathcal{K}$, all the zeros (x, y_0, y_1) of p have a finite y_1. When i_n does not belong to $\mathcal{K}$, to any point of the algebraic variety of i_n in the (x, y_0) plane there corresponds at least one zero of p with an infinite y_1. At such points, there is obviously no differentiable solution of the differential equation $p(x, y_0, y_1) = 0$. Such points can not be regular points.

This can also be seen as follow: if p is given by (1), the separant of p is

$$s(x, y_0, y_1) = \frac{\partial p}{\partial y_1} = n \, i_n \, y_1^{n-1} + \ldots + i_1(x, y_0),$$

and thus has the same initial as p up to a factor in $\mathcal{K}$. A zero (x, y_0, y_1) of p with an infinite y_1 is such that (x, y_0) is a zero of i_n and thus it is also a zero of s. It is a singular point of the differential equation.

Now

$$p_x + y_1 \, p_{y_0} = \left(\frac{\partial i_n}{\partial x} + y_1 \, \frac{\partial i_n}{\partial y_0} \right) y_1^n + \left(\frac{\partial i_{n-1}}{\partial x} + y_1 \, \frac{\partial i_{n-1}}{\partial y_0} \right) y_1^{n-1} + \ldots + \left(\frac{\partial i_0}{\partial x} + y_1 \, \frac{\partial i_0}{\partial y_0} \right)$$

Thus a zero (x, y_0, y_1) of p with an infinite y_1 is a contact singular point if

- $\dfrac{\partial i_n}{\partial y_0}(x, y_0) = 0$ when i_n is not free of y_0
- $\left(\dfrac{\partial i_n}{\partial x} + \dfrac{\partial i_{n-1}}{\partial y_0}\right)(x, y_0) = 0$ when i_n is free of y_0.

Algebraic characterization

The locus of singular points V_s is the algebraic variety of (p, s).

$$V_s = \mathcal{V}(p, s).$$

If we assume that p has no factor independent of y_1, V_s is an algebraic curve.

The locus of contact singular points is a sub-variety V_c of V_s.

$$V_c = \mathcal{V}\left(p, s, p_x + y_1\, p_{y_0}\right).$$

Actually V_s splits into the locus of regular singular points, V_r, and the locus of contact singular points, V_c.

$$V_s = V_r \cup V_c$$

and

$$V_r = V_s - V_c \subset \mathcal{V}\left((p, s) : \left(\frac{\partial p}{\partial x} + y_1 \frac{\partial p}{\partial y_0}\right)^{\infty}\right).$$

We shall see that the locus of contact singular points $\mathcal{V}_c$ can be split further.

L.2.2 Example: (an example given in [IY93])

Consider the equation

$$y_1^2 - 2xy_1 + y_0 = 0.$$

The locus of singular points is the algebraic variety of

$$R_s = \langle p, p_{y_1} \rangle = (y_1 - x, y_0 - x^2)$$

which is projected by π into the parabola $y_0 = x^2$. The locus of contact singular points is the variety of

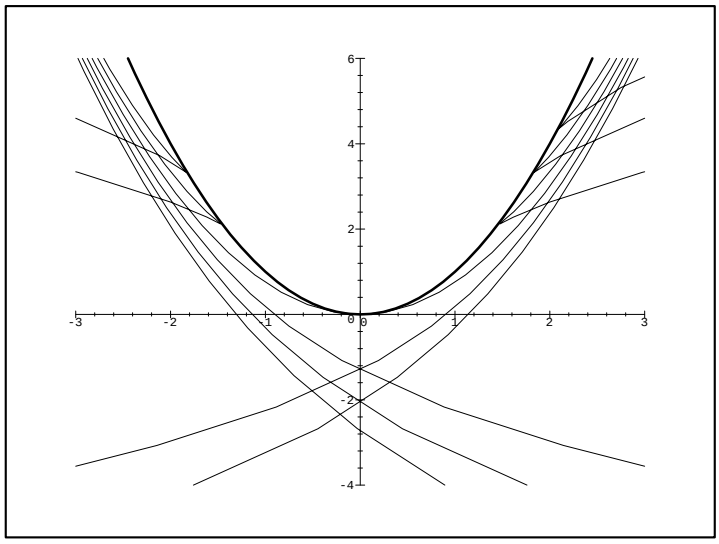
$$R_c = \langle p, p_{y_1}, p_x + y_1 p_{y_0} \rangle$$

which consists only of the origin O.

The integral curves can be parameterized away from the line $y_1 = 0, y_0 = 0$ as

$$\left\{ \begin{array}{lcl} x(t) & = & \frac{a}{t^2} + \frac{2}{3}t \\ y_0(t) & = & 2\,t\,x(t) - t^2 \\ y_1(t) & = & t \end{array} \right.$$

If we sketch the graphs of the solutions in the (x, y_0) we see that the solutions have a branch point on the singular locus parabola $y_0 = x^2$, except at the origin. The origin is crossed by two smooth solutions.



L.3 Singular integral curves

We have defined the singular solutions as the solutions consisting of singular points. Assume that $f : x \to f(x)$ is such a solution. As along γ_f, as defined by (2), the tangent ξ satisfies $\mathrm{d}x(\xi) = 1$, γ_f consists of contact singular points.

Conversely, assume that the locus of contact singular points is a curve. Along this curve we have

$$p_{y_1} = 0, \quad p_x + y_1 p_{y_0} = 0 \quad \text{and} \quad p_x \mathrm{d}x + p_{y_0} \mathrm{d}y_0 + p_{y_1} \mathrm{d}y_1 = 0$$

from which follows that

$$p_{y_0} \left(\mathrm{d}y_0 - y_1 \, \mathrm{d}x \right) = 0.$$

If we make the assumption that $\mathcal{S}_p$ is everywhere regular, p_{y_0} can not vanish at a contact singular point. And therefore a curve of contact singular point is an integral curve. It projects into a singular solution whenever $\mathrm{d}x$ does not vanish. But we can question what happens when p_{y_0} vanishes on a curve of contact singular points. Along such a curve, $\mathcal{S}_p$ admits no tangent space. By the following two examples we show that the answer can not be brought simply.

L.3.1 Example: Consider the differential equation

$$p \; = \; (y_1 - 1)^2 + y_0^2 = \; 0$$

The locus of singular points consists only of contact singular points. It is the algebraic variety of

$$R_s \;=\; R_c \;=\; \langle p, 2\,(y_1 - 1)\rangle = \langle y_0, y_1 - 1\rangle.$$

$p_{y_0} = 2\,y_0$ vanishes on the curve $\mathcal{V}(y_0, y_1 - 1)$ and obviously $\mathcal{V}(y_0, y_1 - 1)$ is not an integral curve.

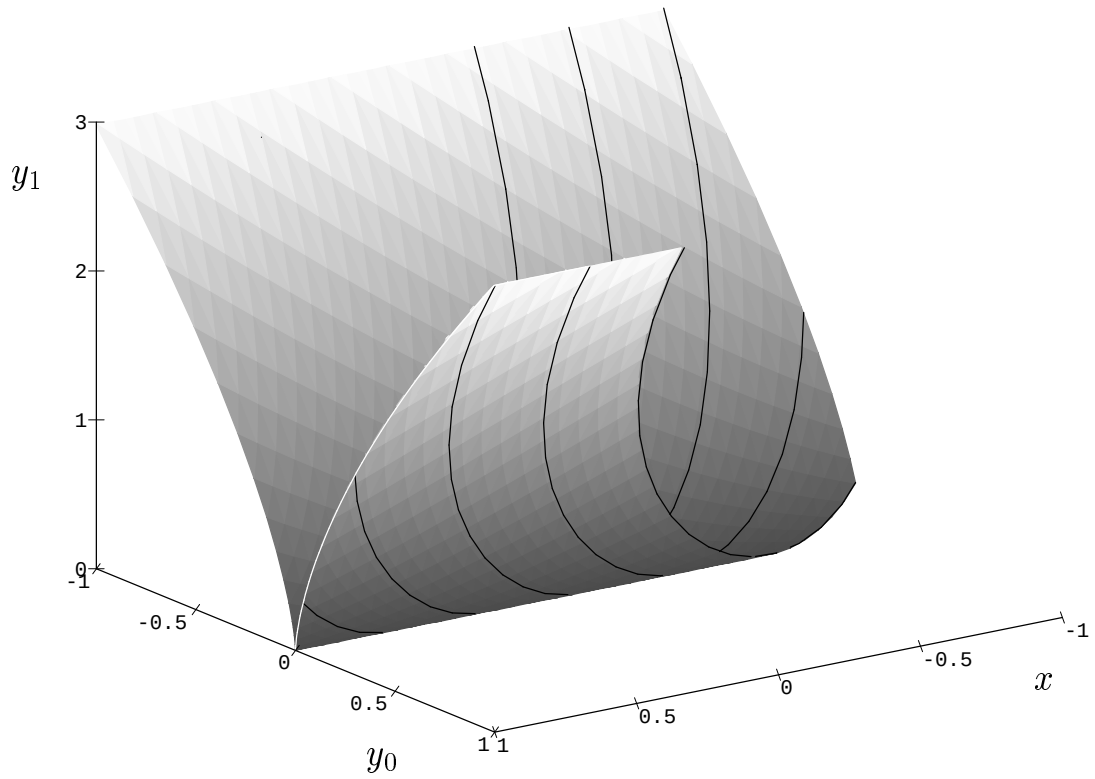
L.3.2 Example: Conversely consider

$$p = y_1^3 - 27y_0^2 = 0$$

The locus of singular points consists only of contact singular points. It is the algebraic variety of

$$R_s = R_c = \langle p, s\rangle = \langle y_1^3 - 27y_0^2, 3y_1^2\rangle = \langle y_0, y_1\rangle$$

It turns out that $R_s = \langle p, p_x, p_{y_0}, p_{y_1}\rangle$ and thus $\mathcal{S}_p$ admits no tangent space along the singular locus. Nonetheless, the line $y_0 = 0, y_1 = 0$ is easily seen to be an integral curve. Furthermore, the non-singular integral curves are tangent to this line.



Therefore, when the locus of contact singular points V_c contains a curve and if $p_{y_0} = 0$ vanishes on this curve, we would need further criteria to decide whether this curve is an integral curve or not.

In the setting of differential algebra, in Part II , we have presented reduction algorithms which decide when a set of algebraic differential equations admits a solution. If we apply these algorithms on $p,\ p_{y_1},\ p_{y_0},\ p_x$, we can determine if this set defines an integral curve which can be projected, locally, into a solution.

In interpreting x as another dependent variable, we could as well use the algorithm above mentioned to decide whether the curve is an integral curve. This can be interesting when the contact curve can at none of its points be parameterized by x, as in the example below.

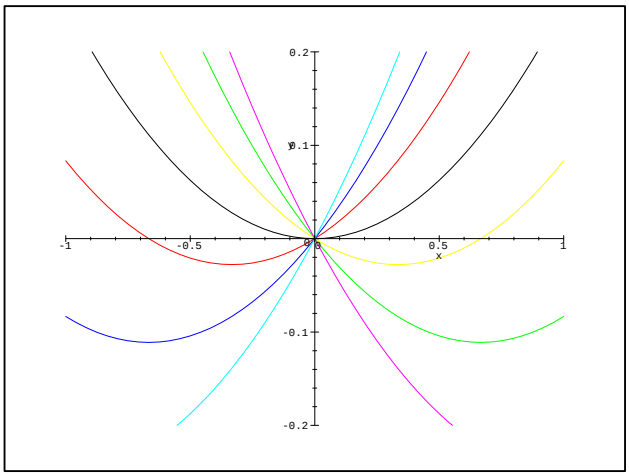
L.3.3 Example: Consider the differential equation

$$p(x, y_0, y_1) \;=\; 4xy_1 - 4y_0 + x^2 \;=\; 0.$$

The locus of singular point is the algebraic variety of

$$R_s = (x, y_0)$$

which is exactly the locus of contact singular points. p_{y_0} does not vanish on this line and therefore $x = 0, y_0 = 0$ is an integral curve. But it is projected by π into a single point.



M Analytic approach

Let $p(x, y_0, y_1) = 0$ be a differential equation of first order, where p is a polynomial with coefficient in a field $\mathcal{K}$. In the previous chapter we have classified the zeros $(x, y_0, y_1) \in \mathcal{K}^3$ of p into the regular points, the regular singular points and the contact singular points. We shall see in the two first cases what sort of solutions we can expect at these points. As we have said it, contact singular points are the intrinsic singular points. The behavior of the solutions at such points needs a case by case analysis.

M.1 Cauchy points

The zero of the resultant of p and $s = \frac{\partial p}{\partial y_1}$ with respect to y_1 determines the points where p and s have a common root in y_1, that is the singular points.

Suppose we are given an initial condition (x^o, y_0^o), in a field extension $\mathcal{K}'$ of $\mathcal{K}$, that is not a zero of the resultant of p and s. Then $p(x^o, y_0^o, y_1) = 0$ admits only simple roots in y_1. As we have noted it in the previous chapter, these roots must be finite.

For such a root y_1^o, (x^o, y_0^o, y_1^o) is a regular point. At this point, by the implicit function theorem, the differential equation is locally equivalent to an explicit ordinary differential equation $y_1 = g(x, y_0)$, where g is smooth. The Cauchy theorem ensures then the local existence, uniqueness and smoothness of the solution at this point. We can develop the unique solution of $p(x, y_0, y_1) = 0$ at this point into a converging power series:

$$\bar{y} = y_0^o + (x - x^o)y_1^o + \frac{(x - x^o)}{2}y_2^o + \cdots = \sum_{i \geq 0} \frac{(x - x^o)^i}{i!} y_i^o$$

The y_i^o, for $i > 1$, are easily obtained with the successive derivatives of p. Indeed

$$\delta p = s\, y_2 + t_1,\ \delta^2 p = s\, y_3 + t_2, \cdots$$

where s, t_1 involve only x, y_0, y_1 and t_2 involves only x, y_0, y_1, y_2. Hence, as

$s(x^o, y_0^o, y_1^o) \neq 0$,

$$y_2^o = \frac{t_1(x^o, y_0^o, y_1^o)}{s(x^o, y_0^o, y_1^o)},\ y_3^o = \frac{t_2(x^o, y_0^o, y_1^o, y_2^o)}{s(x^o, y_0^o, y_1^o)}, \cdots .$$

Note that this process is certainly not efficient for actually computing the convergent power series solution at a regular point.

M.2 Branch points

The regular singular points are in fact the singularities of the projection π only. Shall we make another projection, there will be no singularity. We adopt another coordinate system (X, Y_0, Y_1) of $\mathcal{K}^3$ given by

$$X = y_1,\ Y_0 = x\, y_1 - y_0,\ Y_1 = x.$$

The diffeomorphism

$$\begin{array}{rccc} L: & \mathcal{K}^3 & \to & \mathcal{K}^3 \\ & (x, y_0, y_1) & \mapsto & (y_1,\ x\, y_1 - y_0,\ x) \end{array}$$

is the *Legendre transformation*. From the definition $L^{-1} = L$ and if we apply this contact transformation to our differential equation, we obtain a new differential equation

$$P(X, Y_0, Y_1) = p \circ L^{-1}(X, Y_0, Y_1) = p(Y_1, X\, Y_1 - Y_0,\ X)$$

in the new coordinate system (X, Y_0, Y_1).

M.2.1 LEMMA: γ is an integral curve of the differential equation $p(x, y_0, y_1) = 0$ if and only if $L \circ \gamma$ is an integral curve of the differential equation $P(X, Y_0, Y_1) = 0$.

Working out the partial derivatives at a point (X^o, Y_0^o, Y_1^o) corresponding to (x^o, y_0^o, y_1^o) through L, we show the following

$$\begin{aligned} \frac{\partial P}{\partial Y_1}(X^o, Y_0^o, Y_1^o) &= \left(\frac{\partial p}{\partial x} + y_1 \frac{\partial p}{\partial y_0}\right)(x^o, y_0^o, y_1^o) \\ \left(\frac{\partial P}{\partial X} + Y_1 \frac{\partial P}{\partial Y_0}\right)(X^o, Y_0^o, Y_1^o) &= \frac{\partial P}{\partial Y_1}(X^o, Y_0^o, Y_1^o) \end{aligned}$$

As a consequence, if (x^o, y_0^o, y_1^o) is a regular singular point of $p(x, y_0, y_1) = 0$, (X^o, Y_0^o, Y_1^o) is a regular point of $P(X, Y_0, Y_1) = 0$. We may thus find a converging power series solution of this latter differential equation at this point

$$Y_0(X) = Y_0^o + (X - X^o)\, Y_1^o + \frac{(X - X^o)^2}{2}\, Y_2^o + \cdots$$

together with its derivative

$$Y_1(X) = Y_1^o + (X - X^o)\, Y_2^o + \frac{(X - X^o)^2}{2}\, Y_3^o + \cdots .$$

If $Y_0(X) = Y_0^o + (X - X^o)\, Y_1^o$ then $x = x^0$, $y_0 = y_0^o$ is an integral curve. Otherwise there must be some $k \geq 1$ such that $Y_{k+1}^o \neq 0$. Let ν be the smallest such k and let $a_\nu = \frac{Y_{\nu+1}^o}{\nu!}$. Then, taking $t = X - X^o$, an integral curve of $p(x, y_0, y_1) = 0$ at (x^o, y_0^o, y_1^o) can be given as

$$\begin{aligned} x(t) &= x^o + \nu\, a_\nu\, t^\nu\ (1 + \ldots\ldots) \\ y_0(t) &= y_0^o + a_\nu \left(\frac{\nu}{\nu+1} + y_1^o\right) t^{\nu+1}\ (1 + \ldots\ldots) \\ y_1(t) &= t \end{aligned}$$

The solutions have there a branch point of order ν. They can in fact be given as converging Puiseux series in x.

M.3 A polygon process

A polygon process as introduced by Briot and Bouquet in [BB56] and Fine [Fin89] will manage the integral power series at a regular point, without derivating the equation, as well as the Puiseux series solutions at a regular singular point, without going through the Legendre transform.

This polygon process can also be used to find the Puiseux series at contact singular points. But the results on the existence and convergence of the series there obtained suffer some gaps. Cano obtained some results in that direction [Can93b], [Can93a].

Indeed, the less known behaviors of the integral curves of the differential equation $p(x, y_0, y_1) = 0$ are to be found in the neighborhood of contact singular points. L.Dara gave a complete classification [Dar75] of the contact singular points in the case the surface $\mathcal{S}_p\ :\ p(x, y_0, y_1) = 0$ is regular.

N The general solution

Let us assume that the differential equation $p(x, y_0, y_1) = 0$ admits a singular solution. Then according to Section L.3 the points of the above integral curve are contact singular points. There is thus far no general result on the behavior of the *non-singular* solutions around these points. But one shall consider that then $p(x, y_0, y_1) = 0$ does not characterize fully the non-singular solutions. With a basis of the general component, we can look for a maximal set of initial conditions for which we can ensure the existence and uniqueness of a converging power series solution.

We make the following assumptions on p which are not damaging to generality: p has no multiple factor (p is square free) and p has no factor independent of y_1 (the content of p according to y_1 is in $\mathcal{K}$). We shall say that p is *regular*. Then $s = \frac{\partial p}{\partial y_1}$ has no common factor with p.

Just as we named $y_1 = \frac{\mathrm{d}y_0}{\mathrm{d}x}$, we can also set

$$y_2 = \frac{\mathrm{d}^2 y_0}{\mathrm{d}x^2}, \quad y_3 = \frac{\mathrm{d}^3 y_0}{\mathrm{d}x^3}, \cdots$$

N.1 Computing the differential basis of the general component

We gave in Section G.1 a definition of the general solution. Consider a differential polynomial p and its separant s. The general solution is defined by the general component of p, $\mathcal{G}_p = \{p\} : s$, which is a prime differential ideal when p is irreducible. When p is regular, the general solutions can also be defined by the differential radical ideal $\{p\} : s$, the essential components of which are all essential in the decomposition of $\{p\}$: if $p = \prod_{i=1}^{r} p_i$ is the factorization into irreducible factors and s_i is the separant of p_i then

$$\{p\} : s = \bigcap_{i=1}^{r} \{p_i\} : s_i.$$

We noted in Section H.3 that when p was a first order differential polynomial, we could always compute a differential basis of the general component and we gave a process for that.

In [Coh76] it is shown, in a somewhat more direct way the following theorem.

N.1.1 THEOREM: Let p be a regular differential polynomial of first order in $\mathcal{K}(x)\{y\}$. Let s be its separant and ω be the degree of p in y_1. Let G_ω be a basis of $\langle p, \delta p, \ldots, \delta^{\omega-1}p\rangle : s$ in $\mathcal{K}(x)[y_0, \ldots, y_\omega]$. Then G_ω is a differential basis of $\{p\} : s$.

Note that we need to consider the polynomials $p, \delta p, \ldots, \delta^{\omega-1}p$ as polynomials in the indeterminates $y_0, \ldots, y_\omega$ with coefficient in the field $\mathcal{K}(x)$. It was pointed out in Section E.2 why it is not enough to work with the ring $\mathcal{K}[x]$, as the coefficient ring. This point is the reason why differential algebra is not suited for the analysis of singularity.

To offset this difficulty, we shall lead the computations in $\mathcal{K}[x][y_0, \ldots, y_\omega] = \mathcal{K}[x, y_0, \ldots, y_\omega]$ but with an order on the monomials which makes the results valid in $\mathcal{K}(x)[y_0, \ldots, y_\omega]$. This is a crucial point for the validity of our algorithmic analysis of singular points of the general solution.

x is said to be reverse-prevailing for an order on the monomials of $\mathcal{K}[x, y_0, \ldots, y_\omega]$ if $x^\alpha r > x^\beta t$ whenever r and t are monomials in $\mathcal{K}[y_0, \cdots, y_\omega]$ such that r is greater than t. If G is a Gröbner basis of an ideal I in $\mathcal{K}[x, y_0, \ldots, y_\omega]$ according to an order where x is reverse prevailing, then G is also a Gröbner basis of the ideal generated by I in $\mathcal{K}(x)[y_0, \ldots, y_\omega]$ [BW93, lemma 8.93].

According to Proposition G.1.2, $\langle p, \delta p, \ldots, \delta^{\omega-1}p\rangle : s = (p, \delta p, \ldots, \delta^{\omega-1}p) : s^\infty$. Thus a basis of $(p, \ldots, \delta^{\omega-1}p) : s^\infty$ in $\mathcal{K}(x)[y_0, \ldots, y_\omega]$ will provide a differential basis of the general component of p.

On $\mathcal{K}[x, y_0 \cdots, y_\omega, z]$, a term order $>$ where z prevails is a term order such that $z^\alpha r > z^\beta t$ for any monomials r and t of $\mathcal{K}[x, y_0, \cdots, y_\omega]$ whenever α is greater than β.

N.1.2 PROPOSITION: Let p be a differential polynomial of first order and let ω be the degree of p in y_1 and s its separant. Let G'_ω be a Gröbner basis of $(s\,z - 1, p, \delta p, \ldots, \delta^{\omega-1}p)$ in $\mathcal{K}[x, y_0, \ldots, y_k, z]$ according to an order where x is reverse prevailing and z prevails. $G_\omega = G'_\omega \cap \mathcal{K}[x, y_0, \ldots, y_k]$ is a differential basis of the general component of p.

Because then, G_ω is a Gröbner basis of the saturation ideal $(p, \delta p, \ldots, \delta^\omega p) : s^\infty$ in $\mathcal{K}[x, y_0, \ldots, y_\omega]$ according to the induced term order [BW93, 6.2]. For this latter term order, x is still reverse prevailing, and therefore G_ω is a basis of $(p, \delta p, \ldots, \delta^\omega p) : s^\infty$ in $\mathcal{K}(x)[y_0, \ldots, y_\omega]$.

N.2 Integral power series solutions

Assume we have a formal power series solution of the differential equation $p(x, y_0, y_1) = 0$:

$$\tilde{y}_0(x) \;=\; y_0^o + (x - x^o)\, y_1^o + \frac{(x - x^o)^2}{2}\, y_2^o + \cdots = \sum_{i \geq 0} \frac{(x - x^o)^i}{i!} y_i^o \qquad (1)$$

where x^o, y_i^o belong to a field extension $\mathcal{K}'$ of $\mathcal{K}$. This means that p vanishes when substituting y_0 by $\tilde{y}_0(x)$ and y_1 by its formal derivative

$$\tilde{y}_1(x) = y_1^o + (x - x^o)\, y_2^o + \cdots = \sum_{i \geq 0} \frac{(x - x^o)^i}{i!} y_{i+1}^o.$$

Then (x^o, y_0^o, y_1^o) is an *algebraic zero* of p: $p(x^o, y_0^o, y_1^o) = 0$.

Consider the derivative of the differential equation $p(x, y_0, y_1) = 0$ according to x :

$$\delta p = \frac{\partial p}{\partial y_1}\, y_2 + \frac{\partial p}{\partial y_0} y_1 + \frac{\partial p}{\partial x}.$$

Then $(x^o, y_0^o, y_1^o, y_2^o)$ is a zero of the ideal $\langle p, \delta p \rangle$ in $\mathcal{K}[x, y_0, y_1, y_2]$.

Likewise, $(x^o, y_0^o, \ldots, y_k^o)$ is a zero of the ideal $\langle p, \delta p, \ldots \delta^{k-1} p \rangle$ in $\mathcal{K}[x, y_0, y_1, \ldots, y_k]$.

Now

$$\langle p, \delta p, \ldots \delta^{k-1} p \rangle = \langle p, \delta p, \ldots \delta^{k-1} p \rangle : s \;\cap \langle s, p, \delta p, \ldots \delta^{k-1} p \rangle$$

where $s \notin \langle p, \delta p, \ldots \delta^{k-1} p \rangle : s$.

If the formal power series (1) is a singular solution,

$$s\left(x, \tilde{y}(x), \frac{\mathrm{d}\tilde{y}}{\mathrm{d}x}(x)\right) = 0,$$

then $(x^o, y_0^o, \ldots, y_k^o)$ is a zero of $\langle s, p, \delta p, \ldots \delta^{k-1} p \rangle$. Otherwise $(x^o, y_0^o, \ldots, y_k^o)$ is a zero of $\langle p, \delta p, \ldots \delta^{k-1} p \rangle : s$.

Note that for $k = 1$, we have $\langle p \rangle : s = (p)$ because p is regular. Thus $\langle p \rangle : s \subset \langle s, p \rangle$. For $k > 1$, we can still have

$$\langle p, \delta p, \ldots \delta^{k-1} p \rangle : s \subset \langle s, p, \delta p, \ldots \delta^{k-1} p \rangle.$$

This means that for some initial condition x^o, y_0^o, on the singular solution, the singular solution and the non-singular solutions have at least a k^{th} order contact, that is they have the same k first derivatives.

If the singular solution is essential, the non-singular solutions and the singular solutions must split from one another for some k. According to Theorem N.1.1, this happens for $k = \omega$, the degree of p in y_1. Then

$$\langle p, \delta p, \ldots \delta^{\omega-1} p \rangle : s \not\subset \langle s, p, \delta p, \ldots \delta^{\omega-1} p \rangle.$$

N.3 Non singular power series solutions

Consider a differential equation of k^{th} order

$$q(x, y_0, \ldots, y_k) = 0.$$

The separant of such an equation is $\dfrac{\partial q}{\partial y_k}$. At a point $(x^o, y_0^o, \ldots, y_k^o)$ that is a zero of q but that is not a zero of the separant of q, the differential equation is locally equivalent to an explicit differential equation (according to the implicit function theorem). By Cauchy theorem, there thus exists a unique analytic solution. The points $(x^o, y_0^o, \ldots, y_k^o)$ which are the common zeros of q and its separant are here again the singular points of the differential equation $q(x, y_0, \ldots, y_k) = 0$.

A basis of the general solution of $p(x, y_0, y_1) = 0$ consists of differential equations of order greater than one. Nonetheless, as is set forth in the following example, we cannot define the set of singular points of the general solution simply as the intersection of the singular points of the elements of the differential basis. We need to undergo a proper extension process.

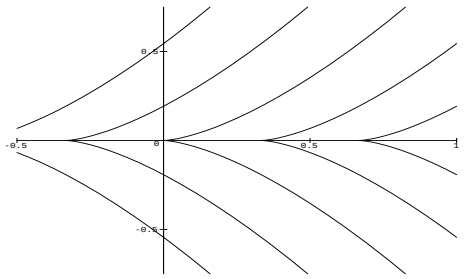
N.3.1 Example: Consider the equation $p = 8\,y_1^3 - 27\,y_0 = 0$. The locus of singular points is $y_0, y_1 = 0$. It forms up a singular solution $\bar{y}(x) = 0$. The degree of p in y_1 is $\omega = 3$ and therefore a differential basis of the general component of p is given by a basis of

$$\langle p, \delta p, \delta^2 p\rangle : s = \langle 8\,y_1^3 - 27\,y_0, 3\,y_0\,y_2 - y_1^2, 8\,y_1\,y_2 - 9, 9\,y_3 + 8\,y_2^3\rangle.$$

The general component contains the differential polynomial $8\,y_1\,y_2 - 9$ and thus $\bar{y}(x) = 0$ is not an essential singular solution. The general solution consists only of the non-singular solutions. Furthermore, these solutions satisfy $9\,y_3 + 8\,y_2^3$ that has no singular point. Yet the general solution can be given as the algebraic function

$$(\tilde{y}(x))^2 = (x - a)^3.$$

These solutions have an infinite second derivative.



N.3.2 DEFINITION: Let $p(x, y_0, y_1) = 0$ be a differential equation of first order, the degree in y_1 being ω. A zero $(x^o, y_0^o, \ldots, y_w^o)$ of $\langle p, \delta p, \ldots, \delta^{\omega-1} p\rangle : s$ will be called a singular point of the general solution if it provides no Cauchy condition to any differential equation associated to a polynomial in $\langle p, \delta p, \ldots, \delta^{\omega-1} p\rangle : s$.

To determine the set of singular points of the general solution, we shall proceed as follow. We start of any point (x^o, y_0^o) in $\bar{\mathcal{K}}^2$ and we seek under which condition a converging power series solution can be found at this point.

We primarily need to determine when the ω first coefficients y_k^o can be found. We shall achieve that with the well known Extension theorem.

The next stage is to determine which zeros of $\langle p, \delta p, \ldots, \delta^{\omega-1} p\rangle : s$ provide a Cauchy condition for one of the differential equation in the basis of the general solution.

The Extension theorem

This theorem, its proof and related considerations can be found in many text-books. See for instance [CLD92].

N.3.3 THEOREM: Let I be the ideal generated by some $g_1, \ldots, g_l \in \mathcal{K}[z_1, \cdots, z_m, z]$. Let J be the elimination ideal of I according to z: $J = I \cap \mathbb{Q}[z_1, \cdots, z_m]$. For each $1 \leq i \leq l$ write g_i in the form :

$$g_i = q_i(z_1, \ldots, z_m)\, z^{N_i} + \quad \text{terms of degree } < N_i \text{ in z},$$

where $N_i \geq 0$ and g_i is non-zero.

Suppose $(a_1, \ldots, a_m) \in \bar{\mathcal{K}}^m$ is a zero of J. We call it a partial solution. If at least one of the q_i does not vanish for $(a_1, \cdots, a_m)$ then there exists $a \in \bar{\mathcal{K}}$ such that $(a_1, \ldots, a_m, a)$ is a zero of I.

Note that we only have a sufficient condition for the extension step to work: the partial solution must not be on the algebraic variety of the leading coefficients, $\mathcal{V}(q_1, \ldots, q_l)$. Moreover the q_i depend on the given basis $g_1, \ldots, g_l$ of I.

But if $g_1, \cdots, g_l$ is a Gröbner basis of I according to an order where z prevails the z-homogenization of the g_i will give a basis of the z-homogenization I^h of I. The projective variety of I^h is the projective closure of the affine variety of I. Therefore if a partial solution $(a_1, \ldots, a_m)$ makes all the leading coefficient q_i vanish, there is at least one way to extend this solution with an infinite value for z.

Extension process

We thus wish to find the maximal set of initial conditions that we can extend to a zero of $(p, \ldots, \delta^{\omega-1}p) : s^\infty$. To this aim, we shall compute first a Gröbner basis G_ω of $(p, \ldots, \delta^{\omega-1}p) : s^\infty$ in $\mathcal{K}[x, y_0, \ldots, y_\omega]$ according to a lexicographical order $x < y_0 < y_1 < \ldots < y_\omega$. With such an order, G_ω will also be a Gröbner basis in $\mathcal{K}(x)[y_0, \ldots, y_\omega]$ according to the lexicographical order where $y_0 < y_1 < \ldots < y_\omega$. Furthermore $G_\omega \cap \mathcal{K}[x, y_0, \ldots, y_k]$ is Gröbner basis of

$$(p, \ldots, \delta^{k-1}p) : s^\infty = (p, \ldots, \delta^{\omega-1}p) : s^\infty \cap \mathcal{K}[x, y_0, \ldots, y_k],$$

for all $1 \leq k \leq \omega$. Therefore, we can read out of G_ω the successive Gröbner basis G_k of the ideal $(p, \ldots, \delta^{k-1}p) : s^\infty$, according to the induced orders on $\mathcal{K}[x, y_0, \ldots, y_k]$.

This has the form :

$$G_\omega \left\{ \begin{array}{l} G_3 \left\{ \begin{array}{l} G_2 \left\{ \begin{array}{ll} G_1 & \left\{ \; g_1^1 = q^1(x, y_0) y_1^m + \ldots \right. \\ g_1^2 = & q_1^2(x, y_0, y_1) y_2^{N_1} + \cdots \\ \vdots & \\ g_i^2 = & q_i^2(x, y_0, y_1) y_2^{N_i} + \cdots \end{array} \right. \\ g_1^3 = \; q_1^3(x, y_0, y_1, y_2) y_3^{N_{i+1}} + \cdots \\ \vdots \end{array} \right. \\ \quad \ldots \\ \vdots \\ g_k^\omega = \; q_k^\omega(x, y_o, \ldots, y_{m-1}) y_m^{N_r} + \cdots \end{array} \right.$$

where $g_1^1 = p$.

We give the following notations: for some $2 \leq r \leq \omega$, $\mathbf{g}^r$ will be the set of polynomials in $G_r \backslash G_{r-1} = \{g_r^l\}_l$, and $\mathbf{q}^r$ the set of leading coefficients of the extension theorem:

$$\mathbf{q}^r = \left(\bigcup_{l=1,r-1} \mathbf{g}^l \right) \cup \{q_l^r\}_l.$$

- provided (x^o, y_0^o) is not a root of q^1, y_1^o can be found in $\bar{K}$ such that (x^o, y_0^o, y_1^o) is a zero of p, that is a zero of G_1.
- (x^o, y_0^o, y_1^o) extends to a zero $(x^o, y_0^o, y_1^o, y_2^o)$ of G_2 if $(x^o, y_0^o, y_1^o) \notin \mathcal{V}(\mathbf{q}^2)$.

Taking similar successive steps we will find the conditions under which (x^o, y_0^o) can be extended to a zero $(x^o, y_0^o, y_1^o, \ldots, y_\omega^o)$ of G_ω. The set of points where an extension is not possible is

$$\mathcal{S}_\omega = \bigcup_{r=1}^{\omega} \mathcal{V}(\mathbf{q}^r) = \mathcal{V}\left(\bigcap_{r=1}^{\omega} (\mathbf{q}^r)\right).$$

These points are singular points of the general solution.

We shall point out that if a partial solution $(x, y_0^o, \ldots, y_{k-1}^o)$ is in $\mathcal{V}(\mathbf{q}^k)$, it does not mean that there is no power series solution extending it. It just means that there is a way to extend it with an infinite y_k^o.

Let $q_l^{\omega+1}$ denote the partial derivatives of g_l^ω w.r.t. y_ω. A point of $\mathcal{V}(G_\omega)\backslash\mathcal{S}_\omega$ for which at least one of the $q_l^{\omega+1}$ does not vanish is a regular point of the general solution: the differential polynomial the separant of which, the $q_l^{\omega+1}$, does not vanish is endowed with a Cauchy initial condition. There thus exists a convergent power series solution extending this initial condition taken on $\mathcal{V}(G_\omega)$.

Conversely, if they all vanish, it does not mean that there is no power series solution extending it, just as it is the case when you consider a single equation. But the singular points thus defined are proper to the general solution.

N.3.4 Proposition: Consider $p(x, y_0, y_1) = 0$ a first order differential equation. Assume ω is the degree of p in y_1. Let G_ω be a Gröbner basis of $(p, \delta p, \ldots, \delta^{\omega-1}p)$ in $\mathcal{K}[x, y_0, \ldots, y_\omega]$ according to a lexicographic order such that $x < y_0 < \ldots < y_\omega$. If the $\mathbf{q}^r$, $1 \leq r \leq \omega + 1$ are defined as previously on this basis, then the set of singular points of the general solution is

$$\bigcup_{r=1}^{\omega+1} \mathcal{V}(\mathbf{q}^r) = \mathcal{V}\left(\bigcap_{r=1}^{\omega+1} (\mathbf{q}^r)\right).$$

Indeed, if a differential polynomial belongs to $\langle p, \delta p, \ldots, \delta^k p\rangle : s$, for $k < \omega - 1$, its derivative belongs to $\langle p, \delta p, \ldots, \delta^{k+1} p\rangle : s$. Its separant is the leading coefficient of its derivative.

N.3.5 Example: Consider the differential equation

$$p \;=\; x^2\, y_1^2 + 2\, x\, y_0\, y_1 + y_0^2 - 4x^2\, y_0 \;=\; 0.$$

$s = \dfrac{\partial p}{\partial y_1} = 2x(xy_1 + y_0)$ and the resultant of p and s is $r = 16x^6 y_0$.

Thus for initial conditions $(x^o, y_0^o) \in \mathbb{C}^2$ where $y_0^o \neq 0$ and $x \neq 0$, a root y_1^o of $p(x^o, y_0^o, y_1) = 0$ is finite and such that (x^o, y_0^o, y_1^o) is a regular point of the differential equation. We can develop the solution into a converging power series. We are going to show that the initial condition (x^o, y_0^o) can be extended into a

converging power series solution under the less restrictive assumption that only $x^o \neq 0$.

Note that the algebraic variety of $\langle p, s\rangle$ has two components

$$\langle p, s\rangle \quad = \quad \langle x, y_0\rangle \cap \langle y_0, y_1\rangle$$

$x, y_0 = 0$ is a contact singular point while $y_0, y_1 = 0$ corresponds to a singular solution $\bar{y}(x) = 0$.

A differential basis of the general solution is given by a basis G_2 of $\langle p, \delta p\rangle : s = (p, \delta p) : s^\infty$.

A Gröbner basis of $(p, \delta p) : s^\infty$ in $\mathcal{K}[x, y_0, y_1, y_2]$ according to a lexicographic order such that $y_2 > y_1 > y_0 > x$ is a differential basis of the general solution. This is computed with MapleV.3.

$$\begin{aligned}(p, \delta p) : s^\infty \quad = \quad & (\ \mathbf{2x^2}\, y_2 + 3\, x\, y_1 - y_0 - 4\, x^2, \\ & \mathbf{2x\, y_0}\, y_2 + x y_1^2 + 5\, y_0\, y_1 - 8 x\, y_0, \\ & (\mathbf{5x\, y_1} + \mathbf{y_0})\, y_2 + 8\, y_1^2 - 10\, x\, y_1 - 4\, y_0, \\ & \mathbf{2y_0^2}\, y_2 - 5\, x\, y_1^3 - 9\, y_0\, y_1^2 + 20\, x\, y_0\, y_1 - 8\, y_0^2, \\ & \mathbf{x^2} y_1^2 + 2\, x\, y_0\, y_1 + y_0^2 - 4\, x^2\, y_0\ \ )\,.\end{aligned}$$

The bold terms correspond to the leading coefficients.

In virtue of theorem N.3.3, given the initial condition (x^o, y_0^o), we may find $y_1^o \in \mathbb{C}$ a root of $p(x^o, y_0^o, y_1)$ provided $x^o \neq 0$.

For finding y_2^o we need to look at the algebraic variety of the leading coefficient of y_2.

$$\langle p,\ 2\, y_0^2,\ 5\, x\, y_1 + y_0,\ 2\, x\, y_0, 2\, x^2\rangle = (x,\ y_0).$$

Note that it corresponds to the contact singular point. According to the Extension theorem, for a given zero of p, (x^o, y_0^o, y_1^o) such that $(x^o, y_0^o) \neq (0, 0)$ we may find $y_2^o \in \mathbb{C}$ such that $(x^o, y_0^o, y_1^o, y_2^o)$ is a zero of $(p, \delta p) : s^\infty$.

Thus, up to now, the set of singular point of the general solution consists of $(x, y_0) = (0, 0)$. Besides, the singular locus of $\mathbf{2x^2}\, y_2 + 3\, x\, y_1 - y_0 - 4\, x^2 = 0$ consist exactly of the points such that $x = 0, y_0 = 0$.

Note that a zero (x^o, y_0^o, y_1^o) of p satisfies $(x^o, y_0^o) \neq (0, 0)$ as soon as $x^o \neq 0$. Therefore, if $x^o \neq 0$, we can find a zero $(x^o, y_0^o, y_1^o, y_2^o) \in \bar{K}^4$ of $(p, \ldots, \delta p) : s^\infty$ and further a converging power series non-singular solution which begins as

$$\tilde{y}(x) = y_0^o + (x - x^o) y_1^o + \frac{(x - x^o)}{2}\, y_2^o + \cdots$$

Let us take an initial condition on the singular solution: $y_0^o = 0$. We must chose $x^o \neq 0$ and $y_1^o = 0$. With such an initial condition there is only one polynomial in

y_2 which does not vanish: $q = 2x^2y_2+3x\,y_1-y_0-4x^2$. Thus $y_2^o = 2$. Differentiating q we will get y_3^o : $\delta q = 2\,x^2\,y_3 + 7\,x\,y_2 + 2\,y_1 - 8\,x$. Consequently $y_3^o = -\frac{3}{x^o}$.

Carrying on that way we find the formal power series solution around the point $(x^o, 0)$:

$$\tilde{y}(x) = (x-x^o)^2 - \frac{(x-x^o)^3}{x^o} + \frac{23(x-x^o)^4}{48(x^o)^2} - \frac{15(x-x^o)^5}{22(x^o)^3} + \frac{533(x-x^o)^6}{1152(x^o)^4} + \cdots .$$

Besides, we can check that $\tilde{y}(x) = \frac{4}{9}x^2$ is a smooth solution in the neighborhood of $x^o = 0$. But note that the general solution is given by

$$\tilde{y}_b(x) = \frac{4}{9}x^2 + \frac{9}{16}\frac{b^2}{x} + b\sqrt{x}$$

where b is an arbitrary constant. When b is not zero, the solution has an infinite tangent at the origin.

Bibliography

[Arnon] V.I. Arnold. *Geometrical Methods in the Theory of Ordinary Differential Equations*. A series of Comprehensive Studies in Mathematics. Springer-Verlag, 1988, second edition.

[BB56] C.A. Briot and J.C. Bouquet. Propriétés des fonctions définies par des équations différentielles. *Journal de l'Ecole Polytechnique*, 36:133–198, 1856.

[BLOP95] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In A.H.M. Levelt, editor, *ISSAC'95*. ACM Press, 1995.

[Bou94] F. Boulier. *Etude et Implantation de Quelques Algorithmes en Algèbre Différentielle*. PhD thesis, Université de Lille, 1994.

[Bou96] F. Boulier. Some improvements of a lemma of Rosenfeld. *Submitted to AAECC*, 1996.

[Bou97] F. Boulier. Computing representations for radicals of finitely generated differential ideals. In preparation, 1997.

[BP94] D. Bini and V. Pan. *Polynomial and Matrix Computations*, volume Volume I - Fundamental Algorithm of *Progress in Theoretical Computer Science*. Birkhaüser, 1994.

[BW93] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra*. Springer-Verlag, 1993.

[Can93a] J. Cano. An extension of the Newton-Puiseux polygon construction to give solutions of pfaffian forms. *Ann. Inst. Fourier, grenoble*, 43(1):125–142, 1993.

[Can93b] J. Cano. On the series defined by differential equations, with an extension of the Puiseux polygon construction to these equations. *International Journal of Analysis and its Application*, 1993.

[CLD92] D. Cox, J. Little, and D.O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag, 1992.

[Coh41] R. Cohn. On the analog for differential eqaution of the Hilbert-Netto theorem. *Bulletin of the American mathematical Society*, 47:268–270, 1941.

[Coh76] R. Cohn. The general solution of a first order differential polynomial. *Proceedings of the American Mathematical Society*, 55(1):14–16, 1976.

[Dar75] L. Dara. *Singularités génériques des équations différentielles multiformes*. PhD thesis, Université Louis Pasteur - Strasbourg, 1975.

[Dio89] S. Diop. *Théorie de l'élimination et principe du modèle interne en automatique*. PhD thesis, Université de Paris Sud, 1989.

[Fin89] H.B. Fine. On the functions defined by differential equations with an extension of the Puiseux polygon construction to these equations. *American Journal of mathematics*, 1889.

[GTZ88] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6:149–167, 1988.

[Ham93] M. Hamburger. Ueber die sigulären lösungen der algebraischen differenzialgleichnungen erster ordnung. *Journal für die reine und angewandte Mathematik*, 112:205–246, 1893.

[Hil43] A.P. Hillman. A note on differential polynomials. *Bulletin of the American Mathematical Society*, 49:711–712, 1943.

[Hil52] A.P. Hillman. On the differential algebra of a single differential polynomial. *Annals of mathematics*, pages 157–168, 1952.

[HM62] A.P. Hillman and D.G. Mead. On the Ritt polygon process. *American Journal of Mathematics*, pages 629–634, 1962.

[Hub96] E. Hubert. The general solution of an ordinary differential equation. In *ISSAC'96*. ACM Press, 1996.

[Hub97a] E. Hubert. Detecting degenerate behaviors in first order algebraic differential equations. *Theoretical Computer Science, special issue on Computer Algebra*, 187, 1997. To appear.

[Hub97b] E. Hubert. Essential components of an algebraic differential equation and the computation of their differential bases. Preprint, January 1997.

[IY93] S. Izumiya and J. Yu. How to define singular solutions. *Kodai Mathematical Journal*, 16:227–234, 1993.

[Kol65] E.R. Kolchin. Singular solutions of algebraic differential equations and a lemma of Arnold Saphiro. *Topology*, 3:309–318, 1965. suppl. 2.

[Kol73] E.R. Kolchin. *Differential Algebra and Algebraic Groups*, volume 54 of *Pure and Applied Mathematics*. Academic Press, 1973.

[KRHM] A. Kandri-Rody, H.Maârouf, and M.Ssafini. Triviality and dimension of a system of algebraic differential equations. *Journal of Symbolic Computations*.

[Lev42] H. Levi. On the structure of differential polynomials and on their theory of ideals. *Transaction of the American Mathematical Society*, 51:532–568, 1942.

[Lev45] H. Levi. The Low power theorem for partial differential equations. *Annals of the Mathematical Society*, 46:113–119, 1945.

[PG97] A. Peladan-Germa. *Tests effectifs de nullité dans les extensions de corps différentiels*. PhD thesis, Polytechnique, 1997.

[Rau33] H.W. Raudenbush. Differential fields and ideals of differential forms. *Annals of Mathematics*, 34:509–517, 1933.

[Rit30] J.F. Ritt. Manifolds of functions defined by systems of algebraic differential equations. *Transaction of the American Mathematical Society*, 32:569–598, 1930.

[Rit36] J.F. Ritt. On the singular solutions of algebraic differential equations. *Annals of Mathematics*, 37(3):552–617, 1936.

[Rit45a] J.F. Ritt. Analytical theory of singular solutions of partial differential equations of the first order. *Annals of Mathematics*, 46(1):120–143, 1945.

[Rit45b] J.F. Ritt. On the manifold of partial differential polynomial equations. *Annals of Mathematics*, 46(1):102–112, 1945.

[Rit66] J.F. Ritt. *Differential Algebra*. Dover Publications, Inc, 1966.

[Ros59] A. Rosenfeld. Specializations in differential algebra. *Transaction of the American Mathematical Society*, 90:394–407, 1959.

[Sei56] A. Seidenberg. An elimination theory for differential algebra. *University of California Publications in Mathematics*, 3(2):31–66, 1956.