ÉCOLE POLYTECHNIQUE

THÈSE

présentée pour obtenir le titre de

DOCTEUR EN SCIENCES
SPÉCIALITÉ : MATHÉMATIQUES

par

Jacques-Arthur WEIL

Constantes et polynômes de Darboux en algèbre différentielle : applications aux systèmes différentiels linéaires.

Soutenue le 15 septembre 1995 devant la commission d'examen :

J.P. RAMIS, Président, Rapporteur

M.F. SINGER, Rapporteur

M. BRONSTEIN,
J. DELLA DORA ,
M. GIUSTI ,
J. MOULIN OLLAGNIER ,
J.M. STRELCYN ,
F. ULMER, Examinateurs

Remerciements

On m'a appris qu'avoir de la chance, c'était de savoir mettre son pied en travers d'une porte avant qu'elle ne se referme. En ce sens, un travail de recherche est une affaire de chance, et particulièrement de rencontres.

Les bouillonnements conceptuels de Jean-Pierre Ramis sont une source intarissable de fascination pour un jeune chercheur ; j'y ai puisé beaucoup d'idées et d'enthousiasme. C'est donc pour moi un très grand honneur qu'il ait accepté de rapporter sur ma thèse et d'en présider le jury.

Michael Singer m'a encouragé depuis les balbutiements de ce travail ; j'ai été très heureux qu'il accepte de le lire en détail et d'écrire un rapport, et je le remercie encore de ses très nombreux commentaires. Les spécialistes reconnaîtront dans cette thèse l'énorme influence de ses idées, de son humanisme et (peut-être, j'espère) de la beauté de ses articles.

Jean Moulin Ollagnier a dirigé ce travail et canalisé mes délires utopiques avec une bienveillance rare. Je ne serais certainement pas allé bien loin sans ses incessantes suggestions et demandes de clarification. Il m'a aussi appris que répondre à la question "qu'est-ce que résoudre" apporte beaucoup d'indications sur les moyens de donner une réponse effective à la question "comment résoudre".

Félix Ulmer a consacré une substantielle partie de son temps a répondre aux nombreuses questions souvent naïves ou maladroites dont je l'ai bombardé depuis quelques années. Il m'a aussi donné la chance de travailler avec lui sur les équations du second ordre, ce qui reste une expérience exceptionnelle.

Marc Giusti m'a accueilli dans son laboratoire où il a su instaurer de superbes conditions de travail, d'un point de vue tant humain que matériel. Il m'a aussi fait bénéficier de ses exigences scientifiques, souvent passionnées et toujours stimulantes.

Mes nombreux contacts avec Manuel Bronstein m'ont bien aidé à dissiper le brouillard qui entoure une recherche débutante ; notamment, cela m'a permis de mieux identifier les algorithmes réellement "efficaces" parmi ceux existant pour l'étude des équations différentielles algébriques. Je le remercie aussi d'avoir lu (et corrigé) presque tout ce que j'ai pu écrire.

Jean Della Dora m'a initié à sa conception visionnaire de la recherche à travers ses cours théâtraux et le beau sujet qu'il m'a proposé pour mon D.E.A ; c'est donc un grand plaisir pour moi qu'il soit venu participer à mon jury.

Enfin, Jean-Marie Strelcyn est un expert *es* polynômes de Darboux et j'ai été heureux qu'il vienne prendre dans ce jury la place qui lui revenait naturellement.

Je devrais maintenant citer un par un tous les membres du centre de calcul formel de l'école Polytechnique dans ces remerciements.

La maestria avec laquelle Nicole Dubois et Joël Marchand administrent cette équipe leur vaudrait à elle seule une place à part. Qu'il me soit aussi permis de remercier Nicole de son attentive et chaleureuse gentillesse, et Joël de sa faculté de répondre quasi-instantanément à toute question (parfois même avant qu'elle ne soit posée).

François Ollivier et Marc Chardin m'ont souvent fait profiter de leurs lumières (respectivement en algèbre différentielle et en algèbre commutative) et de leurs encouragements face au doute. De tels encouragements sont parfois aussi venus du centre de mathématiques, particulièrement d'Olivier Piltant et de l'humour ravageur d'Éric Boix.

Vincent Cossart, Brigitte Chauvin, et Guillermo Moreno m'ont initié, à Versailles, à un plaisir d'enseigner qui ne s'est pas démenti depuis.

Et puis j'ai partagé avec beaucoup de bonheur le bureau, les humeurs, et les espoirs d'Albert Shih et de la très pétillante Ariane Péladan-Germa.

Je l'ai dit, ce travail s'est nourri d'innombrable rencontres dans mille endroits inattendus. Que tous leurs protagonistes reçoivent ici mes remerciements pour tous ces échanges miraculeux qui font le sel de la recherche. Je voudrais plus particulièrement saluer très chaleureusement :

Didier Hirsch, Jacques Glowinsky, Olivier Chapuis, Bruno Salvy, Mark van Hoeij et Élie Compoint, qui m'ont bien fait avancer à diverses étapes de ce travail ;

Marius van der Put, Arjeh Cohen, Fritz Beukers, et Ton Levelt, qui m'ont fait l'honneur et le plaisir de m'inviter à Groningen après cette thèse, et qui m'ont fait bénéficier de leurs grandes connaissances durant sa préparation ;

Bob Caviness pour ses encouragements et ses conseils sur la méthode de Darboux ;

Vladimir Popov, Fokko Du Cloux et Harm Derksen (en plus des sus-cités) qui m'ont éclairés sur quelques aspects de la théorie des représentations ;

Et puis Kim et mon entourage dont la présence fut salvatrice, tant les émotions sont fondatrices de la raison.

Sommaire

I : Constantes et polynômes de Darboux en algèbre différentielle

III : Équations différentielles linéaires du second ordre

IV : Annexes

Introduction

On cherche depuis bien longtemps à résoudre des équations différentielles, le mot "résoudre" prenant d'ailleurs une variété considérable de sens différents dans la littérature.

Je travaillerai ici dans le cadre de l'algèbre différentielle. Le premier sens que je donnerai au mot "résoudre" est de chercher à classer les solutions d'une équation donnée par leur degré de transcendance : étant donnée une équation différentielle à coefficients, disons, dans $\mathbb{C}(x)$, on voudrait savoir si ses solutions satisfont des équations différentielles d'ordre plus petit.

Il n'existe pas de méthode générale pour décider si une équation différentielle admet des solutions d'ordre plus petit. Une stratégie classique est alors de chercher des intégrales premières de l'équation. Mais, là encore, il n'y a pas d'algorithme général pour décider si une équation différentielle (ou un système) admet des intégrales premières d'un type donné (par exemple rationnelles). On utilise donc des heuristiques. Je me concentrerai ici sur une méthode introduite par Darboux pour la recherche d'intégrales premières de champs de vecteurs du plan. La préoccupation sous-jacente est l'effectivité, c'est à dire que je chercherai à rendre les calculs les plus automatiques possible pour pouvoir les faire réaliser par un système de calcul formel*. En particulier, on verra que cette méthode donne des résultats intéressants pour les systèmes différentiels linéaires à coefficients rationnels.

Dans le reste de cette introduction, je vais présenter la méthode de Darboux et décrire rapidement le contenu de cette thèse ; je discuterai aussi la place qu'a occupé l'implantation dans ce travail.

Les trois parties devraient pouvoir être lues de manière indépendante (le début de chaque partie contient les rappels nécessaires à sa lecture). Chaque chapitre est précédé d'un résumé détaillé.

La méthode de Darboux

Soient $P, Q \in \mathbb{C}[x, y]$ deux polynômes, et l'équation (E) : $P(x, y)y' = Q(x, y)$. Pour Darboux, résoudre consiste à chercher une fonction $f(x, y)$ telle que, si $y(x)$ est une solution de l'équation, alors $f(x, y(x)) = c \in \mathbb{C}$ pour tout x ; cela revient à considérer la dérivation

* Mes algorithmes sont implantés dans le système MAPLE et disponibles auprès de l'auteur ou sur le réseau Internet à l'adresse `http://medicis.polytechnique.fr/gage/weil.html`.

en les solutions de (E), notée $D = P(x,y)\frac{\partial}{\partial x} + Q(x,y)\frac{\partial}{\partial y}$, et à chercher une fonction $f(x,y)$ telle que $Df = 0$. On dit qu'une telle fonction f est une intégrale première de l'équation.

Dans son mémoire [Darboux], l'éminent géomètre s'intéresse aux intégrales premières rationnelles : il cherche $f \in \mathbb{C}(x,y)$ telle que $Df = 0$. Supposons que f s'écrit $f = \frac{N}{M}$ où M et N sont des polynômes premiers entre eux. Remarquant que D est une dérivation de l'anneau $\mathbb{C}[x,y]$, Darboux caractérise M et N de la manière suivante :

$$Df = 0 \Longleftrightarrow D(N).M - N.D(M) = 0 \Longleftrightarrow \exists \alpha \in \mathbb{C}[x,y] \text{ tel que } \begin{cases} D(M) = \alpha M \\ D(N) = \alpha N \end{cases}$$

On dit de nos jours que M et N sont des *polynômes de Darboux* pour D, ce qui signifie qu'ils divisent leur dérivée par D dans l'anneau $\mathbb{C}[x,y]$.

Darboux met alors en évidence les quatre propriétés fondamentales suivantes :

1 Un polynôme est de Darboux si et seulement si tous ses facteurs irréductibles sont de Darboux.
2 Si F est un polynôme de Darboux, si y est une fonction vérifiant $F(x,y(x)) = 0$, et si $\frac{\partial F}{\partial y}(x,y(x)) \neq 0$, alors $P(x,y)y' = Q(x,y)$.
3 L'équation admet une intégrale première rationelle si et seulement si elle admet une infinité de polynômes de Darboux premiers entre eux.
4 Pour une équation $P(x,y)y' = Q(x,y)$, le degré des polynômes de Darboux irréductibles est borné.

Ces résultats ont donné lieu à de très nombreuses études. Dans [Jou79], Jouanolou ramène ces résultats à l'étude de formes de Pfaff algébriques homogènes à trois variables, et les généralise à des formes de Pfaff en un nombre arbitraire de variables. Mais, étonnament, il n'existe pas une telle généralisation à des champs de vecteurs en un nombre arbitraire de variables : c'est l'objet du premier chapitre que d'étudier dans quelle mesure les quatre propriétés ci-dessus sont valides (ou non) pour un champs de vecteurs polynomial quelconque. Toute la suite consistera a appliquer ces idées à l'étude des systèmes différentiels linéaires.

Chapitre I : Constantes et polynômes de Darboux

Dans ce chapitre, nous commençons par rappeler quelques notions d'algèbre différentielle, ce qui nous permet de définir précisément ce que nous entendons par solution d'équation différentielle. Nous indiquons ensuite un critère dû à Kolchin qui formalise algébriquement le lien entre intégrales premières (ou constantes transcendantes) et solutions (page 17).

On peut définir, abstraitement, les polynômes de Darboux de la manière suivante. Soit k un corps différentiel de caractéristique zéro (par exemple $k = \mathbb{C}(x)$), et soit D une dérivation

de $k[Y_1, \ldots, Y_n]$; on dit que $F \in k[Y_1, \ldots, Y_n]$ est un élément de Darboux pour D s'il existe $\alpha \in k[Y_1, \ldots, Y_n]$ tel que $DF = \alpha F$.

Par analogie avec la description ci-dessus de l'approche de Darboux, nous considèrons des dérivations D en les solutions d'un champs de vecteurs sur k (ou d'une équation différentielle quasi-linéaire). Les polynômes de Darboux correspondent alors à des variétés de codimension 1 invariantes sous l'action du champs.

Nous indiquons une stratégie de calcul et montrons quelques propriétés des polynomes de Darboux, notamment le résultat de rationalité suivant (page 23) :

Proposition 15. *Soit $K \supset k$ une extension algébrique finie de k. Soit D une dérivation de $k[Y_1, \ldots, Y_n]$ et D_K son extension à K. Alors, D_K admet un polynôme de Darboux non-trivial dans $K[Y_1, \cdots, Y_n]$ si et seulement si D admet un polynôme de Darboux non-trivial dans $k[Y_1, \cdots, Y_n]$.*

Soit $P(y, y', \ldots, y^{(n)}) = 0$ une équation différentielle quasi-linéaire, et D la dérivation en les solutions de P. Nous montrons page 25 le lien entre polynômes de Darboux de D et solutions de P (ce qui généralise la propriété 2 de Darboux et rafine le critère de Kolchin pour ce cas) :

Théorème 17. *Soit F un polynôme de Darboux d'ordre $n-1$ pour D. Alors, tout zéro non-singulier η de F est un zéro de P.*
Réciproquement, si P admet un zéro η d'ordre $n-1$, alors le polynôme minimal F de η est un polynôme de Darboux pour D.

Nous étudions ensuite le cas des champs de vecteurs du plan où nous rappelons les résultats de Darboux et Prelle-Singer ; nous proposons, grâce à un lemme de Collins et Christopher qui caractérise les polynômes de Darboux de dérivations homogènes à deux variables, une méthode de calcul des polynômes de Darboux dans ce cas.

Pour des champs de vecteurs généraux, nous montrons page 32 (en étendant une preuve de Singer) que la donnée de suffisamment de polynômes de Darboux est équivalente à la présence d'une intégrale première rationnelle (c'était la propriété 3 de Darboux) :

Proposition 25. *Soit $d = \max(\deg(Q_i))$. Alors D admet $\binom{n+d-1}{n} + n$ polynômes de Darboux premiers entre eux si et seulement si D admet une intégrale première rationelle.*

Nous montrons aussi que la propriété 4 de Darboux ne se généralise pas, i.e le degré des polynômes de Darboux irréductibles n'est pas borné en général. Nous indiquons alors des

directions de recherche pour lever cet obstacle. Certains résultats de ce chapitre sont parus dans [Wei94].

Chapitre II : Systèmes différentiels linéaires

Dans ce chapitre, qui est le noyau de ce travail, nous étudions les intégrales premières rationnelles et liouvilliennes des systèmes différentiels linéaires homogènes non autonomes. Soit le système

$$(A) : \qquad Y' = AY \quad \text{avec} \quad A \in \mathcal{M}_{n,n}(k) \tag{0.1}$$

Comme plus haut, on définit la dérivation en les solutions de (A)

$$D = \partial_k + A_1 Y \frac{\partial}{\partial y_1} + A_2 Y \frac{\partial}{\partial y_2} + \ldots + A_n Y \frac{\partial}{\partial y_n}$$

et les polynômes de Darboux. Nous montrons pages 40 et 53 qu'un tel système a une intégrale première liouvillienne si et seulement si il admet un polynôme de Darboux homogène (**proposition 31**) ; nous considérons dans ce qui suit que tous les polynômes de Darboux sont homogènes.

Pour de tels systèmes, on dispose d'une "théorie de Galois" analogue à celle qui existe pour les polynômes. Soit C le corps des constantes de k qu'on suppose algébriquement clos. Les solutions de $Y' = AY$ forment un C-espace vectoriel V. On appelle extension de Picard-Vessiot une extension minimale $K \supset k$ de corps différentiel engendrée par les composantes d'un système fondamental de solutions. Le groupe G des automorphismes de K qui laissent chaque élément de k fixe est appelé le groupe de Galois différentiel. Ce groupe "décrit" les relations différentielles qui existent entre les solutions. De plus, comme chaque élément de G envoie une solution sur une autre solution, G agit sur V, ce qui lui confère une structure de sous-groupe algébrique linéaire de $GL_n(C)$. Il y a une correspondance galoisienne (à chaque sous-corps différentiel de K on peut associer un sous-groupe de G), qui implique entre autres qu'un élément de K est dans k si et seulement si il est fixé par le groupe ; ce point est la clé des implantations.

L'approche géométrique de Chevalley consiste à caractériser un tel groupe par des construction sur V qu'il laisse invariantes. Dans cet esprit, nous montrons (page 42) la proposition suivante, qui nous amène à centrer ce chapitre sur une étude systématique des puissances symétriques de V :

Proposition 33. *Notons $S^m(V)^*$ le dual d'une puissance symétrique de V, et soit $Y' = S^m(A)^*Y$ un système dont l'espace de solutions soit G-isomorphe à $S^m(V)^*$.*
Le système $Y' = AY$ admet un polynôme de Darboux homogène de degré m si et seulement s'il existe f exponentiel sur k (i.e $f'/f \in k$) et un vecteur v à coefficients dans k tels que fv est une solution du système $Y' = (S^m(A)^*)Y$.

Ce résultat nous permet de donner une correspondance bijective entre les invariants (resp. semi-invariants) de la représentation duale du groupe de Galois et les intégrales premières polynomiales (resp. polynômes de Darboux) du système (**théorème 38** page 46). Le problème du degré des polynômes de Darboux devient donc un problème de théorie des représentations. Dans le cas où G est réductif, le même résultat est vrai sans prendre le dual (page 48) :

Corollaire 43. *Supposons que le groupe de Galois G du système $Y' = AY$ est réductif. Alors, à multiplication scalaire près, il y a une bijection entre les polynômes de Darboux du système (resp. les intégrales premières polynomiales) et les semi-invariants (resp. invariants) de G.*

Notre algorithme consiste donc à déterminer des solutions exponentielles de puissances symétriques duales de systèmes (voir aussi la partie implantations dans le chapitre IV) ; nous montrons pour ce faire les avantages qu'on peut tirer de vecteurs non-cycliques dans la transformation des systèmes en équations. Ces résultats sont parus dans [Wei95].

Nous montrons ensuite que les outils classiques qui permettent de construire "automatiquement" des invariants (hessien, jacobien, etc) s'appliquent aux polynômes de Darboux (**proposition 50** page 57). Nous remarquons alors que certains coefficients des polynômes de Darboux donnent explicitement certains semi-invariants (**théorème 52** page 60). Nous en déduisons page 62 une accélération de la méthode de Singer et Ulmer pour le calcul de solutions algébriques d'équations différentielles linéaires, en simplifiant le calcul d'invariants qu'elle requiert.

Enfin, nous consacrons la fin de ce chapitre à la mise au point de plusieurs critères pour décider l'existence de polynômes de Darboux.

III : Équations différentielles linéaires du second ordre

Dans ce chapitre, nous appliquons nos méthodes à la résolution des équations différentielles linéaires du second ordre ; l'essentiel de ce chapitre est un travail commun avec Felix Ulmer, paru dans [UWe94]. Ici, résoudre peut prendre quatre sens : écrire les solutions sous forme une 'explicite' (liouvillienne*), écrire le polynôme différentiel minimal d'une solution, calculer des intégrales premières, ou calculer le groupe de Galois. Le joli résultat est que ces quatre approchent coïncident ici.

Soit $L(y) = y'' + a_1 y' + a_0 y$. Si $u = y'/y$, alors u satisfait l'équation de Riccati $Ri(u) = u' + u^2 + a_1 u + a_0 = 0$. Résoudre sous forme liouvillienne est équivalent à trouver une

* Une solution est *liouvillienne* si on peut l'obtenir par une tour d'extensions différentielles dont chaque étape est obtenu par adjonction d'un élément algébrique, d'une intégrale, ou de l'exponentielle d'une intégrale.

solution algébrique à l'équation de Riccati. Sous quelques hypothèses, Kovacic avait montré que cela se ramenait à calculer un semi-invariant du groupe de Galois (ce qui se fait en cherchant les solutions exponentielles de certaines équations linéaires construites à partir de L, en l'occurrence ses puissances symétriques). Kovacic utilise alors la classification des sous-groupes de $SL_2(C)$ pour établir un bel algorithme ([Kov86]).

Pour améliorer cela, nous montrons comment caractériser *toutes* les solutions de l'équation dans le cas d'un groupe fini (**lemme 72** page 85) ; nous obtenons ensuite (sans les hypothèses de Kovacic) une bijection générale entre les semi-invariants du groupe et les polynômes de Darboux de l'équation de Riccati (**théorème 77** page 88), ce qui produit des solutions algébriques de $Ri(u) = 0$. Ceci nous permet de *choisir* parmi toutes les solutions celles qui sont les plus simples à calculer, en l'occurrence celles qui correspondent à des solutions rationnelles d'équations auxiliaires. En étudiant finement les sous-groupes de $SL_2(C)$, nous en déduisons une variante rationnelle, simple et efficace, de l'algorithme de Kovacic. À titre d'illustration, je montre à la fin du chapitre comment ces techniques permettent de résoudre facilement les équations de Riccati par radicaux (quand c'est possible).

Le rôle de l'implantation

On devine déjà dans ce résumé que l'implantation a joué un rôle crucial dans ce travail.

C'est par exemple une délicate tentative d'implantation qui m'a aidé a identifier précisément les difficultés de l'algorithme de Kovacic et m'a suggéré des directions de recherche pour l'améliorer. Ces améliorations ont ensuite procédé d'un traitement mathématique plus abstrait, parfois éloigné (mais en apparence seulement) de la motivation originale.

Le souci d'effectivité des algorithmes oblige à très sérieusement préciser ce qu'on entend par résoudre et fait entrevoir où sont les réelles difficultés du problème. C'est alors une étude mathématique poussée qui permet de comprendre en profondeur la source de ces difficultés (et en particulier leur caractère intrinsèque ou non). Dans mes travaux sur les systèmes différentiels linéaires, l'implantation est devenue beaucoup plus naturelle et performante une fois que les mathématiques du problème étaient bien comprises.

Enfin, la réalisation de programmes efficaces est un travail à part entière. C'est pourquoi il semble que, bien qu'ils n'apparaissent qu'en annexe du texte, les programmes réalisés (dans le système de calcul formel MAPLE) devraient être compris comme partie intégrante de cette thèse ; c'est aussi pourquoi j'ai inclus de nombreux exemples qui montrent les capacités (et les limites) de mes implantations. Ces dernières ont déjà servi à quelques auteurs ([Ulm94, Com95a]) ; même si ma contribution est d'abord de nature mathématique, je serais aussi heureux si mes programmes permettent d'assister d'autres mathématiciens dans leur travail.

CHAPITRE I

Constantes et polynômes de Darboux en algèbre différentielle

Dans ce chapitre, nous introduisons la méthode de Darboux pour calculer des intégrales premières de systèmes différentiels ordinaires et montrons comment elle s'adapte au cas d'équations différentielles quasi-linéaires. Nous commençons par rappeler quelques notions d'algèbre différentielle et nous définissons ce que nous entendons par solution d'équation différentielle. Nous indiquons ensuite un critère dû à Kolchin qui formalise algébriquement le lien entre intégrales premières et solutions.

Nous introduisons alors les polynômes de Darboux et montrons qu'on peut les calculer sans faire d'extension algébrique du corps de base (proposition 15). Pour le cas des équations quasi-linéaires, nous montrons comment les propriétés des polynômes de Darboux permettent de donner une variante plus forte du critère de Kolchin (théorème 17) et indiquons une stratégie de calcul.

Nous étudions ensuite le cas des champs de vecteurs du plan où nous rappelons les résultats de Darboux et Prelle-Singer ; nous proposons, grâce à un lemme de Collins et Christopher, une méthode de calcul des polynômes de Darboux dans ce cas.

Pour des champs de vecteurs généraux, nous montrons que la donnée de suffisamment de polynômes de Darboux est équivalente à la présence d'une intégrale première rationnelle (proposition 25). Nous montrons aussi que le degré des polynômes de Darboux irréductibles n'est pas borné en général ; nous indiquons alors des directions de recherche pour lever cet obstacle.

---

1. Algèbre différentielle ordinaire

Dans cette partie, nous rappelons quelques bases du formalisme de l'algèbre différentielle. C'est un survol très rapide, qui serait profitablement complété par la lecture de plusieurs ouvrages. L'ouvrage fondateur de Ritt ([Rit50]) est très accessible et contient beaucoup de choses ; le livre d'introduction de Kaplansky ([Kap57]) est également remarquable et présente de plus des idées que nous utilisons dans le deuxième chapitre ; le livre de Kolchin ([Kol73]) est le plus difficile mais aussi de loin le plus complet ; enfin, mentionnons trois introductions rapides dont la lecture peut être utile : le chapitre 2 du livre de Buium ([Bui94]), l'article [Ros72] de Rosenlicht, et la thèse de Boulier ([Bou94]).

1.1. Idéaux différentiels

Dans tout ce travail, k désignera un corps commutatif de caractéristique zéro. Une *dérivation* de k est une application de $\partial : k \mapsto k$ vérifiant:

$$\begin{aligned} \forall a, b \in k,\ \partial(a+b) &= \partial(a) + \partial(b) \\ \forall a, b \in k,\ \partial(ab) &= \partial(a)b + a\partial(b) \text{ (règle de Leibniz)} \end{aligned}$$

On dit que (k, ∂) est un *corps différentiel* (ordinaire)*. On notera k pour un corps différentiel et ∂_k sa dérivation (quand il y aura ambiguïté sur le corps) ; nous utiliserons souvent la notation standard $a' = \partial(a)$.

Une extension $K \supset k$ est une *extension de corps différentiel* si K est muni d'une dérivation ∂_K dont la restriction à k est ∂_k (on dit aussi que ∂_K *étend* ∂_k à K). Dans tout ce qui suit, les extensions seront toujours des extensions différentielles. Un *morphisme de corps différentiels* sera un morphisme qui commute avec les dérivations.

On appellera *corps des constantes* l'ensemble $C = \{c \in k | c' = 0\}$. On peut vérifier, par exemple, que $\mathbb{C}(x)$ (muni de la dérivation usuelle $\frac{d}{dx}$ qui envoie chaque élément de $\mathbb{C}$ sur 0 et x sur 1) est bien un corps différentiel dont le corps des constantes est $\mathbb{C}$. Pour mieux comprendre ce qui suit, le lecteur non familier avec ces notions peut penser k comme étant un corps de fonctions méromorphes sur des régions données du plan complexe clos sous la différentiation ([Ros72] or [Bui94] p. 40). Ces définitions s'étendent *mutatis mutandis* au cas des anneaux.

Considérons un ensemble dénombrable d'indéterminées notées $Y^{(i)}$; si l'on pose $Y^{(i+1)} = Y^{(i)'}$, alors on peut considérer l'anneau différentiel $k\{Y\} := k[Y, Y', Y'', \ldots]$ des *polynômes différentiels en* Y et Y est appelé une *indéterminée différentielle*. On peut de la même manière adjoindre un nombre fini d'indéterminées différentielles $Y_1, \cdots, Y_n$ à k et considérer l'anneau différentiel $k\{Y_1, \cdots, Y_n\}$. Le corps des fractions de $k\{Y_1, \cdots, Y_n\}$ sera noté $k\langle Y_1, \cdots, Y_n\rangle$. Un idéal de $k\{Y_1, \cdots, Y_n\}$ est un *idéal différentiel* s'il est stable pour la dérivation. Si $\Sigma \subset k\{Y_1, \cdots, Y_n\}$ est un ensemble fini de polynôme différentiels, l'idéal différentiel $[\Sigma]$ engendré par Σ est l'idéal engendré (algébriquement) par les polynômes de Σ et toutes leurs dérivées. On notera aussi $\{\Sigma\}$ l'idéal radical engendré par Σ, c'est-à-dire le plus petit idéal radical contenant $[\Sigma]$. Les idéaux radicaux ont la propriété remarquable suivante :

Lemme 1 (de la base différentielle, [Rit50, Kap57]). *Si I est un idéal radical de l'anneau $k\{Y_1, \cdots, Y_n\}$, alors il existe un ensemble* fini $\Sigma \subset k\{Y_1, \cdots, Y_n\}$ *de polynômes différentiels tels que $I = \{\Sigma\}$.*

* Plus généralement, on parle de corps différentiel si k est muni d'un monoïde de dérivations, mais nous n'étudierons que le cas différentiel ordinaire dans ce travail

Dans ce qui suit, le mot "idéal" désignera toujours (sauf mention contraire) un idéal différentiel.

1.2. Solutions de systèmes différentiels

Soit $\eta = (\eta_1, \cdots, \eta_n)$ un n-uplet d'éléments d'une extension différentielle de k. L'ensemble $I(k, \eta)$ des polynômes différentiels de $k\{Y_1, \cdots, Y_n\}$ qui s'annulent en η forme un idéal différentiel premier. Quand nous parlerons de solution ou de zéro d'équations (ou d'idéal), nous identifierons toujours un n-uplet d'éléments d'une extension différentielle de k à l'idéal premier associé.

Soit $\Sigma \subset k\{Y_1, \cdots, Y_n\}$ un ensemble fini de polynômes différentiels. On dit que η est un *zéro* de Σ si $\Sigma \subset I(k, \eta)$. Si I est un idéal différentiel de $k\{Y_1, \cdots, Y_n\}$, on dit que η est un *zéro* de I si η est un zéro de tous les polynômes de I.

Si I est un idéal premier de $k\{Y_1, \cdots, Y_n\}$, on peut toujours trouver un n-uplet $y = (y_1, \cdots, y_n)$ d'éléments d'une extension de k tels que $I = I(k, y)$: il suffit de prendre pour y la classe de $(Y_1, \cdots, Y_n)$ dans $k\{Y_1, \cdots, Y_n\}/I$. Un tel y sera nommé un *zéro générique* de I. Tout zéro η de I est une *spécialisation* de y : toute relation différentielle satisfaite par y sera satisfaite par η. Nous adoptons dans tout le reste de ce chapitre la convention suivante : les grandes lettres désigneront des indéterminées (par exemple Y_1) et les petites lettres (par exemple y_1) désigneront des zéros d'idéaux.

Soit maintenant $\Sigma \subset k\{Y_1, \cdots, Y_n\}$ et $I = \{\Sigma\}$ l'idéal radical qu'il engendre. Le lemme simple suivant montre que la notion de zéro de Σ est liée à la maximalité de I :

Lemme 2. *Soit I un idéal différentiel de $k\{Y_1, .., Y_n\}$, et soit $\xi := (\xi_1, .., \xi_n)$ un zéro de I. Soit $\mathcal{P} = I(k, \xi)$ l'idéal premier dont ξ est un zéro générique. Alors, $I \subset \mathcal{P}$.*

Preuve. - Soit ρ l'épimorphisme d'évaluation de $k\{Y_1, .., Y_n\}$ qui à Y_i associe ξ_i. Comme ξ est générique pour $\mathcal{P}$, on a $\mathrm{Ker}(\rho) = \mathcal{P}$. Or, $\forall Q \in I, Q(\xi) = 0$, d'où $Q \in \mathrm{Ker}(\rho)$, et $I \subset \mathcal{P}$. □

D'un point de vue algébrique, résoudre Σ revient donc à trouver des idéaux premiers qui contiennent I. En particulier, I est maximal si et seulement si tout zéro de I est générique. Dans tout ce qui suit, nous faisons deux hypothèses fondamentales :

> Par idéal maximal, nous entendons un idéal maximal de $k\{Y_1, \cdots, Y_n\}$ autre que $\{Y_1, \cdots, Y_n\}$; en d'autre termes, nous *choisissons* de ne pas considérer $(0, \cdots, 0)$ comme une solution de nos systèmes différentiels.

Nous supposons que nous travaillons toujours en dimension différentielle zéro, c'est-à-dire que si y est un zéro générique d'un idéal premier I, alors $k\{y\}$ est de degré de transcendance (algébrique) fini sur k.

Nous dirons que Σ est *différentiellement réductible* s'il existe un idéal maximal qui contienne strictement $I = \{\Sigma\}$. Notons que trouver un idéal maximal qui contienne I ne donne pas nécessairement un zéro de I de degré de transcendance minimal sur k :

Exemple. - Soit $k = C(x)$ et

$$L = \left(-x+1+x^2\right)Y''' + \left(1-3\,x+x^2-x^3\right)Y'' - x\left(-x+1+x^2\right)Y' + \left(2\,x^2-x^3+x^4-1\right)Y$$

L'idéal différentiel engendré par L est premier. Si y est un zéro générique de L, alors le degré de transcendance $dtr_k k\{y\}$ de $k\{y\}$ sur k est égal à 3. On peut vérifier que $[L]$ est inclus respectivement dans les deux idéaux premiers $[L_1]$ et $[L_2]$ où

$$\begin{aligned} L_1 &= Y' - xY \\ L_2 &= Y'' - xY \end{aligned}$$

On peut montrer (voir le chapitre III) que $[L_1]$ et $[L_2]$ sont maximaux. Soient y_1, y_2 des zéros génériques de $[L_1]$ et $[L_2]$ respectivement. Ce sont tous les deux des zéros (non génériques) de $[L]$, mais $dtr_k k\{y_2\} = 2 > dtr_k k\{y_1\} = 1$. Si l'on raisonne en termes de "vraies" solutions au sens classique (données par des conditions initiales), tout ceci signifie que *génériquement* les solutions de $L(y) = 0$ ne vérifieront pas d'équation d'ordre plus petit mais que *certaines* solutions vérifieront $L_1(y) = 0$ ou $L_2(y) = 0$. La maximalité de L_i nous dit alors que ces solutions exceptionnelles ne vérifieront pas d'équation d'ordre plus petit. En fait, les idéaux $[L_1]$ et $[L_2]$ caractérisent des "classes" de conditions initiales correspondant à des solutions non-génériques de $L(y) = 0$. $\diamond$

1.3. Solutions d'équations différentielles quasi-linéaires

Soit $Q = Q(Y, Y', \cdots, Y^{(n)}) \in k\{Y\}$ un polynôme différentiel ordinaire d'ordre n et algébriquement irréductible (i.e Q est irréductible quand on le voit comme un polynôme non-différentiel à plusieurs variables sur k), et $[Q]$ l'idéal différentiel engendré par Q. Le *séparant* $\mathrm{Sep}(Q)$ est défini comme $\frac{\partial Q}{\partial Y^{(n)}}$; Si Q est de degré m en $Y^{(n)}$, alors, l'*initial* $\mathrm{In}(Q)$ est le coefficient de ${Y^{(n)}}^m$ dans Q. Le séparant est l'initial de toutes les dérivées de Q.

Si nous notons H le semi-groupe multiplicatif engendré par $(\mathrm{Sep}(Q), \mathrm{In}(Q))$, alors l'idéal $I(Q) := [Q] : H = \{P \in k\{Y\} \text{ s.t } \exists n_I, n_S \in \mathbb{N} \ : \mathrm{In}(Q)^{n_I}\mathrm{Sep}(Q)^{n_S} P \in [Q]\}$ est premier. La réciproque est vraie : si I est premier, alors il existe Q tel que $I = [Q] : H$ (on trouvera une preuve de cette assertion dans [Rit50] pages 30,31,45,57 et [Kol73] lemme 2 page 167, ou dans [Bui94] p. 28).

On dit qu'un élément η d'une extension différentielle de k est un *zéro* de Q si $Q \in I(k\,;\eta)$; un zéro générique y de $I(Q)$ est appelé un *zéro générique* de Q (c'est à dire, un zéro de Q qui ne soit un zéro d'aucun polynôme différentiel plus petit). Tout zéro non-singulier de Q est une *spécialisation** de y : toute relation différentielle satisfaite par y sera satisfaite par tout zéro de $I(Q)$, donc en particulier par tous les zéros non-singuliers.

Dans la suite de ce chapitre (jusqu'à la partie 6), la notation P désignera toujours un polynôme différentiel *quasi-linéaire* en une variable différentielle, ce qui signifie que P est linéaire en sa dérivée d'ordre le plus élevé :

$$P = s(Y, \cdots, Y^{(n-1)})Y^{(n)} + t(Y, \cdots, Y^{(n-1)}).$$

Un zéro η de P sera appelé un *zéro d'ordre* r si le plus petit polynôme différentiel Q tel que $Q(\eta, \eta', \cdots) = 0$ est d'ordre r. Dans l'exemple de la partie précédente, le zéro générique de L est d'ordre 3 alors que les zéros génériques de L_1 et L_2 sont d'ordre 1 et 2 respectivement.

Donc, dans notre contexte, "résoudre une équation différentielle" signifie "caractériser les zéros du polynôme différentiel associé", et cela signifie que nous voulons classer les zéros de P par leur ordre sur k. On dira qu'un polynôme différentiel est *différentiellement réductible* s'il existe un idéal différentiel maximal I tel que $I(P) \subsetneq I$.

Dans le paragraphe suivant, nous rappelons la méthode de Ritt pour tester si un polynôme différentiel Q satisfait $I(P) = I(Q)$ (si l'on spécifie des conditions initiales, une version plus générale de cette méthode est donnée dans [PGe95] et les références incluses). Le but de la suite de ce chapitre va être d'indiquer une stratégie pour trouver un tel Q. Nous ne connaissons pas d'algorithme général pour tester si un idéal différentiel est maximal donc, pour l'instant, le mieux que nous puissions faire est de proposer de bonnes heuristiques : nous montrerons comment chercher des intégrales premières (ou des polynômes de Darboux, voir la définition plus bas) fournit des solutions d'ordre plus petit.

La réduction de Ritt.

Donnons nous maintenant un ordre sur les monômes de $k\{Y\}$. Dans ce qui suit, nous considérons l'ordre lexicographique avec $i > j \Rightarrow Y^{(i)} > Y^{(j)}$. Deux monômes m_1 et m_2 qui diffèrent juste par multiplication par un élément de k sont dit *équivalents* ($m_1 \sim m_2$). Tout polynôme différentiel Q a un monôme dominant, noté $lm(Q)$; pour tous polynômes $Q, R \in k\{Y\}$, on a alors :

$$Q \gtrsim R \text{ si } \ \mathrm{lm}(Q) \gtrsim \mathrm{lm}(R)$$

Si on se donne deux polynômes différentiels $Q \gtrsim R$ avec $\mathrm{ord}(Q) = n$, $\mathrm{ord}(R) = r$ et

* On peut trouver des équations différentielles pour lesquelles certaines solutions singulières ne sont pas des spécialisations de la solution générique. Par exemple, si $Q = (y')^2 - 4 * y$, la solution générique vérifie $y'' - 2 = 0$, ce que ne vérifie pas la solution singulière $y = 0$. Je remercie Evelyne Hubert de m'avoir rappelé ce point.

$n \geq r$, alors nous pouvons réduire Q par R de la manière suivante (voir [Rit50]) : On a $R^{(n-r)} = \mathrm{Sep}(R)Y^{(n)}$+termes plus petits. Donc, nous obtenons $\mathrm{Sep}(R)Q = \alpha_{n-r}R^{(n-r)} +$ des termes en $Y^{(n-1)}$ et des plus petits (avec $\alpha_{n-r} \in k\{Y\}$). Répétant ce processus, nous réduisons de nouveau jusqu'à ce que le reste soit d'ordre r. Nous opérons alors une réduction algébrique pour obtenir la relation :

$$\mathrm{In}(R)^m \mathrm{Sep}(R)^{n-r} Q = \sum_{i=0}^{i=n-r} \alpha_i R^{(i)} + R_1$$

où $Q \gtrsim R > R_1$ et m est un entier. Le polynôme R_1 est la *réduction* de Q par R.

Quoique simple, ce processus de réduction s'avère très puissant ; il nous donne en particulier les deux résultats qui suivent. On dit qu'un zéro d'un polynôme différentiel Q est *singulier* s'il est aussi un zéro de $\mathrm{Sep}(Q)$ ou $\mathrm{In}(Q)$. Pour illustrer la méthode de Ritt, nous pouvons montrer le résultat suivant, qui nous donne une première classe de zéros de P :

Proposition 3. *Soit $P = s(Y, \ldots, Y^{(n-1)})Y^{(n)} + t(Y, \ldots, Y^{(n-1)})$. Alors, on peut décider si P a des zéros singuliers et produire algorithmiquement leurs polynômes différentiels minimaux.*

Preuve. - D'après la forme de P, la question est juste de décider si s et t ont un zéro en commun, ce qui peut être fait de la manière suivante (voir [Bou94] pour un algorithme plus général d'élimination différentielle). Supposons que $s \gtrsim t$ (sinon, échanger leurs rôles). Réduisant s par t, nous obtenons un nouveau polynôme t_1. Un point clé est que tout zéro commun à s et t est un zéro de t_1. Nous réduisons s et t par t_1 et, ainsi de suite, produisons des polynômes toujours plus petits dont les zéros communs à s et t sont des zéros. Si le processus nous produit le polynôme 1 (ou tout élément de k), alors s et t n'ont pas de zéro commun. Sinon, le processus s'arrête et, dans notre collection de polynômes, il y a un polynôme t_1 qui est minimal. La minimalité de t_0 implique que s et t sont réduits à zéro par t_0 ; donc, tout zéro non singulier de t_0 est un zéro commun à s et t. Si tous les zéros de t_0 sont singuliers, alors t_0 n'est pas algébriquement irréductible, donc nous réduisons s et t par rapport à tous les facteurs de t_0 et itérons le processus. □

Intéressons nous maintenant aux zéros non-singuliers de P.

Un critère très général.

La réduction de Ritt nous donne théoriquement un critère général pour tester si P est différentiellement réductible.

Lemme 4. *Le polynôme P a un zéro d'ordre r si et seulement s'il existe un polynôme différentiel R algébriquement irréductible, un entier m, et des polynômes $\alpha_i \in k\{Y\}$, pour*

$i = 0, \ldots, n-r$ tels que :

$$\mathrm{In}(R)^m Sep(R)^{n-r} P = \sum_{i=0}^{i=n-r} \alpha_i R^{(i)} \tag{1.1}$$

Preuve. - L'identité (1.1) implique clairement qu'un zéro générique de R est un zéro de P (car $\mathrm{In}(R)$ et $\mathrm{Sep}(R)$ sont plus petits que R).
Réciproquement, supposons que P a un zéro d'ordre r. Alors, il existe un $R \in k\{Y\}$ d'ordre r et minimal tel que le zéro générique ρ de R soit un zéro de P. La minimalité de R implique qu'il soit algébriquement irréductible. Réduisant P par R, nous obtenons :

$$\mathrm{In}(R)^m \mathrm{Sep}(R)^{n-r} P = \sum_{i=0}^{i=n-r} \alpha_i R^{(i)} + Q$$

où Q est plus petit que R. Mais $Q(\rho) = 0$; donc, comme ρ est générique pour R, nous obtenons $Q = 0$. □

Bien sur, ce critère est loin d'être effectif : étant donné P, il n'y a pas (pour l'instant) de méthode générale pour tester s'il existe un tel R. Ce critère sert surtout à tester si un R donné définit effectivement des zéros d'ordre au plus r de P.

Remarque. - On peut aussi voir ce critère comme un analogue non-linéaire de la factorisation des opérateurs pour des équations différentielles linéaires (voir l'appendice 1 ou les chapitres II,III). ⋄

2. Une collection de propriétés des constantes

Dans les ouvrages classiques, on lit que "la connaissance d'une intégrale première d'un système permet d'abaisser l'ordre du système". Dans cette partie, nous allons donner une formulation algébrique (et plus précise) de cette phrase, due à Kolchin dans [Kol48b]. Nous donnerons ensuite, pour mémoire, quelques propriétés standard des constantes en algèbre différentielle.

2.1. Constantes, solutions, et degré de transcendance

Soit Σ un ensemble fini de polynômes de $k\{y_1, \cdots, y_n\}$ et $\{\Sigma\}$ l'idéal différentiel radical engendré. Caractériser un idéal premier I tel que $\{\Sigma\} \subsetneq I$ est très difficile, en général. Nous donnons ci-dessous un résultat utile dans cette direction, adapté de la preuve du théorème 1 de [Kol48b] :

Théorème 5 (Kolchin)[Kol48b]. *Soit I un idéal radical de l'anneau $k\{Y_1, \cdots, Y_n\}$, et soit $J \in k\{Y_1, \cdots, Y_n\} \setminus I$; et soit ξ un zéro de I tel que $J(\xi_1, .., \xi_n) \neq 0$.*
S'il existe une constante β dans $k\langle \xi_1, \ldots, \xi_n \rangle$ transcendante sur C_k, alors il existe un zéro $\eta_1, .., \eta_n$ de I tel que $J(\eta) \neq 0$, qui vérifie :

$$\mathrm{dtr}_k k\langle \eta_1, .., \eta_n \rangle < \mathrm{dtr}_k k\langle \xi_1, .., \xi_n \rangle.$$

En particulier, il existe un zéro η de I tel que $J(\eta) \neq 0$ et le corps des constantes de $k\langle \eta \rangle$ est algébrique sur celui de k.

Une conséquence immédiate de ce théorème est bien sur que $I(\xi) \subsetneq I(\eta)$; plus précisément, il signifie qu'il existe $c \in C$ tel que l'équations $\beta(y) = c$ a un zéro commun avec I

Si C_k est algébriquement clos, ce résultat montre qu'on peut toujours trouver une solution qui n'introduise pas de nouvelle constante. Si C_k n'est pas algébriquement clos, Seidenberg a donné un exemple d'équation pour laquelle toute solution introduit une nouvelle constante ([Sei56, Wei92]).

Remarque. - Le fait que $k\langle \xi_1, .., \xi_n \rangle$ ne contienne pas de constante transcendante n'implique pas que I soit maximal. Par exemple, considérons l'équation $L(y) = y'' - (1 + x^2)y = 0$ et $k = C(x)$. Avec les techniques du chapitre III, on montre facilement que, si y est un zéro générique de L, alors $k\langle y \rangle$ ne contient pas de constante transcendante (avec les notations du chapitre III : L est réductible mais non complètement réductible et admet un unique polynôme de Darboux). Pourtant, cette équation admet la solution non-générique $y = e^{x^2/2}$ (i.e, $[L] \subsetneq [L, y' - xy]$). $\diamond$

Ce résultat sur les constantes est crucial pour montrer l'existence des extensions de Picard-Vessiot pour les systèmes différentiels linéaires (voir chapitre II), et Kolchin l'a montré dans ce but. Ce résultat a été montré de manière différente (mais toujours dans le même esprit) par plusieurs auteurs ; on pourra consulter notamment* [Lev89, Fah93, Bui94, Mag94].

Le reste de ce travail consistera à élaborer des techniques qui permettent d'exhiber des constantes transcendantes quand elles existent, et de "résoudre" les équations différentielles par ce biais.

2.2. Lemmes standard sur les constantes

Avant de continuer, rappelons quelques résultats très classiques sur les constantes que nous utiliserons (parfois même tacitement) par la suite.

* Dans une lettre à Daniel Bertrand (1989), Michael Singer donne également une preuve qu'il attribue à Rosenlicht

Lemme 6. *Soit $y \in k$. Si y est algébrique sur C, alors $y \in C$ (i.e C est algébriquement clos dans k).*

Preuve. - Soit $M(y) = 0$ le polynôme minimal de y. Dérivant cette égalité, nous obtenons $y' \frac{\partial M}{\partial y} = 0$ donc $y' = 0$. □

Lemme 7. *Soit $K \supset k$ et D une dérivation sur K qui étende ∂_k. Soit $c \in K$ une constante pour D. Si c est algébrique sur k, alors c est algébrique sur C.*

Preuve. - Soit $M = c^n + \sum_{i=0}^{n-1} a_i c^i = 0$ le polynôme minimal de c sur k. Appliquant D à cette égalité, nous obtenons $\sum_{i=0}^{n-1} a_i' c^i = 0$. Donc, par minimalité de M, $a_i' = 0$ pour tout i et c est donc algébrique sur C □

Ce lemme s'étend immédiatement en la proposition suivante (voir par exemple [Kap57] page 33) :

Proposition 8 [Kap57]. *Soit $K \supset k$ et D une dérivation sur K qui étende ∂_k. Soient $c_1, \cdots, c_n$ des constantes pour D. Si $c_1, \cdots, c_n$ sont algébriquement indépendantes sur C, alors elles sont algébriquement indépendantes sur k.*

Lemme 9. *Soit $K \supset k$ et D une dérivation sur K qui étende ∂_k. Alors C_K et k sont linéairement disjoints sur C_k (i.e, des constantes de K sont linéairement dépendantes sur k si et seulement si elles sont linéairement dépendantes sur C_k).*

Preuve. - La preuve est identique à celle des lemmes précédents en considérant une relation de dépendance de longueur minimale : d'une relation de dépendance linéaire $\sum_{i=1}^{n} k_i C_i$ (où n est minimal), on déduit (en dérivant) une relation $\sum_{i=1}^{n} c_i C_i = 0$ où les c_i sont des constantes (non toutes nulles) de C_k. □

3. Quelques utiles généralités sur les dérivations

3.1. Dérivation associée à un système quasi-linéaire

Soit (k, ∂_k) un corps différentiel et $A = k[Y_1, \cdots, Y_n]$ une algèbre de polynômes finiment engendrée. On étends ∂_k à A par $\partial_k(Y_1) = \cdots = \partial(Y_n) = 0$ (c'est-à-dire que l'image de $M \in A$ par ∂_k est le polynôme dont les coefficients sont les dérivées des coefficients de M) ; on note $\frac{\partial}{\partial Y_i}$ la dérivée partielle par rapport à la variable Y_i. Alors, toute dérivation D de A

qui étende ∂_k s'exprime par (cf [Lan92] p. 370)

$$D = \partial_k + \sum f_i \frac{\partial}{\partial Y_i} \quad \text{avec } f_i = D(Y_i)$$

Dans la suite, nous formerons systématiquement des dérivations dans le contexte suivant. Soient $f_1, \cdots, f_r, g_1, \cdots, g_r \in k[Y_1, \cdots, Y_n]$ et le système différentiel

$$\begin{cases} g_1(Y_1, \cdots, Y_n)Y_1' = f_1(Y_1, \cdots, Y_n) \\ \vdots \\ g_r(Y_1, \cdots, Y_n)Y_n' = f_n(Y_1, \cdots, Y_n) \end{cases} \tag{3.1}$$

Considérons l'anneau $k[y_1, \cdots, y_n]$ muni de la dérivation

$$D = \left(\prod_{j=1}^{n} g_j\right) \partial_k + \sum_{i=1}^{n} \left(\prod_{\substack{j=1 \\ j\neq i}}^{n} g_j\right) f_i \frac{\partial}{\partial y_i} \tag{3.2}$$

Pour étudier les propriétés vérifiées par les solutions, on se placera dans $(k[y_1, \cdots, y_n], D)$. Par exemple, une constante pour D sera une intégrale première pour le système, c'est-à-dire une fonction qui est constante sur les solutions.

3.2. Dérivations homogènes ou isobares

Il est parfois commode d'associer un poids aux variables de $k[Y_1, \cdots, Y_n]$. On dit qu'un polynôme $f \in k[Y_1, \cdots, Y_n]$ est *isobare* de degré (ou ω-degré) p s'il existe un n-uplet d'entiers $\omega = (\omega_1, \cdots, \omega_n)$ tels que $f(t^{\omega_1}Y_1, \cdots, t^{\omega_n}Y_n) = t^p f(Y_1, \cdots, Y_n)$; on dira aussi que f est ω-isobare.

Si $M = \prod Y_i^{d_i}$, alors le ω-degré de M est $p = \sum \omega_i d_i$; un polynôme est ω-isobare si tous ses monômes ont même ω-degré. Le ω-degré d'un polynôme non-isobare sera le maximum des ω-degrés de ses monômes. Enfin, on vérifie aisément que si $f, g \in k[Y_1, \cdots, Y_n]$ et si fg est ω-isobare alors f et g sont chacun ω-isobares.

Notons que, si f est ω-isobare, alors on a la relation d'Euler généralisée :

$$\omega_1 Y_1 \frac{\partial f}{\partial Y_1} + \cdots + \omega_n Y_n \frac{\partial f}{\partial Y_n} = pf \tag{3.3}$$

En particulier, si $\omega_1 = \cdots = \omega_n = 1$, alors on dit que f est homogène, et on retrouve la relation d'Euler usuelle.

Ces notions s'étendent bien sur immédiatement à $k(Y_1, \cdots, Y_n)$: le degré (resp ω-degré) d'une fraction est la différence des degrés respectifs de son numérateur et de son dénominateur (voir e.g [Now94] p.20). Nous aurons dans la suite à considérer des dérivations du type suivant :

Définition 10. Soit D une dérivation de $k[Y_1, \cdots, Y_n]$. On dit que D est *homogène* de degré s si l'image par D d'un monôme de degré p est un polynôme homogène de degré $p+s$. On dit que D est ω-isobare de degré s si l'image par D d'un monôme de ω-degré p est un polynôme ω-isobare de ω-degré $p+s$.

Par exemple, la dérivation $\frac{\partial}{\partial Y_i}$ est homogène de degré -1 et elle est ω-isobare de degré $-\omega_i$. L'intérêt de ces notions provient de la remarque (simple) que toute dérivation D de A peut s'écrire comme une somme de dérivations homogènes (ou isobares) de degré croissant ; certaines propriétés de D se liront mieux sur les composantes homogènes.

4. Polynômes de Darboux

Soit D une dérivation sur $k(Y_1, \cdots, Y_n)$. Soit $A := k[Y_1, \cdots, Y_n]$ et $F, G \in A$ premiers entre eux tels que $D(F/G) = 0$. Alors, on a $GD(F) - FD(G) = 0$. Comme F et G sont premiers entre eux, il en découle que F divise $D(F)$ et G divise $D(G)$ dans A. Ceci motive la définition suivante :

Définition 11. Soit D une dérivation de $k[Y_1, \cdots, Y_n]$. On dit que $F \in k[Y_1, \cdots, Y_n]$ est un *polynôme de Darboux* pour D si F divise $D(F)$, c'est-à-dire s'il existe $\alpha \in k[Y_1, \cdots, Y_n]$ tel que

$$D(F) = \alpha F.$$

Notons que, en termes d'algèbre différentielle, les polynômes de Darboux correspondent aux idéaux principaux de $k[Y_1, \cdots, Y_n]$ qui sont différentiels (i.e $D(F) \in (F)$). Chaque élément de k est bien sûr un polynôme de Darboux *trivial* pour D ; dans la suite, quand nous chercherons si D admet des polynômes de Darboux, il faudra toujours comprendre "non triviaux", c'est-à-dire n'appartenant pas à k.

Exemple. - Considérons la dérivation $D = Y_1 Y_2 \frac{\partial}{\partial Y_1} + n Y_2^2 \frac{\partial}{\partial Y_2}$. Nous avons deux polynômes de Darboux $F_1 = Y_1$ (avec $DF_1 = Y_2 F_1$) et $F_2 = Y_2$ (avec $DF_2 = n Y_2 F_2$). On notera que, dans ce cas, $D(F_1^n / F_2) = 0$. $\diamond$

L'utilisation de telles polynômes pour trouver des intégrales premières remonte à Darboux ([Darboux]). Ils ont ensuite été étudiés (entres autres) par Painlevé, Poincaré, Picard, Autonne, Lagutinskii au $19^{\text{ème}}$ siècle. On les trouve sous une très grande variété de noms dans la littérature. Selon les articles, ils peuvent apparaître sous le nom "polynômes spéciaux" ([Bro90, Wei94, UWe94, Rao94]), "courbes algébriques invariantes" ([Sch93, CLN91], "polynômes propres" (eigenpolynômials dans [Man94]), "solutions algébriques" ([Darboux, Jou79]), "séparatrices" ([CLN91]), "intégrales partielles" ([DLS95, MMi95]) ou d'autres noms encore...

À ma connaissance, ils ont été essentiellement utilisés pour la recherche d'intégrales premières. La terminologie "polynômes spéciaux" a été introduite par Bronstein ([Bro90]) pour comprendre comment la théorie de l'intégration en forme finie s'étends aux extensions du type $y' = H(y)$, $H \in k[y]$ (voir [Rao94] pour les extensions du type $s(y)y' = t(y)$, et également [Ros72, WGOS]).

4.1. Premières propriétés des polynômes de Darboux

Lemme 12. *Si F et G sont des polynômes de Darboux pour D, alors FG est un polynôme de Darboux pour D. Réciproquement, si F est un polynôme de Darboux pour D, alors tous ses facteurs irréductibles sont des polynômes de Darboux pour D.*

Preuve. - Si $D(F) = \alpha_F F$ et $D(G) = \alpha_G G$, avec $\alpha_F, \alpha_G \in A$, alors

$$D(FG) = D(F)G + FD(G) = (\alpha_F + \alpha_G)FG.$$

Réciproquement, supposons que $D(F) = \alpha_F F$ (avec $\alpha_F \in A$) et que $F = F_1^n F_2$ (où F_1 est irréductible et F_1, F_2 sont premiers entre eux). Nous avons alors deux expressions pour $D(F)$:

$$\alpha_F F_1^n F_2 = nF_1^{n-1}D(F_1) + F_1^n D(F_2).$$

Comme F_1^n divise les deux membres de cette équation et que F_1 est premier avec F_2, F_1 doit diviser $D(F_1)$; similairement, F_2 divise $D(F_2)$ et, par récurrence, tous les facteurs irréductibles de F sont des polynômes de Darboux. □

Les polynômes de Darboux forment donc un semi-groupe multiplicatif que nous noterons $\mathcal{S}_D$ (ou simplement $\mathcal{S}$ s'il n'y a pas d'ambiguïté). Notons que $k \subset \mathcal{S}$. Nous dirons qu'un polynôme de Darboux est *trivial* s'il appartient à k. Il découle du lemme précédent que $\mathcal{S}$ est entièrement déterminé par ses éléments non-triviaux irréductibles (mais qui ne sont pas nécessairement en nombre fini). Dans certains cas, on peut même mieux caractériser les éléments de $\mathcal{S}$ (cf [MNS93, Wei94, Now94]) :

Lemme 13. *Soit $\omega = (\omega_1, \cdots, \omega_n)$ un n-uplet d'entiers, et soit D une dérivation ω-isobare de degré p de $k[Y_1, \cdots, Y_n]$. Si F est un polynôme de Darboux vérifiant $DF = \alpha F$ alors α est ω-isobare de degré p et toutes les composantes ω-isobares F_i de F vérifient aussi $DF_i = \alpha F_i$.*
En particulier, si D est homogène de degré 0, alors $\alpha \in k$.

Preuve. - Découle immédiatement de la définition du degré d'une dérivation □

Ce résultat nous sera particulièrement utile pour l'étude des systèmes différentiels linéaires dans le chapitre suivant.

Remarque. - Le lemme précédent fournit aussi une première stratégie simple pour prouver la non-existence de polynômes de Darboux pour une dérivation D donnée. Soit ω un n-uplet d'entiers. On peut écrire $D = \sum_{i=1}^{\nu} D_i$ où les D_i sont des dérivations ω-isobares de degrés d_i croissants. Dans ce cas, on voit facilement que D admet un polynôme de Darboux seulement si D_1 et D_ν admettent chacune un polynôme de Darboux. C'est, par exemple, par ce biais que Nishioka a montré la transcendance de la première transcendante de Painlevé* (voir [Nis89b]). $\diamond$

4.2. Polynômes de Darboux et extensions

Dans cette partie, nous étudions comment la notion de polynôme de Darboux se comporte par rapport à d'éventuelles extensions de k.

Lemme 14. *Soit K une extension différentielle de k, et D_K l'extension à K de D. Alors, $F \in k[Y_1, \cdots, Y_n]$ est un polynôme de Darboux pour D_K si et seulement si il est un polynôme de Darboux pour D.*

Preuve. - Supposons que $D_K(F) = \alpha F$ avec $\alpha \in K[Y_1, \cdots, Y_n]$. Comme $F \in k[Y_1, \cdots, Y_n]$, on a $D_K(F) = D(F)$. La relation $D(F) = \alpha F$ donne un système linéaire sur k pour les coefficients de α, et donc $\alpha \in k[Y_1, \cdots, Y_n]$. $\square$

Le problème suivant est celui de la *rationalité* : si C n'est pas algébriquement clos, peut-on toujours calculer un polynôme de Darboux sans introduire de nouvelle constante ? la réponse positive est donnée comme cas particulier de la proposition suivante* :

Proposition 15. *Soit $K \supset k$ une extension algébrique finie de k. Alors, D_K admet un polynôme de Darboux non-trivial dans $K[Y_1, \cdots, Y_n]$ si et seulement si D admet un polynôme de Darboux non-trivial dans $k[Y_1, \cdots, Y_n]$.*

Preuve. - Soit** t un élément primitif de l'extension K/k, de telle sorte que $K = k(t)$ notons Q le polynôme minimal de t, K_1 le corps de décomposition de Q et G le groupe de Galois de K_1/k. Soit $M \in K[Y_1, \cdots, Y_n]$ un polynôme de Darboux pour D_K (l'extension unique de D à $K[Y_1, \cdots, Y_n]$) vérifiant $D_K M = \alpha M$ avec $\alpha \in K[Y_1, \cdots, Y_n]$. On a $M \in K_1[Y_1, \cdots, Y_n]$ et M est un polynôme de Darboux pour D_{K_1}. Rappelons que, par unicité de l'extension de D à $K[Y_1, \cdots, Y_n]$, les éléments de G commutent avec D_{K_1} ; il en découle que,

* Une preuve analogue a été donnée par Kolchin et par Kovacic dans une lettre à M.F Singer (1975)

* Durant la rédaction finale de ce travail, j'ai reçu l'article [McM94] de Mac Callum et Man qui donnent un résultat analogue pour une dérivation de $C[Y_1, Y_2]$

** Cette preuve m'a été suggérée par Jean Moulin Ollagnier

pour tout $g \in G$, on a $D_{K_1}(g(M)) = g(\alpha)g(M)$ Considérons le polynôme $\mathcal{M} = \prod_{g\in G} g(M)$, c'est-à-dire la norme de M sous G. On a alors

$$D_{K_1}(\mathcal{M})/\mathcal{M} = \sum_{g\in G} D_{K_1}(g(M))/g(M) = \sum_{g\in G} g(\alpha).$$

Il en découle que $\mathcal{M}$ est un polynôme de Darboux pour D_{K_1}. Or, les coefficients de $\mathcal{M}$ sont fixés par G et ainsi $\mathcal{M} \in k[Y_1, \cdots, Y_n]$; de même, $\sum_{g\in G} g(\alpha) = Tr_G(\alpha) \in k[Y_1, \cdots, Y_n]$. Il découle du lemme 14 que $\mathcal{M}$ est spécial pour D. Pour vérifier que $\mathcal{M}$ est non trivial, on met un ordre sur les variables Y_i ; si Y est le monôme dominant de M (i.e $M = \mu Y + \cdots$ avec $\mu \in K$), alors le coefficient dominant de $\mathcal{M}$ est $\left(\prod_{g\in G} g(\mu)\right) Y^{|G|}$. Comme la norme $\left(\prod_{g\in G} g(\mu)\right)$ de μ sous G est non-nulle, le polynôme $\mathcal{M}$ est un polynôme de Darboux non-trivial pour D. □

On voit sur cette preuve que, pour éviter une extension algébrique, on peut être conduit à considérer des polynômes de Darboux de degré plus élevé. Nous en verrons des exemples au chapitre III ; en particulier, dans la section 5 page 100 du chapitre III, nous verrons comment, pour les équations de Riccati du premier ordre, on peut abaisser le degré des polynômes de Darboux en faisant des extension radicales successives de k.

Une conséquence triviale mais intéressante de la proposition 15 est le résultat de rationalité suivant : on n'a pas besoin d'étendre le corps des constantes pour calculer un polynôme de Darboux.

4.3. Polynômes de Darboux des équations quasi-linéaires

Si nous considérons un polynôme différentiel quasi-linéaire

$$P = s(Y, \cdots, Y^{(n-1)})Y^{(n)} - t(Y, \cdots, Y^{(n-1)}),$$

nous pouvons définir la *dérivation en un zéro générique* par

$$D = s\partial_k + s\sum_{i=0}^{n-2} y^{(i+1)}\frac{\partial}{\partial y^{(i)}} + t\frac{\partial}{\partial y^{(n-1)}}.$$

On dira alors que P admet un polynôme de Darboux si D en admet un. Comme D est une dérivation de l'anneau $k[y, \cdots, y^{(n-1)}]$, un polynôme de Darboux pour P est par définition au plus d'ordre $n-1$. Le semi-groupe des polynômes de Darboux pour D sera noté $\mathcal{S}_P$. Notons que D est aussi une dérivation de $k\{y\}$ et que, pour tout polynôme $F \in k\{y\}$ d'ordre $< n-1$, on a $DF = sF'$.

Lemme 16. *Soit $F \in \mathcal{S}_P$ un polynôme de Darboux irréductible. Alors, soit F divise s, soit F est d'ordre $n-1$.*

Preuve. - Les éléments de $\mathcal{S}_P$ sont d'ordre au plus $n-1$. Supposons qu'il existe $F \in \mathcal{S}_P$ irréductible d'ordre $i < n-1$; Alors, F' ne contient pas de terme en $Y^{(n)}$. Considérons l'identité $DF = \alpha F$ entre polynômes à n variables. L'irréductibilité de F implique qu'il divise s ou F'. Si F divise F' alors, comme F' est d'ordre $i+1$, F doit diviser $\frac{\partial F}{\partial Y^{(i)}}$; comme F a un plus grand degré en $Y^{(i)}$, c'est impossible. Donc, F divise s. □

Nous pouvons maintenant montrer le lien entre polynômes de Darboux et solutions d'équations différentielles :

Théorème 17. *Soit F un polynôme de Darboux d'ordre $n-1$ pour P. Alors, tout zéro non-singulier η de F est un zéro de P.*
Réciproquement, si P admet un zéro η d'ordre $n-1$, alors le polynôme minimal F de η est un polynôme de Darboux pour P.

Preuve. - Supposons que $DF = \alpha F$ et soit η un zéro non-singulier de F. Alors :

$$\begin{aligned} sF(\eta)' &= s\left((\partial_k F)(\eta) + \sum_{i=1}^{n-1} \eta^{(i+1)} \frac{\partial F}{\partial Y^{(i)}}(\eta)\right) \\ &= (DF)(\eta) + P(\eta)\left(\frac{\partial F}{\partial Y^{(n-1)}}\right)(\eta) \\ &= \alpha(\eta)F(\eta) + P(\eta)\left(\frac{\partial F}{\partial Y^{(n-1)}}\right)(\eta) \end{aligned}$$

Comme η est non-singulier pour F, il en découle que $P(\eta) = 0$.

Réciproquement, soit η un zéro d'ordre $n-1$ de P, et soir F son polynôme différentiel minimal. Alors, $F(\eta)' = 0$ et donc $(DF)(\eta) = 0$. Réduisant DF par F, nous obtenons que, pour un entier m et $\beta \in k\{y\}$, $\mathrm{In}(F)^m DF - \beta F = G$ avec $G < F$. Mais F est minimum pour η donc G doit être identiquement nul. Ainsi, $\mathrm{In}(F)^m DF = \beta F$. Comme F est irréductible, $\mathrm{In}(f)^m$ divise β et donc $F \in \mathcal{S}_P$ □

Le calcul de polynômes de Darboux d'équations différentielles quasi-linéaires est un problème ouvert à ce niveau de généralité. Le premier (très difficile) problème est de déterminer quel peut être le degré m des candidats éventuels. Si nous connaissons m, prenons un polynôme F à degrés indéterminés. Réduisant DF par F, nous obtenons un système différentiel du premier ordre pour les coefficients de F (avec autant d'équations que de coefficients). Malheureusement, le processus de réduction induit des termes non-linéaires dans le système, donc trouver ses solutions rationnelles est essentiellement une affaire d'habileté. Cela apparaît néanmoins être une heuristique intéressante pour des petits ordres et des petits degrés. Prelle et Singer ont proposé une méthode pour $n = 1$ (voir [PSi83, Sch93], et [MOl92],[Sin92] pour des références à d'autres approches) qui est implantée dans les systèmes de calcul formel MACSYMA et REDUCE. Nous étudierons cette méthode à la fin de ce chapitre.

4.4. Intégrales premières rationnelles des équations différentielles quasi-linéaires

En suivant le formalisme précédent, nous nous concentrons maintenant sur les intégrales premières rationnelles. Nous disons qu'une fraction F/G est sous forme canonique si $\gcd(F,G) = 1$, G est unitaire, et $F \gtrsim G$.

Définition 18. On dit que le polynôme P admet un *intégrale première rationnelle* (ou une *constante générique*) s'il existe $F/G \in k\langle y\rangle$ sous forme canonique telle que $(DF)G - F(DG) = 0$.

Cette définition revient à dire qu'il y a une constante transcendante dans le corps des fractions $k\langle y\rangle$ de $k\{y\}$; Cela signifie aussi que, pour tout zéro η de P, $\frac{F}{G}(\eta)$ est une constante. Le lemme suivant donne une version un peu raffinée du théorème 5 de Kolchin dans notre contexte :

Lemme 19. *Si le polynôme P admet une constante générique F/G (sous forme canonique), alors F est d'ordre $n-1$. Il en découle :*

> *S'il existe une constante $c_1 \in C$ telle que l'ordre de $F - c_1G$ soit inférieur à $n-1$ alors, pour toute constante $c \in C - \{c_1\}$, tout zéro non singulier de $F - cG$ est un zéro de P. Sinon, pour toute constante $c \in C$, tout zéro non singulier de $F - cG$ est un zéro de P.*

Preuve. - Comme F et G sont premiers entre eux, $(DF)G - (DG)F = 0$ implique que F divise DF. Donc, F et G sont des polynômes de Darboux avec le même facteur ; ceci reste vrai pour $F - cG$.

Si $F - cG$ est d'ordre $n-1$, alors les conclusions du lemme sont une conséquence immédiate du théorème 17. Supposons que F et G sont tous deux d'ordre inférieur à $n-1$ (i.e F et G sont deux facteurs de s). Alors, $DF = F'$ et donc $F'G - G'F = 0$. Soit m l'ordre de F ; comme F' est d'ordre plus élevé que F, F ne peux diviser F'que si F divise $\frac{\partial F}{\partial y^{(m)}}$, ce qui est impossible. Donc, la relation $F'G - G'F = 0$ impliquerait que F ait un facteur en commun avec G, contrairement aux hypothèses ; donc, F est d'ordre $n-1$.

Supposons, que pour $c_1 \in C$, $F = c_1G + f_1$ avec $ord(f_1) < n-1$. Alors, G doit être d'ordre $n-1$. S'il existe c_2 tel que $F = c_2G + f_2$ et $ord(f_2) < n-1$, alors $(c_2 - c_1)G$ est d'ordre inférieur à $n-1$, donc $c_1 = c_2$. Donc, pour tout $c \in C - \{c_1\}$, $ord(F - cG) = n-1$ et le théorème 17 montre que tout zéro non-singulier de $F - cG$ est aussi un zéro de P. Bien sur, s'il n'existe pas de constante $c_1 \in C$ telle que $F = c_1G + f_1$ avec $ord(f_1) < n-1$, alors le théorème 17 s'applique à $F - cG$ pour toute constante $c \in C$. □

Remarque. - S'il existe $c_1 \in C$ telle que $F = c_1 G + f_1$ avec $ord(f_1) < n-1$, alors f_1 divise s et, comme $ord(G) = n-1$, le théorème 17 montre que, pour toute constante $c \in C$, tout zéro non singulier de $G - cf_1$ est un zéro de P. $\diamond$

Il découle de ce lemme que les techniques pour trouver des polynômes de Darboux nous donnent deux informations : premièrement, elles montrent le lien entre intégrales premières rationnelles et solutions, et deuxièmement, elles donnent un moyen d'obtenir des intégrales premières rationnelles. Dans ce but, on peut utiliser le lemme suivant :

Lemme 20. *Supposons k est un corps différentiel tel qu'on sache trouver les solutions rationnelles d'équations différentielles linéaires homogènes à coefficients dans k. Soit m un entier et $\alpha \in k\{y\}$. Alors, on peut décider effectivement s'il existe $F \in k\{y\}$ de degré m tel que $DF = \alpha F$, et calculer ses coefficients.*

Preuve. - Supposons que F a des coefficients inconnus. La relation $DF - \alpha F = 0$ implique que tous les coefficients du polynôme différentiel $DF - \alpha F$ sont égaux à zéro. Comme nous connaissons m et α, ceci produit un système différentiel linéaire du premier ordre pour les coefficients de F. Il y a des algorithmes pour trouver les solutions rationnelles d'un tel système, ou décider l'existence de telles solutions (voir le chapitre suivant) ; cela nous donne les coefficients de F. $\square$

Remarque. - Supposons que nous nous donnons un polynôme $G \in \mathcal{S}_P$ avec un facteur α et que nous voulons trouver F tel que F/G soit une constante générique. Dans certains cas, on peut déduire de G une borne sur le degré de F : dans ce cas, l'heuristique ci-dessus devient un algorithme. Par exemple, soit $Ri(u) = 0$ une équation de Riccati du premier ordre. Soit G un polynôme de Darboux pour Ri. Alors, on peut décider si G est le dénominateur d'une constante générique et calculer son numérateur ([Wei94]) : Supposons que $\deg_u F = n$ et $\deg_u G = m$; le coefficient dominant de $(DF)G - F(DG)$ est $(n-m)F_n G_m$ et il doit être nul ; donc $n = m$.
Connaissant G, nous connaissons donc m et α. En appliquant la procédure du lemme 20, nous pouvons en déduire F. Nous donnerons dans le chapitre III un algorithme efficace pour calculer les polynômes de Darboux des équations de Riccati du premier ordre $\diamond$

Exemple. - Considérons l'équation* différentielle du premier ordre suivante sur $\mathbb{Q}(x)$:

$$P := x\,(2\,y + x - 1)\,y' - y\,(y + 2\,x + 1) = 0.$$

Nous avons la solution $y = 0$, donc $y \in \mathcal{S}_P$. De fait, $sy' = \alpha y$ avec $\alpha = y + 2\,x + 1$. Donc, pour trouver une constante générique, nous choisissons un degré m, nous prenons un polynôme générique $F := \sum f_i y^i$ de degré m en y, et nous considérons la relation $DF - \alpha F = 0$.

* cet exemple m'a été donné par Bob Caviness

On peut vérifier qu'il n'y a pas de candidats pour $m = 1$ or $m = 2$. Pour $m = 3$, on a le système différentiel suivant pour les coefficients de F :

$$\begin{aligned}
x\,(x-1)\frac{\partial}{\partial x}f_0(x) - f_0(x)\,(2\,x+1) &= 0,\\
x\,(x-1)\frac{\partial}{\partial x}f_1(x) + 2\,x\frac{\partial}{\partial x}f_0(x) - f_0(x) &= 0,\\
x\,(x-1)\frac{\partial}{\partial x}f_2(x) + 2\,x\frac{\partial}{\partial x}f_1(x) + (2\,x+1)\,f_2(x) &= 0,\\
x\,(x-1)\frac{\partial}{\partial x}f_3(x) + (4\,x+2)\,f_3(x) + f_2(x) + 2\,x\frac{\partial}{\partial x}f_2(x) &= 0,\\
2\,f_3(x) + 2\,x\frac{\partial}{\partial x}f_3(x) &= 0.
\end{aligned}$$

Nous calculons les solutions rationnelles de ce système, ce qui nous donne :

$$F = \frac{-c_0y^3 + 3(x-1)c_0y^2 + ((-3x^2-3)c_0 + xc_1)\,y + (x-1)^3c_0}{x}$$

où c_0 et c_1 sont des constantes arbitraires, et F/y est une constante générique pour P. En particulier, pour $c1 = 6c0$, on retrouve l'intégrale première que donne MACSYMA pour ce problème (taper USAGE(ODEFI) sous MACSYMA) :

$$\frac{(-y+x-1)^3}{xy}.$$

◇

Cet exemple montre que, pour calculer un $F \in \mathcal{S}_P$ tel que $DF = \alpha F$, on devrait d'abord chercher des candidats sur le facteur α. Cela peut se faire en cherchant des solutions singulières, ou (c'est le cas ici) quand il y a une solution particulière simple. Cette heuristique est valable pour des équations de tous ordres.
Une méthode similaire a récemment été proposée par Mansfield et Milne ([MMi95]). Notons aussi que la plupart des stratégies de calcul développées pour calculer des polynômes de Darboux de champs de vecteurs du plan (voir par exemple [PSi83, Sto88, Man94]) se généralisent immédiatement à un nombre arbitraire de variables.

Étudions maintenant le cas d'équations du premier ordre.

5. Polynômes de Darboux des champs de vecteur du plan

Dans cette partie, nous nous restreignons aux champs de vecteurs autonomes du plan, c'est-à-dire aux champs de vecteurs de la forme

$$\begin{cases} X' = P(X,Y) \\ Y' = Q(X,Y) \end{cases}$$

où $P, Q \in C[X, Y]$, ce qui revient à étudier la dérivation $D = P\frac{\partial}{\partial X} + Q\frac{\partial}{\partial Y}$. Dans ce cas, Nagata et Nowicki ont montré que l'anneau des constantes de D est finiment engendré ([Nag88]). Étudier de tels systèmes est bien sûr équivalent à étudier l'équation du premier ordre $P(X, Y)Y' = -Q(X, Y)$.

5.1. Le théorème de Darboux et la méthode de Prelle-Singer

Les champs de vecteurs du plan sont de fait le cadre qu'avait étudié Darboux [Darboux]. Il était arrivé au théorème remarquable ci-dessous (que nous donnons dans la présentation de Singer [Sin92]). On dit que (x_0, y_0) est un point non-singulier (singulier sinon) de D si $P(x_0, y_0) \neq 0$ ou $Q(x_0, y_0) \neq 0$.

Lemme 21 (Singer) [Sin92]. *Soit $D = P\frac{\partial}{\partial X} + Q\frac{\partial}{\partial Y}$ et (x_0, y_0) un point non-singulier de D. Soient H_1, H_2 deux polynômes de Darboux pour D tels que $H_1(x_0, y_0) = H_2(x_0, y_0) = 0$ et H_1 est irréductible. Alors, H_1 divise H_2.*

Théorème 22 (Darboux) [Darboux, Sin92]. *Considérons la dérivation $D = P\frac{\partial}{\partial X} + Q\frac{\partial}{\partial Y}$ et posons $d = \max(\deg(P), \deg(Q))$.*

1. *Si $G_1, \cdots, G_r$ sont des polynômes de Darboux irréductibles premiers entre eux, alors soit $r < \frac{d(d+1)}{2} + 2$, soit il existe des entiers n_i non tous nuls tels que $D\left(\prod_{i=1}^{m} G_i^{n_i}\right) = 0$.*
2. *Dans ce dernier cas, si G est un polynôme de Darboux irréductible et que C est algébriquement clos, alors soit G divise $pgcd(P, Q)$, soit il existe $(c_1, c_2) \in C^2 - \{(0, 0)\}$ telles que G divise $c_1 \prod_{n_i>0} G_i^{n_i} - c_2 \prod_{n_i<0} G_i^{-n_i}$.*

La première conséquence de ces résultats est que le degré des polynômes de Darboux est borné (pour les champs de vecteurs du plan). On ne connait pas de borne explicite en général ; pour les équations de Riccati, une borne s'obtient en utilisant la théorie de Galois différentielle (voir chapitre III) ; pour certains types de singularités, Cerveau et Lins-Netto donnent une borne intéressante dans [CLN91] (voir références incluses) ; enfin, si P et Q sont homogènes et de même degré, une borne s'obtient très simplement (voir plus bas).

Dans [PSi83], Prelle et Singer donnent une très élégante description des intégrales premières élémentaires de champs de vecteurs (c'est-à-dire celle qui sont obtenues dans des tours d'extensions algébriques, exponentielles ou logarithmiques, voir par exemple [WGOS] pour une définition précise) en termes de polynômes de Darboux. Par exemple, ils montrent le résultat suivant (propositions 1 et 2 pages 224), qui donne un facteur intégrant pour D :

Proposition 23 [PSi83]. *Si D admet une intégrale première élémentaire, alors il existe un entier n et un polynôme de Darboux R tels que $DR = -n(\frac{\partial P}{\partial x} + \frac{\partial Q}{\partial Y})R$*

La méthode de Prelle-Singer a été implantée en MACSYMA (et généralisée à certains corps de fonctions élémentaires) par B. Caviness et R. Stockhamer ([Sto88]), et en REDUCE par Y.K Man ([Man94, McM94]). Le fait de calculer des polynômes de Darboux pour obtenir des intégrales premières est d'ailleurs parfois popularisé comme "méthode de Prelle-Singer". Nous allons maintenant montrer comment simplifier le calcul des polynômes de Darboux pour les dérivations à deux variables.

La recherche de polynômes de Darboux est aussi liée au problème du centre, et a donné lieu a beaucoup de recherche dans cette direction (voir l'article de synthèse [Sch93] de D. Schlomiuk, et les références incluses).

5.2. Lemme de Collins-Christopher et variations sur la méthode de Prelle-Singer

Pour simplifier le calcul des polynômes de Darboux, commençons par étudier le cas où D est homogène (i.e P et Q sont homogènes et de même degré n). Dans ce cas, on peut décrire très simplement tous les polynômes de Darboux. D'abord, si C est algébriquement clos, tout polynôme en deux variables se factorise comme produit de facteurs linéaires sur C donc le degré maximum des polynômes de Darboux homogènes irréductibles est 1. Plus généralement, même si C n'est pas algébriquement clos, les polynômes de Darboux irréductibles sont donnés par le lemme suivant, qu'on peut attribuer indépendamment * à Collins ([Col93, McM94]) et à Christopher ([LP93], lemme 3.1). Le lemme ci-dessous apparaît sous une forme différente chez Collins, et nous en donnons une preuve originale simple.

Lemme 24 (Collins-Christopher). *Soit $D = P\frac{\partial}{\partial X} + Q\frac{\partial}{\partial Y}$ une dérivation homogène. Posons $W = XQ - YP$ et supposons que $W \neq 0$ (i.e D n'est pas un multiple de la dérivation d'Euler). Alors W est un polynôme de Darboux et tout polynôme de Darboux homogène irréductible (sur C) divise W.*

Preuve. - Utilisons la notation $P_X = \frac{\partial P}{\partial X}$ et $P_Y = \frac{\partial P}{\partial Y}$. Soit n le degré de P et Q ; alors, P et Q satisfont la relation d'Euler $XP_X + YP_Y = nP$. Donc :

$$\begin{aligned} DW &= X(PQ_X + QQ_Y) - Y(PP_X + QP_Y) \\ &= nPQ - YPQ_Y + XQQ_Y - nPQ + XQP_X - YPP_X \end{aligned}$$

* Je remercie M. Mac Callum et Y. Man d'avoir attiré mon attention sur ce résultat. Le lemme est également suggéré dans [MNS93], quoique non-explicitement

$$= \quad -(Q_Y + P_X)\,W.$$

Il en découle que W est un polynôme de Darboux (et donc que tous ses facteurs le sont). Réciproquement, soit F un polynôme de Darboux homogène et irréductible avec $DF = \alpha F$. Alors, en raisonnant comme ci-dessus, on trouve :

$$\begin{cases} (X\alpha - mP)F = -WF_Y \\ (Y\alpha - mQ)F = WF_X \end{cases}$$

Si $(X\alpha - mP)$ et $(Y\alpha - mQ)$ étaient simultanément nuls, alors nous aurions $W = 0$, donc nous pouvons supposer que $(Y\alpha - mQ)$ est non nul. Comme nous avons supposé F irréductible, ceci implique que F divides W. □

Exemple. - Considérons* la dérivation $D = (n+1)X\frac{\partial}{\partial X} + nY\frac{\partial}{\partial Y}$. Alors $W = XY$ et nous avons les deux polynômes homogènes irréductibles X et Y qui vérifient $DX = (n+1)X$ et $DY = nY$. On remarque que les facteurs de ces deux polynômes de Darboux verifient une relation de dépendance à coefficients entiers, donc X^n/Y^{n+1} est une intégrale première et, pour toute constante c non nulle, $X^n - cY^{n+1}$ est un polynôme de Darboux non-homogène irréductible pour D. Réciproquement, toutes les composantes homogènes d'un polynôme de Darboux non-homogène sont des polynômes de Darboux, donc sont obtenues par des produits des polynômes irréductibles donnés par le lemme.
Pour obtenir les éventuels polynômes de Darboux irréductibles non-homogènes d'une dérivation homogène, il suffit donc de chercher une relation de dépendance à coefficients entiers entre les facteurs des polynômes de Darboux homogènes et irréductible obtenus par le critère de Collins-Christopher. ⋄

Toute dérivation peut s'écrire comme une somme $D = D_- + \cdots + D_+$ de dérivations homogènes (de degrés croissant) ; Si F est un polynôme de Darboux, alors sa composante homogène F_+ de plus haut degré (resp. F_- de plus bas degré) est un polynôme de Darboux pour D_+ (resp. D_-) et le lemme de Collins-Christopher peut être appliqué à D_- et D_+ pour obtenir des candidats pour F_- et F_+. Bien sûr, cette méthode ne donne de résultats que si W_- et W_+ sont non nuls.

Exemple. - Considérons l'exemple suivant (dû à Mac Callum et Man, [McM94]). Soient $P = Y$ et $Q = Y^2 + 4X^2 + 4X$ sur $\mathbb{Q}$; Nous avons $W_+ = -X(4X^2 + Y^2)$ and $W_- = -(4X^2 + Y^2)$. Le degré minimal est 2 ; Donc, il n'y a pas de polynôme de Darboux de degré 1 et il y a un unique polynôme de Darboux de degré 2 (explicitement, $F = 4X^2 + Y^2$). En appliquant la procédure de Prelle-Singer comme dans [McM94], on trouve l'intégrale première $X + 1/2\log(4X^2 + Y^2)$. ⋄

Notons aussi que le lemme de Collins-Christopher peut servir à étudier des dérivations en un plus grand nombre de variables :

* Les remarques expliquées dans cet exemple m'ont été suggérées par une question de A. Astrelin

Exemple. - Soit la dérivation $D = Z(X^3 - Y^3)\frac{\partial}{\partial X} + (XY^2Z + Z^2)\frac{\partial}{\partial Y} + (Z - 3X)^2\frac{\partial}{\partial Z}$. Décomposant D comme une somme de dérivations homogènes, nous avons $D{=}D_1 + D_2$ où $D_1 = Z(X^3 - Y^3)\frac{\partial}{\partial X} + XY^2Z\frac{\partial}{\partial Y}$ et $D_2 = (Z^2)\frac{\partial}{\partial Y} + (Z - 3X)^2\frac{\partial}{\partial Z}$. Une condition nécessaire pour que D admette un polynôme de Darboux est que D_1 et D_2 admettent un polynôme de Darboux. Or, pour D_1 et D_2, nous pouvons appliquer le lemme de Collins-Christopher, avec l'hypothèse supplémentaire que le polynôme trouvé doit être homogène en X, Y, Z. Comme D_2 est homogène (en X, Y), nous trouvons que le terme de plus haut degré pour un polynôme de Darboux aurait $Z, Y, X^3 - X^2Y - Y^3$ comme seuls facteurs possibles. $\diamond$

6. Degré des polynômes de Darboux et perspectives

Dans cette partie, nous considérons un champs de vecteurs

$$(S) \; : \; \left\{ \begin{array}{rcl} Y_1' & = & Q_1(Y_1, \cdots, Y_n) \\ & \vdots & \\ Y_n' & = & Q_n(Y_1, \cdots, Y_n) \end{array} \right. \quad \text{où } \; Q_i \in C[Y_1, \cdots, Y_n] \text{ et } \; \mathbb{Q} \subset C$$

et la dérivation associée $D = \sum Q_i \frac{\partial}{\partial Y_i}$

Pour les polynômes de Darboux d'un tel système, la situation est moins bien connue. La section précédente a donné deux résultats utiles sur les polynômes de Darboux de champs de vecteurs du plan : le premier était que la donnée de suffisament de polynômes de Darboux engendre une intégrale première rationelle, le deuxième était que le degré est (au moins théoriquement) borné.

6.1. Polynômes de Darboux et intégrales premières

Si l'on examine la preuve du théorème 22, on voit que la partie 1) du théorème 22 reste vraie (à la borne près). Si $d = \max(\deg(Q_i))$, posons $N = \binom{n+d-1}{n}$. Si l'on dispose de $N+1$ polynômes de Darboux irréductibles G_i, alors les $\frac{DG_i}{G_i}$ sont des polynômes en n variables de degré au plus $d-1$; comme il y a exactement N monomes de degré au plus $d-1$ en n variables, les $N+1$ polynômes DG_i/G_i sont linéairement dépendants sur C. En suivant pas à pas la preuve de Singer du théorème 22 ([Sin92] p 687), on obtient finalement (à une réécriture idoine près) la proposition* suivante :

Proposition 25. *Soit $d = \max(\deg(Q_i))$. Alors D admet $\binom{n+d-1}{n} + n$ polynômes de Darboux premiers entre eux si et seulement si D admet une intégrale première rationelle.*

* Notons qu'un résultat analogue a été prouvé par Jouanolou pour les formes de Pfaff algébriques

Preuve. - Supposons que D admet $\binom{n+d-1}{n} + n$ polynômes de Darboux irréductibles G_i premiers entre eux, et posons $\alpha_i = D(G_i)/G_i$. Par construction, on a $\deg(\alpha_i) \leq d-1$. Les polynomes en n variables de degré au plus $d-1$ forment un C-espace vectoriel de dimension $N = \binom{n+d-1}{n}$.
Quite à renuméroter, supposons que $\alpha_1, \ldots, \alpha_l$ forment une base du C espace vectoriel formé par les α_i (notons que $l \leq N$). Alors, pour $j = N+1, \ldots, N+n$, nous avons n relations $\alpha_j = \sum_{i=1}^{l} r_{i,j}\alpha_i$ (où les $r_{i,j}$ sont dans C) que nous réécrivons $\sum_{i=1}^{N+n} r_{i,j}\alpha_i = 0$ (de cette façon, les vecteurs $(r_{i,j})_{i=1..N+n}$ sont linéairement indépendants sur C).
Suivant Singer, nous utilisons maintenant les résultats et notations de [Ros76]. Soient $K = C(Y_1, \ldots, Y_n)$ et $\mathcal{C} = \{c \in K | Dc = 0\}$ son corps de constantes. On pose $\omega_j = \sum_i r_{i,j}\frac{dG_i}{G_i} \in \Omega_{K/\mathcal{C}}$. À numérotation près, supposons que $Q_1 \neq 0$ (c'est à dire que $Y_1 \notin \mathcal{C}$) et posons $\overline{D} = (1/Q_1)D$. On vérifie que $\overline{D}^1(\frac{dG_i}{G_i}) = (1/Q_1)d(\alpha_i) + d(1/Q)\alpha_i$. Il en découle que $\overline{D}^1(\omega_j) = (1/Q_1)d(0) + d(1/Q).0 = 0$ et $\overline{D}^1(dY_1) = d(1) = 0$. Comme $\deg.\mathrm{trans}_{\mathcal{C}}(K) \leq n$, $\dim \Omega_{K/\mathcal{C}} \leq n$ et la proposition 6 de [Ros76] montre qu'il existe $c_0, c_1, \ldots, c_n \in \mathcal{C}$ non tous nuls tels que

$$\begin{aligned} 0 &= c_0 dY_1 + \sum c_i \omega_i \\ &= d(c_0 Y_1) + \sum_{i=1}^{N+n} \left(\sum_{j=1}^{n} c_j r_{i,j} \right) \frac{dG_i}{G_i} \\ &= d(c_0 Y_1) + \sum_{i=1}^{N} \left(\sum_{j=1}^{n} c_j r_{i,j} \right) \frac{dG_i}{G_i} + \sum_{i=N+1}^{N+n} c_{i-N} \frac{dG_i}{G_i} \end{aligned}$$

Alors, les $\sum_{j=1}^{n} c_j r_{i,j}$ sont non tous nuls (car sinon $c_1 = \ldots = c_n = 0$ donc $c_0 \neq 0$ et $Y_1 \in \mathcal{C}$ ce qui est contraire à nos hypothèses). Soit $(t_q)_{q=1,\ldots,\rho}$ une base du $\mathbb{Q}$-espace vectoriel engendré par les $(\sum_j r_{i,j}c_j)_{i=1,\ldots,N+n}$. On a

$$\sum_{j=1}^{n} r_{i,j} c_j = \frac{1}{\nu} \sum_{q=1}^{\rho} p_{i,q} t_q$$

où $\nu, p_{i,q} \in \mathbb{Z}$. Si nous posons $F_q = \prod_{i=1}^{N+n} G_i^{p_{i,q}}$, alors

$$d(c_0 Y_1) + \sum_{q=1}^{\rho} \frac{t_q}{\nu} \frac{dF_q}{F_q} = 0.$$

La proposition 4 de [Ros76] montre alors que chaque F_q est algébrique sur $\mathcal{C}$. D'après le lemme 6, chaque F_q satisfait $\overline{D}(F_q) = D(F_q) = 0$. Comme les $\sum r_{i,j}c_j$ ne sont pas tous nuls, un des $p_{i,q}$ est non nul, disons $p_{1,1}$. Et comme les G_i sont premiers entre eux, F_1 est alors l'intégrale première rationnelle annoncée.
Réciproquement, supposons que D admet une intégrale première rationnelle F/G avec F et G premiers entre eux. Si c est une indéterminée, le polynôme $F - cG \in k[c, Y_1, \cdots, Y_n]$ est irréductible. Comme k est de caractéristique zéro, $k[c, Y_1, \cdots, Y_n]$ est un anneau Hilbertien ([Lan83], page 226). Il y a donc une infinité de valeurs de $\tilde{c} \in C$ telles que le polynôme de Darboux $F - \tilde{c}G$ soit irréductible, ce qui donne autant de polynômes de Darboux premiers entre eux qu'on le souhaite. □

6.2. Degré des polynômes de Darboux

Dans son livre [Jou79], Jouanolou définit une notion de polynôme de Darboux pour les formes de Pfaff algébriques ([Jou79] pages 81,83,99). Il montre ensuite l'analogue du lemme 21 et du théorème 22 (pages 100 à 106) pour les formes de Pfaff en un nombre quelconque de variables. Dans le cas de deux variables, son cadre et le notre coïncident ; dans le cas de trois variables homogène (i.e les Q_i sont tous homogènes de degré 3), on peut construire une forme de Pfaff "associée" à notre système (voir par exemple [MOl92] page 3). En quatre variables, une telle identification n'est plus possible et, contrairement à une confusion très répandue dans la littérature, les résultats de Jouanolou ne s'appliquent plus à notre cadre. La question de savoir quand le degré des polynômes de Darboux irréductibles de D est borné est donc, à ma connaissance, ouverte dans le cas général.

Il y a des réponses (négatives) au problème du degré pour le sous-problème suivant. Soit $A = C[Y_1, \cdots, Y_n]$ et D une C-dérivation de A : l'anneau A^D des constantes de D dans A (les intégrales premières polynomiales) est-il finiment engendré ?

En adaptant le contre-exemple de Nagata au $14^{\text{ème}}$ problème de Hilbert, Derksen a construit une dérivation d'un anneau de polynômes à 32 variables dont l'anneau des constantes n'est pas finiment engendré ([Der93]) ; en particulier, le degré des générateurs ne peut pas être borné. En utilisant aussi le contre-exemple de Nagata, nous donnerons un autre contre-exemple (proposition 63 page 75) dans le chapitre II. Enfin, construisant sur un contre-exemple de Roberts au $14^{\text{ème}}$ problème de Hilbert ([Rob90]), Deveney et Finston montré que l'anneau des intégrales premières polynomiales de la dérivation

$$D = Y_1^3 \frac{\partial}{\partial Y_4} + Y_2^3 \frac{\partial}{\partial Y_5} + Y_3^3 \frac{\partial}{\partial Y_6} + (Y_1 Y_2 Y_3)^2 \frac{\partial}{\partial Y_7}$$

de $C[Y_1, \cdots, Y_7]$ n'est pas finiment engendré. On peut aussi montrer que l'anneau des intégrales premières de la dérivation

$$D = Y_0^3 Y_1^3 \frac{\partial}{\partial Y_4} + Y_0^3 Y_2^3 \frac{\partial}{\partial Y_5} + Y_0^3 Y_3^3 \frac{\partial}{\partial Y_6} + (Y_1 Y_2 Y_3)^2 \frac{\partial}{\partial Y_7}$$

de $C[Y_0, Y_1, \cdots, Y_7]$ n'est pas finiment engendré, ce qui montre que même l'homogénéité ne suffit pas à garantir une borne sur le degré. Dans ces deux exemples, tout polynôme en X_1, X_2, X_3 est (entre autres) un polynôme de Darboux et on peut donc avoir des polynômes de Darboux irréductibles de degré arbitrairement élevé. Nous sommes amenés à poser le problème suivant :

Problème 26. Caractériser les classes de dérivations pour lesquelles le degré des polynômes de Darboux irréductible est borné, et donner une borne effective le cas échéant. Donner des classes de dérivations pour lesquelles on sache borner le degré d'un polynôme de Darboux de degré minimum.

Dans le cas des champs de vecteurs plans, la borne (théorique) sur le degré des polynômes de Darboux irréductibles est obtenue grâce au lemme 21 ; un sous-problème du problème précédent est donc : peut-on caractériser d'autres classes de champs de vecteurs dont les polynômes de Darboux aient une propriété analogue au lemme 21 ?

6.3. Perspectives

Ces résultats négatifs ne doivent pas nous rendre trop pessimistes car, même si une borne existait, il est fort probable qu'elle serait trop grande pour être utilisée en pratique pour établir un algorithme général de détermination des polynômes de Darboux. D'autres approches semblent donc s'imposer, et nous en mentionnons quatre qui nous semblent significatives :

Dans [MNS93], Moulin Ollagnier, Nowicki, et Strelcyn développent une méthode (à partir d'une idée de Levelt) qui montre comment une étude arithmétique en des points donnés (les "points de Darboux") permet de décider la non-existence de polynômes de Darboux. L'idée force de cette approche (comme de la suivante) est que l'existence et le degré des polynômes de Darboux est intimement liée à des notions de géométrie algébrique.

Dans [CLN91], Cerveau et Lins-Netto montrent comment, en présence d'un certain type de singularités, on peut borner le degré des polynômes de Darboux de dérivations à deux variables (voir aussi [CM82]).

Dans [Dra37], Drach donne une méthode pour borner le degré des polynômes de Darboux des équations de Riccati du premier ordre de la manière suivante. Il montre que certaines transformations permettent, à partir d'un polynôme de Darboux, d'en construire d'autres de plus grand degré* ; pouvant calculer ainsi suffisamment de polynômes de Darboux, il obtient une intégrale première rationnelle dont le degré dépend du degré du polynôme initial ; utilisant un analogue du théorème 22.2, il arrive à en déduire des conditions arithmétiques qui bornent le degré du polynôme de Darboux initial**. Notons que, dans ce cas, les mêmes bornes sont aussi données par la théorie de Galois différentielle (voir le chapitre III). Il paraît donc raisonnable de penser que la présence de tels "constructeurs" de polynômes de Darboux soit liée à l'existence de "symétries" de l'équation.

Enfin, pour les systèmes comportant des paramètres, il faut noter que beaucoup d'outils ont été développés en automatique théorique (voir, par exemple, [Oll90]) qui permettent de caractériser l'existence ou non d'intégrales premières.

Il ressort de ce premier chapitre que ces quatre approches sont probablement les plus pleines de promesses optimistes pour l'étude des système différentiels par la méthode des

* Nous donnerons de telles transformations pour les équations linéaires ou de Riccati de tout ordre au chapitre II

** À vrai dire, la note originale contient beaucoup d'erreurs, mais on peut la rendre correcte.

polynômes de Darboux quand il y a plus de deux variables. Nous allons maintenant donner, dans le chapitre qui suit, une description nettement plus aboutie pour les systèmes différentiels linéaires homogènes à coefficients rationnels.

CHAPITRE II

Intégrales premières de systèmes différentiels linéaires

Dans ce chapitre, on étudie les intégrales premières rationnelles et liouvilliennes des systèmes différentiels linéaires homogènes. Nous montrons comment ce problème se réduit à l'étude de polynômes de Darboux d'une forme 'simple'.

Nous montrons comment interpréter les coefficients des polynômes de Darboux en fonction des solutions du système ; ceci produit une correspondance entre les polynômes de Darboux et les semi-invariants d'un groupe de Galois différentiel et nous donne des indications sur les degrés possibles pour les polynômes de Darboux (particulièrement dans le cas de groupes réductifs).

Nous indiquons ensuite un algorithme de calcul et plusieurs améliorations pour le rendre efficace ; comme application, nous montrons comment la connaissance d'un polynôme de Darboux permet de calculer des invariants du groupe de Galois différentiel du système et d'en déduire des solutions algébriques quand le groupe est fini.

Les parties 1 à 4 de ce chapitre sont parues dans [Wei95] et ont été maintenues dans leur langue originale.

---

1. Introduction

Consider the equation $L(y) = y'' + y = 0$. If y is any solution of $L(y) = 0$, it is easy to verify that the total derivative of $(y')^2 + y^2$ is zero. Thus, for any solution y of $L(y) = 0$, there will exist some constant c such that $(y')^2 + y^2 = c$. In that case, we say that $(y')^2 + y^2$ is a *first integral* of L (see below for some more precise definitions). The aim of this chapter is two-fold. First, we will perform a systematic study of first integrals of linear differential systems and propose procedures allowing one to decide whether or not a given system of linear differential equations admits a first integral ; and secondly, we will show how this may help caracterizing the solutions (or the Galois group).

Our strategy to compute first integrals will be to use of the notion of Darboux polynomials (see definition below or chapter I). In [Wei94], we gave a partial procedure for computing Darboux polynomials of given degree for linear differential equations; as systems can be converted to equations, this theoretically included the case of systems. However, this conversion produces intermediate equations with "huge" coefficients, so in this chapter we show how to handle systems directly (without converting to equations); we also study how

to make good use of some degenerate situations, which improves our first algorithm from the practical point of view.

In general, finding the degree of Darboux polynomials is a very difficult problem (see e.g [MNS93], or chapter I). The main result of this chapter is the ability to characterize the Darboux polynomials and their degree by relating them bijectively with the semi-invariants of the differential Galois group. Thus, all results from invariant/representation theory are at our disposal and this provides bounds on the degrees of the Darboux polynomials in many cases.

This chapter is organized as follows: in the rest of this section, we recall some of the properties of the Darboux polynomials of linear differential systems; in section 2, we give a characterization of the coefficients of the Darboux polynomials (proposition 33); in section 3, we show how this characterization provides a correspondence between the Darboux polynomials and the semi-invariants of the differential Galois group (theorem 38). In section 4, we use this material to design computational procedures; in section 5, we develop some structure results on the kind of Liouvillian extensions that are needed for our purposes; in section 6, we expose some remarks to considerably fasten the computation and use them to improve the Singer-Ulmer algorithm for computing algebraic solutions; in section 7, we deal with the degree problem and we then conclude this chapter on some comments and open questions. Sections 1 to 4 of this chapter have appeared in [Wei95];

Remark. - Throughout this chapter, we will study a matrix differential system $Y' = AY$ and call $y_1, \cdots, y_n$ the entries of a solution Y. However, in the implementation we denoted the entries of Y by $y_0, \cdots, y_{n-1}$ (to be coherent with the case of an n-th order linear differential equation); thus, in all our examples, the entries of Y will be denoted by $y_0, \cdots, y_{n-1}$. I hope that this slight contradiction will not disturb the reader. $\diamond$

1.1. Rational first integrals

Let (k, ∂_k) be a differential field with an algebraically closed* constant field $\mathcal{C}$; we will often denote the derivation by the usual symbols ', ", etc. We assume that k has the following property: given a linear differential equation L with coefficients in k, we must have an algorithm that finds the rational and the exponential solutions of L over k (recall that a solution is called exponential over k if its logarithmic derivative lies in k). An example of such a field is $C(x)$, where C is any number field of characteristic 0, with the usual derivation $\frac{d}{dx}$ (see [Br92b, ABP95], and [Sin91] for a wider class of fields).

* This assumption will usually not be used for practical computations, but it is absolutely necessary to prove theorems using differential Galois theory.

In this chapter, we consider the following first order linear differential system:

$$(A): \qquad Y' = AY \quad \text{with} \quad A \in \mathcal{M}_{n,n}(k) \tag{1.1}$$

In what follows, if B is a matrix, the notation (B) will denote the system $Y' = BY$. Let us first introduce the notion of rational first integral. One can algebraically model a "generic solution" of the system (A) the following way. Consider some indeterminates $(y_1, \ldots, y_n)$ and form the field $k(y_1, \ldots, y_n)$. Let A_i denote the i-th row of A and let $Y = (y_1, \cdots, y_n)^t$. Then, one can form the derivation

$$D_k = \partial_k + A_1 Y \frac{\partial}{\partial y_1} + A_2 Y \frac{\partial}{\partial y_2} + \ldots + A_n Y \frac{\partial}{\partial y_n} \tag{1.2}$$

where ∂_k denotes the derivation of the coefficients of an element of $k(y_1, \ldots, y_n)$. This derivation turns $k(y_1, \ldots, y_n)$ into a differential field of rational functions on solutions of (A). Thus, we will say that an element $M \in k(y_1, \ldots, y_n)$ (with $M \notin \mathcal{C}$) is a *rational first integral* for (A) if $D_k M = 0$ (i.e, for any solution Y of (A), $M(Y)$ is a constant). When no confusion is possible, we will simply write D instead of D_k.

1.2. The Darboux polynomials of (A)

Consider the ring $k[y_1, \ldots, y_n]$; this is also turned into a differential ring by D. Suppose that $M \in k(y_1, \ldots, y_n)$ is a rational first integral of (A). Then, M can be written as a quotient $M = \frac{F}{G}$ with $F, G \in k[y_1, \ldots, y_n]$ and F, G relatively prime. Then, $DM = 0$ implies that $D(F)G - D(G)F = 0$. This in turn implies that F divides DF. In other terms, there exist $\alpha \in k[y_1, \ldots, y_n]$ such that $DF = \alpha F$.

Definition 27. Let $F \in k[y_1, \ldots, y_n]$. We say that F is a *Darboux polynomial* for (A) if there exists $\alpha \in k[y_1, \ldots, y_n]$ such that $DF = \alpha F$.

Relating the search for first integrals to the computation of Darboux polynomials is an old method; we now recall some of the essential properties of Darboux polynomials (see the previous chapter for more details and references). Let $\mathcal{S}_{A,k}$ denote the set of the Darboux polynomials for (A) with coefficients in k (denoted simply $\mathcal{S}$ when no confusion is possible). Then, any element of k is obviously in $\mathcal{S}$. Also note that, if $k \subset K$ and $M \in k[y_1, \ldots, y_n]$ is Darboux for D_K, then M is Darboux for D_k (see chapter I).

Lemme 28. *The set $\mathcal{S}$ of Darboux polynomials is a semi-group: if $F, G \in \mathcal{S}$, then $FG \in \mathcal{S}$. Moreover, if $F \in \mathcal{S}$ then all its irreducible factors are in $\mathcal{S}$.*

Thus, to describe $\mathcal{S}$, it will be enough to compute its irreducible elements. In the case of the derivation D defined above, we have additional information because D is a

homogeneous and degree 0 application: if one picks a monomial of degree m in the y_i, then its derivative (by D) is easily seen to be a homogeneous polynomial of the same degree m. As a consequence (Chapter I, lemma 13 page 22).

Lemme 29. *If M is a Darboux polynomial for (A) verifying $DM = \alpha M$, then $\alpha \in k$ and every homogeneous component M_i of M (taken as a multivariate polynomial in the y_i) also verifies $DM_i = \alpha M_i$.*

In the sequel, this lemma will allow us to consider only homogeneous irreducible Darboux polynomials. Before we introduce our next structure lemma, we need a definition:

Definition 30. A differential extension $K \supset k$ is called a *Liouvillian* extension if there exists a tower of extensions $k = k_0 \subset k_1 = k(\theta_1) \subset \ldots \subset k_n = k(\theta_1, \cdots, \theta_n) = K$ such that we have θ_i algebraic over k_{i-1} or $\theta_i' \in k_{i-1}$ or $(\theta_i')/\theta_i \in k_{i-1}$ (for all $i = 1, \cdots, n$).
An element is said to be Liouvillian over k if it belongs to a Liouvillian extension of k.
We will say that (A) has a *Liouvillian first integral* if it has a polynomial first integral over a Liouvillian extension of k.

We refer the reader to [Sin89, Sin81, SUl93b, UWe94, Kap57, Ber86] for more properties of Liouvillian extensions; see also [Sin92], where a more general definition of Liouvillian first integrals is studied. In the sequel, we will use the following structure result, that we prove in section 5.

Proposition 31. *Let $k_1 \supset k$ be a Liouvillian extension of k. Then, the derivation D_{k_1} admits a Darboux polynomial over k_1 if and only if D_k admits a Darboux polynomial over k.*

Proof. - see section 5. □

Remark. - Note that, if $DM = \alpha M$ and $f' = -\alpha f$, then $D(fM) = 0$. If $f \in k$, then this means that fM is a polynomial first integral of (A); else, this means that $\alpha = e^{\int f}$ and fM is a Liouvillian first integral of (A). In fact proposition 31 shows that, for us, these will be the only interesting type of Liouvillian first integrals. ◇

2. Duality and Darboux polynomials

In this section, we will show how to characterize the Darboux polynomials in terms of constructions on the matrix A. This will enable us to interpret the coefficients of Darboux

polynomials as functions of solutions of (A). From now on (by lemma 29), the word "Darboux polynomial" will always mean *homogeneous* Darboux polynomial.

2.1. Solutions.

Let us first focus on the notion of solutions. In the case of a linear differential system, there is a notion of minimal differential extension containing a fundamental set of solutions of (A):

Definition 32. A differential field extension $K \supset k$ is said to be a *Picard-Vessiot extension* for (A) if

1 $K = k(Y_{1,1}, \ldots, Y_{1,n}, \ldots, Y_{n,n})$, where $Y_1, \ldots, Y_n$ is a fundamental set of solutions of (A) (i.e K is the differential field obtained by adjoining to k the components of the vectors $Y_1, \ldots, Y_n$).
2 K and k have the same field of constants.

As the constant field of k is algebraically closed of characteristic 0, one can show that Picard-Vessiot extensions exist and are unique up to differential isomorphism ([Kap57] p.21 and [Kol48b, Kol48a]). In the sequel, the term "solution" will always denote a solution in the Picard-Vessiot extension K.

Consider the n-dimensional $\mathcal{C}$-vector space V of solutions of (A) and denote by U a *fundamental solution matrix* (i.e the columns w of U are solutions of $w' = Aw$ and they span V). We will call *construction on* V a vector space obtained from V by successive use of the following operations: taking the dual, tensor products, direct sums, symmetric and exterior powers. To any construction $Const(V)$, there is a corresponding linear differential system having $Const(V)$ as its solution space (see e.g [Ber86, MRa89]). In this chapter, we only use the dual and the symmetric powers, which we will now make explicit for the reader's convenience.

2.2. The dual system.

We construct a system whose solution space is isomorphic to V^*, the dual space of V. Indeed, consider the inverse transpose matrix $(U^{-1})^t$; it is well defined because the columns of U span V and thus $\det(U)$ does not vanish. Then, for any column w_i of U and any column v_i of $(U^{-1})^t$, we have by construction $\langle v_i, w_j \rangle = \delta_{i,j}$ (the Kronecker symbol); it follows that the columns of $(U^{-1})^t$ span V^*. Now, using the relation $U.U^{-1} = I$, one easily finds that

$(U^{-1})^t$ satisfies $Y' = -A^tY$; in the sequel, we will use the notation $A^* = -A^t$ to denote the matrix of a dual system.

2.3. Symmetric powers.

Let $Y = (y_1, \cdots, y_n)^t$ denote a solution of $Y' = AY$. If we consider a monomial M of degree m in the y_i, then DM is a linear combination of monomials of degree m. As there are $\nu = \binom{n+m-1}{n-1}$ possible monomials of degree m in n variables, we obtain that the vectors $w = (y_1^m, \cdots, y_{n-1}y_n^{m-1}, y_n^m)$ of all monomials of degree m in the y_i satisfy a $\nu \times \nu$ system which we denote by $Y' = S^m(A)Y$. The reason for this notation is that one can show ([BBH88]) that its ν-dimensional solution space is isomorphic to $S^m(V)$, the m-th symmetric power of V (see e.g [Lan92] p. 635 for definition and properties of symmetric powers).

2.4. Back to Darboux polynomials.

These constructions enable the following characterization of Darboux polynomials:

Proposition 33. *The system (A) admits a Darboux polynomial of degree m with a vector v of coefficients if and only if there exists a non-zero f exponential over k (i.e $f'/f \in k$) such that fv is a solution of the system $Y' = (S^m(A)^*)Y$.*

Proof. - Let $M = v_\nu y_n^m + v_{\nu-1}y_n^{m-1}y_{n-1} + \ldots + v_1 y_1^m$ be a polynomial first integral of (A) and let v denote its coefficient vector (i.e $v = (v_1, \cdots, v_\nu)$). Then, for any solution Y of (A), we have $M(Y) \in C$. But now, if we let $w = (y_1^m, \cdots, y_{n-1}y_n^{m-1}, y_n^m)$, then we have $M(Y) = \langle v, w\rangle$; thus, we obtain $\langle v, w\rangle \in C$ and thus $v \in S^m(V)^*$. It follows that v is a rational solution of $(S^m(A)^*)$ if and only if M is a polynomial first integral.
Now, let M be a homogeneous Darboux polynomial of degree M with $DM = \alpha M$ and let v denote the vector of its coefficients. Consider a minimal extension $k_1 = k(f)$ of k containing an element f such that $f' = -\alpha f$ (i.e if k contains such an element, then $k_1 = k$). Then, it is immediately seen that $D(fM) = 0$. Thus, the above construction shows that fv is a solution of the system $Y' = (S^m(A)^*)Y$. Conversely, suppose that fv is a solution of the system $Y' = (S^m(A)^*)Y$ with f exponential over k ($f \neq 0$) and $v \in k^\nu$; let M denote as above the polynomial whose coefficient vector is v. The relation $D(fM) = 0$ is then clearly equivalent to $DM = -\frac{f'}{f}M$ and we are done. □

Remark. - Using the language of vector spaces with a connection, some ideas in this direction were also suggested in [Mor94]. ◇

This characterization will be the key point for the algorithm of section 4. In the following section, we will show how it may also provide a characterization of the degrees of the Darboux polynomials.

3. Darboux polynomials and semi-invariants of the differential Galois group

In this section, we recall and state some useful notions about differential Galois theory (see e.g [Kap57, Sin89, MRa89, Ber86]). In particular, we will show the link between first integrals and semi-invariants of the differential Galois group; only the new results are proved.

3.1. Differential Galois theory

Many of the properties of the solutions of (A) derive from the fact that there is a group action on the vector space of solutions that induces a "differential Galois theory". To follow the frame of classical Galois theory, the Picard-Vessiot extensions will play the role of a splitting field for (A).

Definition 34. The differential Galois group of a differential extension $K \supset k$ is defined as the group of automorphisms of K that commute with the derivation and that leave k pointwise fixed.
The *differential Galois group* G of (A) is defined as the differential Galois group of K/k, where K is a Picard-Vessiot extension of k for (A).

The main property that we will use is the following standard lemma (see e.g [Sin89, SUl93a]):

Lemme 35. *If $y \in K$, then $y \in k$ if and only if $g(y) = y$ for all $g \in G$. If $y \neq 0$, then $y'/y \in k$ if and only if for all $g \in G$ there exists a constant $\psi_y(g) \in C$ such that $g(y) = \psi_y(g)y$.*

If we choose a fundamental set of solutions $\{Y_1, Y_2, \ldots, Y_n\}$ of the system (A), then for each $\sigma \in G$ we get $\sigma(Y_i) = \sum_{j=1}^{n} c_{ij} Y_j$, where $c_{ij} \in \mathcal{C}$. This gives a faithful representation of G as a subgroup of $GL(n, \mathcal{C})$ (in fact, G is a linear algebraic subgroup of $GL(n, \mathcal{C})$). Different choices of bases give equivalent representations. In the sequel, we always consider this equivalence class of representation as *the* representation (module) of G.

Let V be again the solution space of (A); the action of G induces a structure of G-module on V. One can show that any construction on V is also a G-module ([MRa89] p.134) and

that a Picard-Vessiot extension contains a copy of any G-module ([Sin93], theorem 3.9). For example, G acts naturally on the dual V^* and on $V \otimes V$ in the following way. Let $g \in G$ and σ be its representation on V; the action of G on V^* is defined by $\langle g(u), y\rangle = \langle u, g^{-1}(y)\rangle$ for $u \in V^*, y \in V$ (see e.g [Ber86, MRa89]). The representations of g on V^* and on $V \otimes V$ are respectively $(\sigma^{-1})^t$ and $\sigma \otimes \sigma$. The reader may consult [Sin89, Kap57, Kol73, MRa89] for proofs and more properties of the Galois group.

Computing the Galois group is, in general, an open problem. Algorithms exist for n=2 ([UWe94, SUl93a, Kov86] and references therein) and n=3 ([SUl93a]); see also [MRa89] for a survey of other important methods.

Systems of the same type.

Consider the system $Y' = AY$ and suppose we perform a change of variables $Z = PY$ with $P \in GL(n, k)$. Then,

$$Z' = PY' + P'Y = (PAP^{-1} + P'P^{-1})Z. \tag{3.1}$$

We will say that two systems are *of the same type* (or *equivalent*) if such a relation (with P invertible) holds between them.

Note that if U is a fundamental matrix for (A), then PU is a fundamental matrix for $(PAP^{-1} + P'P^{-1})$ and the entries of PU are in the same Picard-Vessiot extension as those of U. Looking at the way the Galois group acts on the solutions, we get a standard property that will be crucial in the sequel: two systems of the same type have the same Galois group (see, e.g [MRa89] or lemmas 2.5 and 2.6 in [Sin94]).

In the sequel, the operation of changing to a system of the same type will be called a *G-change of variables*. A property that we will use without further mention is the following intuitive lemma:

Lemme 36. *Let $\tilde{\phi} : y \mapsto \tilde{y}$ be a G-change of variable. Then, the system (A) has a Darboux polynomial M if and only if $\tilde{\phi}(M)$ is a Darboux polynomial for $(\tilde{A})$.*

Proof. - If V and $\tilde{V}$ are isomorphic G-modules, then $S^m(V^*)$ and $S^m(\tilde{V}^*)$ are also isomorphic G-modules. Thus, the systems $S^m(A)^*$ and $S^m(\tilde{A})^*$ are equivalent and one has a solution fv with $f'/f \in k$ if and only if the other one has the solution $f\tilde{v}$. □

Equations and systems.

For algorithmic issues, we sometimes need to convert systems to equations and vice-versa. We now briefly review the standard ways of performing this task (see also [MRa89, Ber86]).

Consider an ordinary homogeneous linear differential equation

$$L(y) = y^{(n)} - a_{n-1}y^{(n-1)} - \cdots - a_1 y' - a_0 y = 0 \qquad (a_i \in k). \tag{3.2}$$

Then, solving this equation is equivalent to solving the companion system

$$\begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_{n-1} \\ y_n \end{pmatrix}' = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_{n-1} \\ y_n \end{pmatrix}$$

Conversely, suppose that $(y_1, y_2, \cdots, , y_n)$ satisfy a homogeneous first order linear differential system (A) of size n. To find an equation associated with (A), we would like to find a system of the same type (in the above sense) in companion form; this is done by the following cyclic vector process (see e.g [Bar93, MRa89, Ber86] for references and other methods). Consider $\Lambda \in k^n$ and let $z_1 = \Lambda Y = \lambda_1 y_1 + \ldots + \lambda_n y_n$. We compute $z_2 = z_1', \ldots, z_{n+1} = z_1^{(n)}$ by using the relation $Y' = AY$. We obtain $n+1$ linear expressions in the n variables y_i and so they are linearly dependant: this provides a linear differential equation $\mathcal{L}(z_1) = 0$ for z_1. Letting $Z = (z_1, \cdots, z_n)^t$, we now have a relation $Z = PY$ and $Z' = BY$; If the matrix P is invertible, Λ is called a *cyclic vector* for the system and $Z' = (BP^{-1})Z$ is a companion system of the same type as (A). It can be shown (see e.g [Ram85]) that the cyclic vectors form a non-empty Zariski open set, and that almost all choices of Λ will fit.

Thus, in the following, everything that is stated for first order systems is valid for n-th order equations and vice-versa (for example, we call Darboux polynomial of an equation a Darboux polynomial of the associated companion system).

3.2. Invariants and semi-invariants of the differential Galois group

We now show how to characterize Darboux polynomials in terms of representation of the Galois group. Let V be a $\mathcal{C}$ vector space with basis $y_1, \ldots, y_n$ and $G \subseteq GL(V)$ a linear group. One defines an action of G on the symmetric algebra $S(V)$ of V ($S(V) \approx k[Y_1, \ldots, Y_n]$) by $g \cdot (p(Y_1, \ldots, Y_n)) = p\,(g(Y_1), \ldots, g(Y_n))$.

Definition 37. A polynomial P with the property that

$$\forall g \in G, \quad g\,(P(Y_1, \ldots, Y_n)) = \psi_P(g) \cdot (P(Y_1, \ldots, Y_n))\,, \text{ with } \psi_P(g) \in \mathcal{C} \tag{3.3}$$

is called a *semi-invariant* of G of degree $\deg(P)$ (where $\deg(P)$ is the total degree). If $\forall g \in G$ we have $\psi_P(g) = 1$, then $P(Y_1, \ldots, Y_n)$ is called an *invariant* of G.

Remark. - This definition of invariants is the classic one. However, several authors also call invariants elements of *any* construction on V that are left invariant by G. $\diamond$

Remark. - By abuse of language, we shall speak of invariants of a group. Of course, this means that we consider the invariants of a representation of the group, and that it is clear in the context which representation we are studying $\diamond$

As the action of G is homogeneous, the invariants (resp. semi-invariants) are generated by homogeneous invariants (resp. semi-invariants). Therefore, they will be found in the symmetric powers $S^m(V)$ of V. From the definition, we get the following nice characterization of Darboux polynomials:

Theorem 38. *Let G_* denote the differential Galois group of the system $Y' = A^*Y$. Up to scalar multiplication, there is a one to one correspondence between the Darboux polynomials (resp. polynomial first integrals) of (A) and the semi-invariants (resp. invariants) of G_*.*

Proof. - Let M be a Darboux polynomial of degree m and denote by $Sol(S^m(A)^*)$ the solution space of $(S^m(A)^*)$; by construction (and lemma 42), we have a G_*-isomorphism $\phi_m : S^m(V^*) \mapsto Sol(S^m(A)^*)$. By proposition 33, the vector v of coefficients of M is such that there exists f with $f'/f \in k$ and $f.v \in Sol(S^m(A)^*)$; thus, if we call $z_1, \cdots, z_n$ a basis of V^*, there exists some homogeneous $P(z_1, \cdots, z_n) \in S^m(V^*)$ such that $\phi_m(P) = f.v$. By lemma 35, v is left fixed by G_* and, for all $g \in G_*$, there exists a constant $\psi(g)$ such that $g(f) = \psi(g)f$. As ϕ_m commutes with any $g \in G_*$, we deduce that $g(P) = \psi(g)P$ for all $g \in G_*$ and so P is a semi-invariant.
Conversely, let P be a semi-invariant and put $u = \phi_m(P)$ (i.e $u = (u_1, \cdots, u_\nu) \in Sol(S^m(A)^*)$). Select i such that $u_i \neq 0$. For all $g \in G$, we have $g(u) = \psi(g)u$ so that $g(u_i) = \psi(g)u_i$. If we put $f = u_i$, lemma 35 show that $f'/f \in k$. Now, for all $j = 1, \cdots, \nu$, we have $g(\frac{u_j}{f}) = \frac{\psi(g)}{\psi(g)}\frac{u_j}{f}$. Therefore, if we let $v = (u_1/f, \cdots, u_\nu/f)$, we have $v \in k^\nu$ such that $f.v \in Sol(S^m(A)^*)$ and proposition 33 shows that v is the vector of coefficients of a Darboux polynomial. $\square$

This result allows us to use representation theory to find bounds on the degree of Darboux polynomials. For systems that have a Liouvillian solution, bounds have been given by Singer ([Sin81]) and improved/generalized by Ulmer ([Ulm92, SUl93b]). Using representation theory, Singer and Ulmer have obtained sharp bounds for $n = 2$ and $n = 3$ (for $n = 2$ older bounds existed, see the references in [SUl93b, UWe94]). For systems of size $n > 3$, we don't know yet how to bound the degree of a semi-invariant of minimal degree in all cases: this is still an interesting (difficult) open problem (see the corresponding section below).

3.3. Invariants of completely reducible systems.

In this part, we show that, with an assumption on the Galois group, one can restate the above theorem directly in terms of G instead of G^*. Let V be a C-vector space and $G \in GL(V)$. We denote by $\mathrm{Inv}_V(G)$ the G-subspace of elements of V that are left invariant by all elements of G. We will say that G is *reductive** (or *completely reducible*) if all constructions on V are completely reducible G-modules (i.e any G-invariant subspace has a complementary G-invariant subspace); we say that a system is completely reducible if it has a reductive Galois group.

Proposition 39. *Consider a linear differential system with a reductive Galois group G and solution space V; let G_* denote the Galois group of the dual system whose solution space is V^*. Then, G has s invariants (resp. semi-invariants) of degree m if and only if G_* has s invariants (resp. semi-invariants) of degree m.*

In order to prove this, we will need the following three lemmas:

Lemme 40. *The invariants of G on V^* satisfy* $\mathrm{Inv}_{V^*}(G) = \mathrm{Hom}_G(V, \mathcal{C})$

Proof. - We have $u \in \mathrm{Hom}_G(V, \mathcal{C})$ if and only if $\langle u, g(y)\rangle = g(\langle u, y\rangle)$ for all $y \in V$ and all $g \in G$. As $\langle u, y\rangle \in \mathcal{C}$, we have $g(\langle u, y\rangle) = \langle u, y\rangle$. Now, we have $\langle u, g(y)\rangle = \langle g^{-1}(u), y\rangle$, and thus: $\langle u, g(y)\rangle = g(\langle u, y\rangle)$ if and only if $u = g^{-1}(u)$ for all $g \in G$, which is true if and only if u is an invariant of G in V^*. □

Lemme 41. *Suppose that G is reductive. Then,* $\mathrm{Inv}_{V^*}(G)$ *is G-isomorphic with* $\mathrm{Inv}_V(G)$.

Proof. - Let $V_1 = \mathrm{Inv}_V(G)$. As G is reductive, there exist a G-submodule V_2 such that $V = V_1 \oplus V_2$. We embed V_1^* into V^* by letting $u_1 \in V_1^*$ send V_2 to 0, so that $V^* = V_1^* \oplus V_2^*$. Consider $u \in V_1^*$. Any $y \in V$ can be expressed as $y = y_1 + y_2$ with $y_i \in V_i$; thus, $g(\langle u, y\rangle) = \langle u, y\rangle = \langle u, y_1\rangle$. Now, we have $\langle u, g(y)\rangle = \langle u, g(y_1) + g(y_2)\rangle = \langle u, g(y_1)\rangle$ (because the V_i are G-invariant). But, as y_1 is an invariant of G, this implies that $\langle u, g(y)\rangle = \langle u, y_1\rangle = g(\langle u, y\rangle)$. By lemma 40, this implies $u \in \mathrm{Inv}_{V^*}(G)$. If $V_1^* \subsetneq \mathrm{Inv}_{V^*}(G)$ then, as $V_1^{**} = V_1$, the dimensions would be such that $V_1 \subsetneq \mathrm{Inv}_V(G)$, a contradiction. Thus, $V_1^* = \mathrm{Inv}_{V^*}(G)$.
The action of G is trivial on V_1 and V_1^*, and they are of the same dimension, thus they are G-isomorphic. □

* Throughout this chapter, we will not distinguish between the notions of reductive group and linearly reductive group, because these notions coincide in our framework. The non-specialists may consult, for example [Spr77, Spr81] for explanation of these notions.

Lemme 42. *The G-modules $(S^m(V))^*$ and $S^m(V^*)$ are G-isomorphic.*

Proof. - see [FH91] page 476. □

Proof. - [of proposition 39] Suppose that G has s semi-invariants of degree m. This means that there are s 1-dimensional G-invariants submodules V_i and a G-submodule W of $S^m(V)$ such that W has no one-dimensional submodule and $S^m(V) = V_1 \oplus \ldots \oplus V_s \oplus W$. Thus (as in the proof of lemma 41), we have $S^m(V)^* = V_1^* \oplus \ldots \oplus V_s^* \oplus W^*$; by lemma 42, $S^m(V)^*$ is G-isomorphic with $S^m(V^*)$; as the V_i^* are 1-dimensional G-module, lemma 35 shows that the generators of the V_i^* are exponential over k; thus, these are also 1-dimensional G_*-modules.
Suppose that G has s invariants of degree m, i.e $\dim_{\mathcal{C}} \left(\mathrm{Inv}_{S^m(V)}(G)\right) = s$. By lemma 41, we have a G-isomorphism between $\mathrm{Inv}_{S^m(V)}(G)$ and $\mathrm{Inv}_{(S^m(V))^*}(G)$. By lemma 42, the latter is G-isomorphic with $\mathrm{Inv}_{S^m(V^*)}(G)$ and we obtain that $\dim_{\mathcal{C}} \left(\mathrm{Inv}_{S^m(V^*)}(G)\right) = s$. □

Remark: if G is not reductive, then the result is no longer true. For example, consider the operator $L = (\partial^2 - x)(x\partial - 1)$ i.e $L(y) = xy''' - 3y'' - x^2y' + xy$. Then, the equation $L(y) = 0$ has the solution $y = x$, but it can be checked that $L^*(y) = 0$ has no rational solution (where L^* denotes the *adjoint* equation whose solution space is the dual of the solution space of L, [Poole]).

Corollary 43. *Assume that the system (A) has a reductive Galois group G. Up to scalar multiplication, there is a one to one correspondence between the Darboux polynomials (resp. polynomial first integrals) of (A) and the semi-invariants (resp. invariants) of G.*

Proof. - This follows from theorem 38 and proposition 39. □

4. Algorithmic issues

4.1. The algorithm

Let $M = v_\nu y_n^m + v_{\nu-1} y_n^{m-1} y_{n-1} + \ldots + v_1 y_1^m$ be a Darboux polynomial of given degree m and denote as usual by $v = (v_1, \cdots, v_\nu)^t$ the vector of its coefficients.

Definition 44. We say that a solution of $Y' = AY$ is *exponential* over k if it is of the form $f.v$ where $f'/f \in k$ and $v \in k^n$.

We will show in section 5.2 that, if all components of a solution are exponential, then the system has an exponential solution.

Assuming that m is given (by the bounds of the previous section), proposition 33 provides the following algorithm Assuming that m is given (for example by bounds from invariant theory or by the bounds from [Ulm92, SUl93a, SUl93b]), proposition 33 provides the following algorithm for computing v.

1 Compute the matrix $\mathcal{A} = S^m(A)^*$.
2 Take a cyclic vector and compute the G-change of variables P that makes the system equivalent to a companion form, i.e to a homogeneous linear differential equation $\mathcal{L}_m$.
3 Compute the solutions of $\mathcal{L}_m$ whose logarithmic derivative is in k. For any such solution f, go to next step; else, return(0).
4 Apply P^{-1} to derive the corresponding vector $V = fv$ with $v \in k^\nu$. Then, v is the coefficient vector of a Darboux polynomial.

In [Wei94] (section 5.1), we gave a method for computing Darboux polynomials of linear differential equations (and this method can be adapted to systems); it is in fact a subclass of the above algorithm, as it corresponded to always choose $(0, \cdots, 0, 1)$ as a candidate cyclic vector. This yielded degeneracies that were difficult to deal with; this problem does not occur with the above algorithm (and we will see below how to take advantage of the degeneracies).

Remark. - Cyclic vectors are not the only way to solve linear differential systems; see the appendix on the implementation for more details. $\diamond$

4.2. Degenerate cases

If we take a putative cyclic vector Λ , then the corresponding G-change of variables P would be a matrix with rows P_i satisfying $P_1 = \Lambda$ and $P_{i+1} = P_i' + P_i\mathcal{A}$. If the matrix P is invertible, then the solution spaces of $(\mathcal{A})$ and $\mathcal{L}_m$ are isomorphic. However, if P does not have full rank, $\mathcal{L}_m$ has order less than ν and we theoretically cannot deduce the solutions of $(\mathcal{A})$ from those of $\mathcal{L}_m$; this implies that the system is reducible, i.e it can be reduced to lower block-diagonal form and the solution space has a non-trivial G-stable subspace (one can always find such a non-cyclic vector when the system is reducible). In this subsection, we show how one can in fact take advantage of this situation and how our algorithm can be improved in this case.

Let $\ker(P)$ have dimension $r > 0$ and compute a basis $V_1, \cdots, V_r$ of $\ker(P)$. For all i, j we have $P_iV_j = 0$. Now, on one hand, we have $P_{i+1}V_j = P_i'V_j + P_i\mathcal{A}V_j = 0$; on the other hand, we have $(P_iV_j)' = 0 = P_i'V_j + P_iV_j'$; thus, we obtain that $P_i(V_j' - \mathcal{A}V_j) = 0$ and so, for all j, there are $c_{i,j} \in k$ such that $V_j' - \mathcal{A}V_j = \sum_{i=1}^r c_{i,j}V_i$. We compute these elements.

First, let us assume for simplicity that $\mathcal{L}_m$ has no exponential solution. If V is an

exponential solution of $(\mathcal{A})$ then, by construction, V must satisfy $PV = 0$; writing $V = \sum \gamma_i V_i$ in the basis (V_i) of $\ker(P)$, we obtain that $V' - \mathcal{A}V = 0$ if and only if

$$\sum_{i=1}^{r} \left(\gamma_i' + \sum_{j=1}^{r} \gamma_j c_{i,j} \right) V_i = 0.$$

As the V_i form a basis of $\ker(P)$, this yields a system $\Gamma' = C\Gamma$ (with $C = (-c_{i,j})_{i,j}$) for the γ_i. Thus, we have reduced our ν-dimensional problem to finding the exponential solutions of the r-dimensional system $\Gamma' = C\Gamma$.

Example. - Consider the system $Y' = AY$ with

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ -1 & x & -\frac{1}{x} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & x & -\frac{1}{x} \end{pmatrix}$$

We first compute $S^2(A)^*$ (which has dimension 21). Taking $[1, 0, 0, 1, 0, \cdots]$ as a putative cyclic vector, we construct a (non-invertible) matrix P whose kernel is of the form:

$$f_3(x)(y_5y_1 - y_4y_2) + f_2(x)(y_5y_0 - y_3y_2) - f_6(x)(y_4y_0 + y_3y_1) + f_5(x){y_2}^2 + f_4(x)y_2y_1$$
$$+f_9(x)y_2y_0 + f_1(x){y_1}^2 + f_8(x)y_1y_0 + f_7(x){y_0}^2$$

This corresponds to a polynomial first integral if and only if the f_i satisfy the system $Y' = BY$, where

$$B = \begin{pmatrix} 0 & 0 & 0 & -x & 0 & 0 & 0 & -1 & 0 \\ 0 & \frac{1}{x} & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & \frac{1}{x} & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & \frac{1}{x} & -2\,x & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & \frac{2}{x} & 0 & 0 & 0 & 0 \\ 0 & x & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -2 & 0 & -x \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & -1 & \frac{1}{x} \end{pmatrix}.$$

Instead of solving a 21-dimensional system, we reduced the problem to solving a 9-dimensional system. This system has the rational solution $[0, x, -x^2, 0, 0, 0, 0, 0, 0]$, from which we deduce the following first integral:

$$-x^2\,y_5\,y_1 + x\,y_5\,y_0 + x^2\,y_4\,y_2 - x\,y_3\,y_2$$

Note that the above calculation takes several seconds (in MAPLE) whereas the computation

with a real cyclic vector (i.e producing an equation of order 21) is *dramatically* longer (around 45 minutes for this example, i.e 500 times slower). ◇

Remark. - If $\dim(\ker(P)) = 1$ then we directly have that V_1 is the coefficient vector of a Darboux polynomial. Also, note that if $\Gamma' = C\Gamma$ has an exponential solution, then this yields a Darboux polynomial even if $\mathcal{L}_m$ has exponential solutions. Therefore, the above construction leads to a notable improvement of the algorithm (which should be performed before even solving $\mathcal{L}_m$). ◇

Assume that $\mathcal{L}_m$ has an exponential solution f and let $F = (f, \cdots, f^{(\nu-1)})^t$. Letting V_0 be a particular solution of $PV = F$, we obtain a general solution (of $PV = F$) in the form $V = V_0 + \sum \gamma_i V_i$. As $P_{i+1}V = f^{(i)} = (P_iV)'$, we obtain again that $P_i'V + P_i\mathcal{A}V = P_i'V + P_iV'$ and thus $V' - \mathcal{A}V \in \ker P$; in particular, we find elements s_i such that $V_0' - \mathcal{A}V_0 = \sum_{i=1}^{r} s_iV_i$ and derive an $r \times r$ inhomogeneous system $\Gamma' = C\Gamma + S$ for the γ_i. Such a system can be also solved by a cyclic vector process. Note that the produced equation will then be inhomogeneous with an exponential right-hand side and the techniques from [Sin91] must then be used.

4.3. Some examples

The algorithm has been implemented in the computer algebra system Maple. Let us see some examples of computations.

Let L be a linear differential equation and (A) the corresponding system. The *m-th symmetric power* of L, noted $L^{\circledS m}$, is the equation produced from $S^m(A)$ by using the (putative) cyclic vector $(1, 0, \cdots, 0)$ ([Sin81, SUl93a, SUl93b]). This equation has its solution space spanned by all monomials of degree m in the solutions of L.

Consider the equation $L(y) = y'' + y = 0$. Then, its symmetric square is $L^{\circledS 2}(y) = y''' + 4y'$. This has the solution $y = 1$, and thus the Galois group has an invariant of degree 2. The corresponding first integral is $(y')^2 + y^2$.

The Brioschi identity.

More generally* consider the equation $l(z) = z'' - rz$ with $r \in k$ and let z_1, z_2 be a basis for the solution. We can form the equation $L(y) = l^{\circledS 2}(y) = y''' - 4ry' - 2r'y$ with $(y_1 = z_1^2, y_2 = z_1z_2, y_3 = z_2^2)$ as a basis for its solution space. Then, we have $y_1y_3 - y_2^2 = 0$. Thus, $L^{\circledS 2}$ has order 5 (instead of 6) and one can check that the Galois group has an invariant of degree 2. The corresponding polynomial first integral is $-2yy'' + (y')^2 - 4ry^2$

* I am indebted to M.F Singer for having suggested this example.

(for some values of r, this result appears in the literature as the "Brioschi identity", see [Poole]). This is a case where our techniques for degeneracies apply.

The Hurwitz system.

In the sequel, we will use the following system (due to Hurwitz) as a good example. Consider the Hurwitz system $Y' = AY$ with

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -\frac{\frac{792}{343}x-\frac{40805}{24696}}{x^2(x-1)^2} & -\frac{72/7\,x^2-\frac{2963}{252}x+20/9}{x^2(x-1)^2} & -\frac{7x-4}{x(x-1)} \end{pmatrix}.$$

This system is irreducible. Singer and Ulmer have shown in [SUl93c] that it has Galois group G_{168}, the finite simple group of 168 elements. From [SUl93a], we derive that it has an invariant of degree 4 and corollary 43 proves that $(S^m(A)^*)$ has a rational solution. We have used our implementation to treat this example. Using the cyclic vector $(0, \cdots, 0, 1)$, we produced an equation $\mathcal{L}_4$ which was found to admit the rational solution $f = x^8(x-1)^6$; from this, we obtained the Darboux polynomial M equal to:

$$\begin{aligned}
&{y_2}^4 + 2\,\frac{(7x-4)\,{y_2}^3\,y_1}{x(x-1)} + \frac{8\,(342x-49)\,{y_2}^3\,y_0}{441\,x^2(x-1)} + \frac{3\left(-2743\,x+784+2400\,x^2\right){y_2}^2\,{y_1}^2}{98\,x^2(x-1)^2} \\
&+\frac{\left(133920\,x^2-95735\,x+10976\right){y_2}^2\,y_1\,y_0}{2058\,x^3(x-1)^2} + \frac{\left(7464960\,x^3-9607401\,x^2+2292136\,x-153664\right){y_2}^2\,{y_0}^2}{518616(x-1)^3x^4} \\
&+\frac{\left(117504\,x^3-201457\,x^2+115166\,x-21952\right)y_2\,{y_1}^3}{686\,x^3(x-1)^3} \\
&+\frac{\left(3276288\,x^3-4215051\,x^2+1607956\,x-153664\right)y_2\,{y_1}^2\,y_0}{14406(x-1)^3x^4} \\
&+\frac{\left(-71659952\,x+365036544\,x^4-678527307\,x^3+380764774\,x^2+4302592\right)y_2\,y_1\,{y_0}^2}{3630312\,x^5(x-1)^4} \\
&+\frac{\left(-93927904\,x+1451188224\,x^4-2077051005\,x^3+713525139\,x^2+4302592\right)y_2\,{y_0}^3}{98018424\,x^6(x-1)^4} \\
&+\frac{\left(-4298112\,x+5750784\,x^4-13146820\,x^3+11273973\,x^2+614656\right){y_1}^4}{38416\,x^4(x-1)^4} \\
&+\frac{\left(-15004192\,x+45785088\,x^4-85081374\,x^3+56160371\,x^2+1229312\right){y_1}^3\,y_0}{172872\,x^5(x-1)^4} \\
&+(37585800183\,x^3-14153668240\,x^2+17844240384\,x^5-43373550816\,x^4+2215900736\,x \\
&-120472576){y_1}^2\,{y_0}^2/\left(101648736\,x^6(x-1)^5\right) \\
&+(1300959213471\,x^3-343699174616\,x^2+992612745216\,x^5-1988514598464\,x^4 \\
&+39750571840\,x-1686616064)y_1\,y_0^3/\left(19211611104\,x^7(x-1)^5\right) \\
&+(55168371523584\,x^6-142125993591552\,x^5+125442123785361\,x^4-45962050792788\,x^3 \\
&+8156158257856\,x^2-702269066240\,x+23612624896){y_0}^4/\left(9682651996416\,x^8(x-1)^6\right)
\end{aligned}$$

We'll see later on that this complicated expression has a first advantage: given a linear differential equation (or system), one can detect invariants by finding rational solutions of

symmetric power but this does not give their expression; our construction gives us explicit expressions that allow symbolic manipulations on invariants or semi-invariants. We will continue this example in section 6.1 and show how to obtain other Darboux polynomials and values of invariants in a smart way.

5. Liouvillian first integrals of linear differential systems

5.1. Structure results for the Liouvillian first integrals

The above constructions showed how to build polynomial first integrals over k. One may ask whether there exists such first integrals over some given types of extensions of k. We already noted that, if M is a Darboux polynomial with $DM = \alpha M$ and $\alpha = -\frac{f'}{f} \in k$, then fM is a polynomial first integral over $k(f)$ (which is a simple Liouvillian extension of k). Let us now prove a "descent" result that states what happens for other Liouvillian extensions (quoted in the beginning of this chapter as proposition 31):
Let $k_1 \supset k$ be a Liouvillian extension of k; then, the derivation D_{k_1} admits a Darboux polynomial over k_1 if and only if D_k admits a Darboux polynomial over k.

Proof. - [proposition 31] The "If" part is obvious. To prove the "Only if" part, an induction shows that it is enough to prove it for a simple Liouvillian extension $k_1 = k(\theta)$. Proposition 15 shows that, if θ is algebraic over k then we are done, so let us assume that θ is transcendental over k. Let $D_1 = D + \theta' \frac{\partial}{\partial \theta}$ be the extension of D to k_1 and let M be a homogeneous Darboux polynomial for D_1 (over k_1). First, note that if $D_1 M = \alpha M$ and $M = N/d$ (with $d \in k[\theta]$ and N with coefficients in $k[\theta]$), then N is also a Darboux polynomial (with $D_1 N = (\alpha + \frac{d'}{d})N$); thus, we may assume that M has its coefficients in $k[\theta]$. Write $M = \sum_{i=0}^{\nu} M_i \theta^i$; as M is homogeneous, each M_i contains terms in the Y_j (i.e $M_i \notin k$). Let's also write $\alpha = f/g$ with $f, g \in k[\theta]$, $gcd(f, g) = 1$, and g monic. A case study will now show that M_ν is a Darboux polynomial for D over k.

Assume that $\theta' = a \in k$. Then,

$$D_1 M = \alpha M \Longleftrightarrow g \left(\sum_{i=0}^{\nu} D(M_i)\theta^i + a \sum_{i=0}^{\nu-1} (i+1) M_{i+1} \theta^i \right) = fM.$$

If $DM_\nu = 0$, then M_ν is a Darboux polynomial over k; else, comparing the degrees in θ shows that $\deg_\theta f = \deg_\theta g = \gamma$ and $DM_\nu = f_\gamma M_\nu$, so that M_ν is a Darboux polynomial over k.

If $\theta' = a\theta$ with $a \in k$, then

$$D_1 M = \alpha M \Longleftrightarrow g \left(\sum_{i=0}^{\nu} D(M_i)\theta^i + a\theta \sum_{i=0}^{\nu-1} (i+1) M_{i+1} \theta^i \right) = fM.$$

A similar reasoning shows that $\deg_\theta f = \deg_\theta g = \gamma$ and $DM_\nu = (f_\gamma - \nu a)M_\nu$, so that M_ν is a Darboux polynomial over k. □

Remark. - This also means that there is a polynomial first integral over a Liouvillian extension of k if and only if there is a polynomial first integral over $k(f)$ with f exponential over k. ◇

Let L be a homogeneous linear differential equation with Galois group G, and let $(y_1, \ldots, y_n)$ be a fundamental system of solutions of L. The following corollary is that if some element of $C[y_1, \cdots, y_n]$ lies in a Liouvillian extension of k, then there is a Liouvillian first integral:

Corollary 45. *Let L be a homogeneous linear differential equation with Galois group G. If some symmetric power of L has a Liouvillian solution, then G has a semi-invariant.*

Proof. - Assume that some symmetric power of L has a Liouvillian solution. Let $(y_1, \ldots, y_n)$ be a fundamental system of solutions of L. Then, there exists a homogeneous polynomial $M \in C[y_1, \cdots, y_n]$ (of non-zero degree) such that M is Liouvillian over k. Let $k_1 \supset k$ be a Liouvillian extension of k (with no new constants) such that $M \in k_1$. Our theorem 38 tells us that there exists a polynomial first integral of L^* over k_1; then, the above proposition guarantees that there then exists a Darboux polynomial over k for L^* and (by theorem 38 again) a corresponding semi-invariant for L. □

Remark. - The converse is false if some symmetric power of L does not have the correct order. Let $L(y) = y''' - 4xy' - 2y$. This equation has Galois group $G \simeq PSL(2)$. G has a unique invariant of degree 2 and no other irreducible semi-invariant. However, $L^{\circledS 2}$ has order 5 (instead of 6) and no liouvillian solution: this is because the value of the invariant is zero. It follows that, though G has an invariant of degree 2, none of its symmetric powers has a liouvillian solution. ◇

Let us now turn to the relation between Liouvillian first integrals and Liouvillian solutions of L. In [Sin92], Singer proves that a second order linear differential equation has a Liouvillian first integral if and only if it has a Liouvillian solution. Our results show how this statement behaves for higher order equations:

Proposition 46. *Assume that a homogeneous linear differential equation L has a reductive Galois group. If L has a Liouvillian solution, then it has a Liouvillian first integral. The converse is false in general.*

Proof. - If L has a Liouvillian solution, then it has a solution z whose logarithmic

derivative is algebraic (see [Sin81]) and G has a semi-invariant z (by [Sin81] or the next chapter or the above corollary); by theorem 38, we can deduce a Darboux polynomial M_z from this semi-invariant and, then, zM_z is a Liouvillian first integral of L. Conversely, it may happen that there is a semi-invariant but no Liouvillian solution. For example, take the equation $y''-xy=0$. This equation has Galois group $SL(2,C)$ (and no semi-invariant). We form its symmetric square $L(y)=y'''-4xy'-2y=0$. This equation has Galois group $PSL(2,C)$; there is an invariant of degree 2 and L has a rational first integral (see the Brioschi identity in the end of section 4). However, it does not have a Liouvillian solution for otherwise, by the above corollary, $y''-xy=0$ would have a semi-invariant, and thus a Liouvillian solution (see also [SUl93a]). □

Remark. - If the equation is not completely reducible then it may happen that there is a Liouvillian solution and no first integral because, then, the existence of a semi-invariant does not guarantee the existence of a semi-invariant for the dual. For example, consider the operator $L=(\partial^2-x)(x\partial-1)$. It has the rational solution $y=x$, but no Darboux polynomial ⋄

Note that, here, we only considered polynomial first integrals with Liouvillian coefficients. One can give a more general definition of Liouvillian first integrals; this is done in [Sin92] where some other structural properties are derived.

5.2. Exponential solutions of linear differential systems

Recall that we say that a solution of $Y'=AY$ is exponential over k if it is of the form $f.v$ with $f'/f\in k$ and $v\in k^n$.

Proposition 47. *If all components of a solution of $Y'=AY$ are exponential over k, then the system admits an exponential solution.*

The proof of this proposition uses the following result of Rosenlicht (see [Ros75] theorem 1 pages 208-209):

Lemme 48 (Rosenlicht). *Let $k\subset K$ be a differential field extension such that k and K have the same constant field C; let $y_i\in K$ $(i=1,\dots,n)$ be exponential over k and not all zero. If $\sum_{i=1}^n y_i=0$ then, for all i, there exists j such that $y_i/y_j\in k$.*

Proof. - If $y_i=0$ then any non-zero y_j fits, so assume that $y_i\neq 0$. Put $z_1=y_i$; assume that there exists z_j $(j=2,\cdots,N)$, exponential over k such that $\tilde{k}:=k(z_1,\cdots,z_N)$ has no new constants, $z_1/z_j\notin k$ for all j, $\sum_{j=1}^N z_j=0$, and N is minimal with respect to this

property. Then, $\sum_{j=1}^{N} z'_j = 0$ and we derive $\sum_{j=1}^{N}(z'_j/z_j - z'_1/z_1)z_j = 0$. This contradicts the minimality of N unless for all j we have $z'_j/z_j - z'_1/z_1 = 0$, i.e z_j/z_1 is a constant in $\tilde{k}$. As there are no new constants in $\tilde{k}$, this implies that $z_j/z_1 \in C \subset k$, a contradiction. Thus, there exists $j \neq i$ such that $y_i/y_j \in k$. □

Proof. - [Proposition] Let $Y = (y_1, \ldots, y_n)^t$ be a solution of $Y' = AY$ with $y'_i = \alpha_i y_i$ and $\alpha_i \in k$. As the y_i are in a Picard-Vessiot extension, the field $K := k(y_1, \ldots, y_n)$ has the same constant field as k. For all i, we have $\alpha_i y_i = \sum_j A_{i,j} y_j$ which we rewrite as

$$\sum_{j=1}^{n} r_{i,j} y_j = 0.$$

Some component of the solution is non-zero, say y_1. If all $r_{i,1} = 0$, then $(y_1, 0, \ldots, 0)^t$ is a solution of the required form and we are done, so we assume that $r_{i,1} \neq 0$ for some i. After renumbering, let m be such that $y_i = v_i y_1$ with $v_i \in k$ for $i = 1, \cdots, m$ and $y_i/y_1 \notin k$ for $i > m$. If $m = n$ we are done, so we assume that $m < n$. For all i, we have

$$y_1 \sum_{j=1}^{m} r_{i,j} v_j + \sum_{j=m+1}^{n} r_{i,j} y_j = 0.$$

As $y_j/y_1 \notin k$ for $j > m$, Rosenlicht's lemma implies that, for all i, we have

$$\sum_{j=1}^{m} r_{i,j} v_j = 0.$$

Thus, $(y_1, \cdots, y_m, 0, \cdots, 0)^t$ is a solution of $Y' = AY$ of the prescribed form. □

Remark. - Another proof can be written (also using the lemma) by checking the action of the elements of the differential Galois group G of (A). If $g \in G$, then $g(y_i) = c_i y_i$ and, writing that g is differential, we obtain $\sum_j A_{i,j}(c_i - c_j) y_j = 0$ for all i. The proof then goes as above. ◇

The proof (on page 53) of proposition 31 also shows the following:

Proposition 49. *Let $K = k(z_1, \cdots, z_r)$ be a liouvillian extension such that each z_i is transcendental exponential over $k(z_1, \cdots, z_{i-1})$ and k and K have the same constants. If $Y' = AY$ has a solution Y whose components are in K, then it has an exponential solution.*

Proof: the components of Y are the coefficients of a Darboux polynomial of degree one for (A^*). The proof of proposition 31 (page 49) shows that, then the system (A^*) has a Darboux polynomial M *also of degree one* with coefficients in k. Thus, it has a polynomial first integral $f.M$ with f exponential over k and thus $Y' = AY$ has an exponential solution. □

Remark. - This results holds the same if each z_i is transcendental exponential over k, the z_i are algebraically independent, and k and K have the same constants. If the z_i are not transcendental (or are algebraically dependent), then the last result is false. For example, it is explained in the last section of chapter III how one may obtain solutions by radicals of some two by two systems which have no exponential solutions. $\diamond$

6. Accélération des calculs et application au calcul d'invariants

6.1. Constructeurs de polynômes de Darboux

Soit V un C-espace vectoriel de dimension n et $G \in GL(V)$. Supposons que G admet des invariants $I_1, \ldots, I_n$ (resp semi-invariants) sur l'algèbre symétrique $S(V)$. Alors, on construit classiquement d'autres invariants (resp. semi-invariants) de la manière suivante. On définit le Hessien de $M(y_1, \ldots, y_n)$ par $H(M) = \det\left(\partial_{i,j} M\right)_{i,j=1..n}$, avec la notation $\partial_{i,j} = \frac{\partial^2}{\partial y_i \partial y_j}$. On définit ensuite le Hessien bordé de $M_1(y_1, \ldots, y_n), M_2(y_1, \ldots, y_n)$ par :

$$HB(M_1, M_2) = \det \begin{pmatrix} \partial_{1,1} M_1 & \cdots & \partial_{1,n} M_1 & \partial_1 M_2 \\ \vdots & \cdots & \vdots & \vdots \\ \partial_{n,1} M_1 & \cdots & \partial_{n,n} M_1 & \partial_n M_2 \\ \partial_1 M_2 & \cdots & \partial_n M_2 & 0 \end{pmatrix} \tag{6.1}$$

Enfin, le Jacobien de $\left(M(y_1, \ldots, y_n)\right)_{i=1..n}$ est $J = \det\left(\partial_i M_j\right)_{i,j=1..n}$.

Alors (voir [Weber] pages 223-226 ou [Stu94]), les polynômes $H(I_1), HB(I_1, I_2), J(I_1, \cdots, I_n)$ sont encore des invariants (resp. semi-invariants).

Cette propriété s'étend directement aux polynômes de Darboux. Plus précisément, on a :

Proposition 50. *Supposons que $D(M_i) = \alpha_i M_i$ (pour $i = 1, \cdots, n$) sont des polynômes de Darboux pour $Y' = AY$ (avec $A \in \mathcal{M}_n(k)$) de degré m_i. Alors on a :*

$$D(H(M_i)) = (n\alpha_i - 2Tr(A))\, H(M_i) \tag{6.2}$$

$$D(HB(M_i, M_j)) = (2\alpha_j + (n-1)\alpha_i - 2Tr(A))\, HB(M_i, M_j) \tag{6.3}$$

$$D(J(M_1, \cdots, M_n)) = \left(\sum_{i=1}^{n} \alpha_i - Tr(A)\right) J(M_1, \cdots, M_n) \tag{6.4}$$

où $Tr(A)$ désigne la trace de A. De plus, on a $\deg_{tot}(H(M_i)) = n(m_i - 2)$, $\deg_{tot}(HB(M_i, M_j) = (n-1)(m_i - 2) + 2(m_j - 1)$, et $\deg_{tot}(J(M_1, \cdots, M_n)) = -n + \sum_i m_i$.

La preuve de cette proposition est calculatoire mais assez simple ; nous aurons besoin du lemme (classique) suivant (e.g [Mag94]) :

Lemme 51. *Soit M une matrice $n \times n$ sur k ; on note $M = (\rho_1, \cdots, \rho_n)$, où les ρ_i sont les lignes de M. Alors, on a*

$$\det(M)' = \sum_{i=1}^{n} \det(\rho_1, \cdots, \rho_{i-1}, \rho_i', \rho_{i+1}, \cdots, \rho_n)$$

.

Preuve. - Notons $\Delta_{i,j}$ le mineur associé au coefficient $M_{i,j}$. Si on développe $\det(M)$ par rapport à la i-ème ligne, on a $\det(M)' = \sum_{j=1}^{n} \left(M_{i,j}' \Delta_{i,j} + M_{i,j} \Delta_{i,j}' \right)$. La contribution des dérivées des termes de la i-ème lignes dans la dérivée du déterminant est donc $\det(\rho_1, \cdots, \rho_{i-1}, \rho_i', \rho_{i+1}, \cdots, \rho_n)$. Le résultat en découle par symétrie. □

Preuve. - [proposition 50] Commençons par calculer $(D\partial_i)$. Pour ce faire, notons que

$$[D, \partial_i] = -\sum_{l=1}^{n} \left(\sum_{j=1}^{n} \partial_i(A_{l,j} y_j) \partial_l \right) = -\sum_{l=1}^{n} A_{l,i} \partial_l$$

Il en découle que

$$D\partial_i = ([D, \partial_i] + \partial_i D) = -\sum_{l=1}^{n} A_{l,i} \partial_l + \partial_i D \tag{6.5}$$

De la même manière, on obtient aussi $(D\partial_{i,j})$.

$$\begin{aligned} D\partial_{i,j} &= ([D, \partial_i] + \partial_i D)\partial_j \\ &= [D, \partial_i]\partial_j + \partial_i([D, \partial_j] + \partial_j D) \end{aligned}$$

d'où

$$D\partial_{i,j} = -\sum_{l=1}^{n} (A_{l,j} \partial_{l,i} + A_{l,i} \partial_{l,j}) + \partial_{i,j} D. \tag{6.6}$$

Notons $J = Jac(M_1, \cdots, M_n)$ et $\Delta_{i,j}$ les mineurs de J (comme dans la preuve du lemme). Alors, par le lemme et la relation (6.5), on a :

$$\begin{aligned} DJ &= \sum_{i,j=1}^{n} (-1)^{i+j} \Delta_{i,j} \left(-\left(\sum_{l=1}^{n} A_{l,j} \partial_l M_j \right) + \alpha_j \partial_i M_j \right) \\ &= \left(\sum \alpha_i \right) J - \sum_{l=1}^{n} \sum_{i=1}^{n} A_{l,i} \sum_{j=1}^{n} \left((-1)^{i+j} \Delta_{i,j} \partial_l M_j \right) \end{aligned}$$

Or, l'expression $\sum_{j=1}^{n} \left((-1)^{i+j} \Delta_{i,j} \partial_l M_j \right)$ est le développement du déterminant de la matrice obtenue en remplaçant la i-ème ligne par la l-ième ligne ; on a donc $\sum_{j=1}^{n} \left((-1)^{i+j} \Delta_{i,j} \partial_l M_j \right) = \delta_{i,l} J$ (le symbole de Kronecker). Il en découle que

$$\sum_{l=1}^{n} \sum_{i=1}^{n} A_{l,i} \sum_{j=1}^{n} \left((-1)^{i+j} \Delta_{i,j} \partial_l M_j \right) = \sum_{l=1}^{n} \sum_{i=1}^{n} A_{l,i} \delta_{i,l} J = Tr(A) J,$$

d'où le résultat.
Notons $H = H(M)$, avec $D(M) = \alpha M$, et $\Delta_{i,j}$ les mineurs de H. En utilisant le lemme et la relation (6.6), on a

$$\begin{aligned} DH &= \sum_{i,j}(-1)^{i+j}\Delta_{i,j}\left(-\sum_{l=1}^{n}(A_{l,i}\partial_{l,j}M + A_{l,j}\partial_{l,i}M) + \alpha\partial_{i,j}M\right) \\ &= n\alpha H - 2\sum_{i,l}A_{l,i}\sum_{j=1}^{n}(-1)^{i+j}\Delta_{i,j}\partial_{l,j}M. \end{aligned}$$

Raisonnant comme pour le Jacobien, on remarque que $\sum_{j=1}^{n}(-1)^{i+j}\Delta_{i,j}\partial_{l,j}M = \delta_{i,l}H$, et donc $DH = (n\alpha - 2Tr(A))\,H$.
Le calcul est analogue pour le Hessien bordé. On pose maintenant $HB = HB(M_1, M_2)$ et $\Delta_{i,j}$ sont les mineurs de HB. Notons DHB_i le déterminant de la matrice obtenue en ne dérivant que la i-ème ligne dans HB. Pour $i < n+1$, on a :

$$\begin{aligned} DHB_i &= \sum_{j=1}^{n}(-1)^{i+j}\Delta_{i,j}D\partial_{i,j}M_1 + (-1)^{i+n+1}\Delta_{i,n+1}D\partial_i M_2 \\ &= \sum_{j=1}^{n}(-1)^{i+j}\Delta_{i,j}\alpha_1\partial_{i,j}M_1 - \sum_{l,j=1}^{n}(-1)^{i+j}\Delta_{i,j}\left(A_{l,i}\partial_{l,j}M_1 A_{l,j}\partial_{l,i}M_1\right) \\ &\quad +(-1)^{i+n+1}\alpha_2\Delta_{i,n+1}\partial_i M_2 - \sum_{l}(-1)^{i+n+1}\Delta_{i,n+1}A_{l,i}\partial_l M_2 \end{aligned}$$

et

$$\begin{aligned} DHB_{n+1} &= \sum_{i}\left((-1)^{i+n+1}\alpha_2\Delta_{i,n+1}\partial_i M_2 - \sum_{l}(-1)^{i+n+1}\Delta_{i,n+1}A_{l,i}\partial_l M_2\right) \\ &= \alpha_2 HB - \sum_{i,l}(-1)^{i+n+1}\Delta_{i,n+1}A_{l,i}\partial_l M_2. \end{aligned}$$

Il en découle que

$$\begin{aligned} D(HB) &= \sum_{i=1}^{n+1}DHB_i \\ &= n\alpha_1 HB - 2\sum_{i,j,l}(-1)^{i+j}\Delta_{i,j}A_{l,i}\partial_{l,j}M_1 + (\alpha_2 - \alpha_1)HB \\ &\quad -2\sum_{i,l}(-1)^{i+n+1}\Delta_{i,n+1}A_{l,i}\partial_l M_2 + \alpha_2 HB \end{aligned}$$

Raisonnant comme précédemment, on en déduit que $D(HB) = ((n-1)\alpha_1 + 2\alpha_2 - 2Tr(A))\,HB$.
□

Expérimentalement, on constate qu'il est très nettement plus rapide de calculer des polynômes de Darboux par cette méthode que par la méthode directe que nous avons donné dans la section 4 (on peut aussi le vérifier théoriquement, voir plus bas).

6.2. Application au calcul de solutions algébriques

Soit $L(y) = 0$ une équation différentielle linéaire homogène d'ordre n que nous supposons irréductible ; soit K une extension de Picard-Vessiot pour L et G son groupe de Galois différentiel. Nous supposons que G est un groupe unimodulaire (i.e $G \subset SL_n(C)$) et qu'il est de plus fini, c'est à dire que les solutions de L sont algébriques sur k. Dans [SUl93b, SUl93a], Singer et Ulmer montrent comment calculer le polynôme minimal d'une solution. Résumons rapidement cette méthode. Pour un groupe donné, on peut déterminer le degré du polynôme minimal et décomposer ses coefficients sur une base d'invariants du groupe de Galois. Connaissant L et le groupe, on connaît les degrés m_i des invariants ; on calcule donc les solutions rationnelles de $L^{\circledS m_i}(y) = 0$, ce qui nous donne les invariants à multiplication par une constante près. Il ne reste alors qu'à injecter ces solutions dans l'expression du polynôme minimal et ajuster les constantes de manière à ce que le polynôme définisse bien une solution de l'équation.

Calcul des invariants par les polynômes de Darboux.

En pratique, la partie la plus longue (et généralement irréalisable à ce jour si $n > 2$) est de déterminer les invariants. Nous allons donc montrer comment calculer les invariants (resp semi-invariants) de manière élégante et efficace à partir des intégrales premières (resp. polynômes de Darboux) :

Théorème 52. *Soit $L(y) = 0$ une équation différentielle linéaire homogène et $Y' = AY$ le système associé. Soit $y_{1,1}, \cdots, y_{1,n}$ un système fondamental de solutions de L et $u_{1,1}, \cdots, u_{1,n}$ un système fondamental de solutions de l'adjointe L^*. Alors :*

1. *Si M est une intégrale première polynomiale de degré m pour (A), alors le coefficient de y_n^m dans M est un polynôme homogène de degré m en les $u_{1,j}$ (c'est à dire une solution de $(L^*)^{\circledS m}(y) = 0$).*
2. *Si M est une intégrale première polynomiale de degré m pour (A^*), alors le coefficient de y_1^m dans M est un polynôme homogène de degré m en les $y_{1,j}$ (c'est à dire une solution de $L^{\circledS m}(y) = 0$).*

Preuve. - Nous allons montrer la deuxième assertion, qui nous intéresse directement ici ; Par construction, $L(y) = 0$ est l'équation obtenue depuis A en utilisant le vecteur cyclique $[1, 0, \cdots, 0]$; de même, on peut montrer que l'équation $L^*(y) = 0$ est l'équation obtenue depuis A^* en utilisant le vecteur cyclique $[0, \cdots, 0, 1]$. D'autre part, si M est une intégrale première polynomiale de (A) alors, le i-ème coefficient de M est solution de l'équation obtenue depuis $S^m(A)^*$ en utilisant le vecteur cyclique (éventuel) $[0, \cdots, 0, 1, 0, \cdots, 0]$ (où

le 1 apparaît en i-ème position).
Intéressons nous aux intégrales premières à coefficients dans l'extension de Picard-Vessiot K. J'affirme que l'anneau des intégrales premières de (A^*) sur K est engendré par n intégrales premières polynomiales linéaires dont le coefficient de y_1 est une solution de L. En effet, on a $S^1(A^*)^* = (A^*)^* = A$; le coefficient de y_1 est donc solution de l'équation obtenue depuis A en utilisant le vecteur cyclique $[1, 0, \cdots, 0]$, c'est à dire qu'il est solution de L. Comme (A) a n solutions linéairement indépendantes dans K, ces solutions donnent les coefficients de n intégrales premières linéaires pour (A^*) que nous notons M_i.
Soit m un entier donné et $\nu = \binom{n+m-1}{n-1}$. Supposons d'abord que le vecteur $[1, 0, \cdots, 0]$ est cyclique pour $S^m(A)$, c'est à dire que $L^{\circledS m}$ est d'ordre ν. Alors, les monômes de degré m en les $y_{1,j}$ forment une base de solutions (dans K) de $L^{\circledS m}$. Or, à chaque monôme $\prod_{|\alpha|=m} y_{1,j}^{\alpha_j}$, on peut associer l'intégrale première $M_\alpha = \prod_{|\alpha|=m} M_j^{\alpha_j}$; comme les monômes de degré m en les $y_{1,j}$ sont linéairement indépendants sur les constantes, les M_α sont aussi linéairement indépendants sur les constantes et leurs coefficients forment donc une base de solutions de $S^m(A)^*$. Nous en déduisons que, pour toute intégrale première de degré m, le coefficient de y_1^m est un polynôme homogène de $C[y_{1,1}, \cdots, y_{1,n}]$.
Enfin, si l'ordre de $L^{\circledS m}$ est inférieur à ν, nous savons que nous pouvons trouver une équation $\tilde{L}$ de même type que L telle que $\tilde{L}^{\circledS m}$ soit exactement d'ordre ν ([Sin93] prop 3.9 pages 370-371 ou le lemme 3.4 dans [Sin94]). Nous appliquons alors le raisonnement ci-dessus à $\tilde{L}$ et obtenons notre résultat par le lemme 36.
La preuve de la première assertion est tout à fait identique, en utilisant le fait (classique, e.g [Poole]) que le coefficient de y_n dans toute intégrale première linéaire de L est une solution de L^*. □

□

Remarque. - Contrairement à ce que ce résultat pourrait donner à penser, $S^m(A)^* \neq S^m(A^*)$ ⋄

Supposons que nous connaissions une intégrale première polynomiale de (A^*) ; nous en déduisons la valeur* de l'invariant correspondant en examinant le coefficient de y_1^m ; de même, pour un polynôme de Darboux, nous déterminons f tel que fM soit une intégrale première et le coefficient de y_1^m dans fM est la valeur du semi-invariant correspondant. Ensuite, grâce à la proposition 50, nous construisons facilement d'autres polynômes de Darboux qui, à leur tour, donnent des valeurs d'éventuels autres invariants. Nous allons maintenant montrer comment ceci permet d'améliorer notablement l'algorithme de Singer-Ulmer de calcul de solutions algébriques d'équations différentielles linéaires d'ordre 3.

Remarque. - Cette idée d'utiliser des Hessiens et des Jacobiens pour faciliter les calculs d'invariants de groupes de Galois différentiels n'est pas complètement nouvelle. On la trouve

* Par valeur, nous entendons la chose suivante : si $P(X_1, \cdots, X_n)$ est un invariant (resp. un semi-invariant) de G, nous appelons *valeur* de P sa spécialisation en $y_{1,1}, \cdots, y_{1,n}$ (qui est un élément de k, resp. exponentiel sur k). C'est cette valeur qui est utilisée dans les algorithmes de recherche de solutions d'équations différentielles

déjà en 1878 dans un papier de Fuchs où il l'utilise pour accélérer le calcul de solutions algébriques d'équations du second ordre ([Fuc78] ou bien [SUl93b] page 69). Mais, à ma connaissance, cette idée n'a pas été étendue aux équations d'ordre supérieur à deux (jusqu'à ce jour) $\diamond$

Accélération de l'algorithme de Singer-Ulmer pour le calcul de solutions algébriques d'équations d'ordre 2 et 3.

Dans le cas d'une équation d'ordre 2 ou 3, Singer et Ulmer donnent une liste finie de groupes possibles à étudier. Nous étudierons les équations d'ordre 2 dans le chapitre suivant. Pour l'ordre 3, passons en revue les groupes en voyant comment nos améliorations s'insèrent (nous reprenons les notations de [SUl93a, SUl93b]). Nous appelons *invariants fondamentaux* les invariants nécessaires au calcul d'une solution algébrique (suivant les décompositions données par Fakler dans [Fak94]). Pour apprécier ce qui suit, on peut noter l'observation expérimentale suivante : à l'heure où ces lignes sont écrites, on arrive en général à calculer des valeurs d'invariants jusqu'en degré 6 au maximum (si l'on est très patient et que l'on a une machine rapide pour les calculs)

Le groupe de Valentiner $A_6^{SL_3}$:

Soit $L(y) = y''' + a_2y'' + a_1y' + a_0y$ une équation différentielle linéaire dont le groupe de Galois soit le groupe de Valentiner $G = A_6^{SL_3}$, et soit A la matrice companion correspondante. Comme G est unimodulaire, il existe $f \in k$ tel que $f'/f = a_2 = Tr(A)$. Le groupe $A_6^{SL_3}$ a quatre invariants fondamentaux I_i avec I_1 de degré 6, I_2 de degré 12, I_3 de degré 30, et I_4 de degré 45. Ces invariants satisfont $I_2 = H(I_1)$, $I_3 = HB(I_1, I_2)$, et $I_4 = J(I_1, I_2, I_3)$. Pour les obtenir, nous commençons par calculer une intégrale première de degré 6 pour L^*. Par le théorème 48, nous savons que le coefficient de y_1^6 est l'invariant I_1. Nous calculons alors le Hessien $H(M)$ de M (par calcul direct, sans résoudre un nouveau système différentiel) ; la proposition 48 montre alors que $f^2H(M)$ est une intégrale première pour L^*. Alors, le coefficient de y_1^{12} est l'invariant* I_2. Soit HB le Hessien bordé de M et f^2M ; le premier coefficient de f^2HB est alors égal à I_3. Enfin, si J est le Jacobien de M, f^2H, and f^2HB, alors I_4 est le premier coefficient de fJ.
Au lieu de résoudre quatre très gros systèmes différentiels, nous nous sommes donc ramenés à n'en résoudre qu'un seul (de dimension 28) pour la sixième puissance symétrique.

* De manière générale, si $f_1, \ldots, f_6$ sont les 6 premières coordonnées d'un polynôme de Darboux de degré m en trois variables, alors la première coordonnée du Hessien est

$$\left(4\,m\,(m-1)\,f_6\,f_4 - m\,(m-1)\,{f_5}^2\right) f_1 - 2\,(m-1)^2\,f_6\,{f_2}^2 + 2\,(m-1)^2\,f_5\,f_3\,f_2 - 2\,(m-1)^2\,f_4\,{f_3}^2.$$

On peut effectuer le même pré-calcul pour obtenir la première coordonnée de leur Hessien bordé et du Jacobien des trois (mais le résultat ne tient pas dans la marge).

Les groupes alterné $A_5^{SL_3}$ et $A_5^{SL_3} \times C_3$:

Il y a trois invariants fondamentaux avec I_1 de degré 2, I_2 de degré 6 et I_3 de degré 10. Avec les invariants donnés dans [SUl93b] page 64, on vérifie que $I_3 = HB(I_1, I_2)$ est de degré 10 et algébriquement indépendant des 2 autres. Il y a donc deux invariants de degrés 2 et 6 à calculer dans ce cas.

Les groupes Hessien G_{168} et $G_{168} \times C_3$:

Il y a quatre invariants fondamentaux de degrés 4,6,14,21. De plus, on a $I_2 = H(I_1)$, $I_3 = HB(I_1, I_2)$, et $I_4 = J(I_1, I_2, I_3)$. Il y a donc un seul invariant à calculer dans ce cas là.

Les groupes $H_{216}^{SL_3}$ et $H_{72}^{SL_3}$:

Il y a quatre invariants fondamentaux de degrés 6,9,12,12. Par calcul direct sur les invariants donnés dans les références de [SUl93b] (ou dans [Fak94] page 51), on obtient un invariant de degré 12 : $I_3 = H(I_1)$. Nous ne voyons pas encore de moyen d'obtenir astucieusement I_2 et I_4. On peut vérifier que $H(I_2) = I_2 I_3$.

Le groupe $F_{36}^{SL_3}$:

Les invariants précédents sont des invariants de F_{36} mais seuls les trois premiers sont des invariants fondamentaux. Le quatrième invariant fondamental est de degré 6 et le cinquième de degré 12 avec $I_5 = H(I_4)$. On note qu'il y a un semi-invariant de degré 3 (donc un polynôme de Darboux de tel degré).

Nous résumons tout ceci dans la table suivante. La première ligne de chaque colonne désigne le groupe, la suite de la colonne désigne (par le degré de la puissance symétrique) les systèmes différentiels à résoudre pour obtenir les invariants. Par exemple, la colonne $A_5^{SL_3}$ nous dit que la méthode standard doit résoudre des puissances symétriques de degré $2, 6, 10$ et que notre méthode doit résoudre des puissances symétriques de degré $2, 6$.

Groupe :	$A_6^{SL_3}$	$A_5^{SL_3}$, $A_5^{SL_3} \times C_3$	G_{168}, $G_{168} \times C_3$	$H_{216}^{SL_3}$, $H_{72}^{SL_3}$	$F_{36}^{SL_3}$
Méthode directe :	6,12,30,45	2,6,10	4,6,14,21	6,9,12	6,9,12
Notre méthode :	6	2,6	4	6,9,12	6,9

Exemple. - Considérons une équation dont le groupe de Galois est $A_5^{SL_3}$. Pour calculer

une solution algébrique, nous devons calculer la valeur des trois invariants I_1, I_2, I_3. Le calcul de I_1 est simple : nous calculons une solution rationnelle f_1 de $L^{\circledS 2}$. Pour I_2, l'espace de solutions de $L^{\circledS 6}$ est de dimension 2 et nous avons $I_2 = c_1 f_1^3 + c_2 f_2$ (où les c_i sont des constantes et $f_1^3, f_2 \in k$ forment une base de solutions). Appliquant notre méthode, nous obtenons $HB(I1, I2) = f_3(c_1, c_2)$. Pour $L^{\circledS 10}$, il y a un espace de solutions rationnelles de dimension 3 engendré par $I_3, I_2 I_1^2, I_1^5$. Nous n'avons donc pas besoin de calculer $L^{\circledS 10}$ pour en déduire les trois invariants fondamentaux :

$$\begin{aligned} I_1 &= c_0 f_1 \\ I_2 &= c_1 f_1^2 + c_2 f_2 \\ I_3 &= c_3 f_3(c_1, c_2) + c_4 f_2 f_1^2 + c_5 f_1^5 \end{aligned}$$

Disposant de ces valeurs, nous pouvons les substituer dans l'expression du polynôme minimal donné dans [SUl93b] ou [Fak94] et en déduire les valeurs idoines des constantes c_i (ainsi que le polynôme minimal d'une solution algébrique). Notons que nous aurons à déterminer 6 constantes (et non trois comme on pourrait le penser au premier abord). $\diamond$

Remarque. - Nous ne savons pas encore interpréter les autres coefficients des polynômes de Darboux ; il est probable que ça donnerait encore beaucoup plus d'informations pour simplifier les calculs, par exemple pour accélérer l'algorithme de Singer ([Sin81, SUl93b]) de calcul du polynôme minimal des solutions algébriques des équations de Riccati. $\diamond$

Notons que si l'équation est irréductible alors on a quatre possibilités pour le groupe : imprimitif (dans ce cas, il y a un semi-invariant de degré 3), primitif fini (dans ce cas là, nous venons d'énumérer les cas), $PSL_2(C)$ (dans ce cas là, il y a une unique intégrale première de degré 2, donnée en exemple dans la section 4 sous le nom d'identité de Brioschi) ou bien $SL_3(C)$. Nous résumons ceci dans le résultat suivant (qui est implicite chez Singer et Ulmer) :

Proposition 53. *Soit A une matrice 3×3 de groupe de Galois irréductible. Si (A) admet un polynôme de Darboux, alors il admet au moins un polynôme de Darboux de degré 2,3,4,ou 6 ; Si de plus le groupe est primitif et unimodulaire, alors le système admet une intégrale première polynomiale de degré 2,4 ou 6.*

Remarque. - Dans le double papier de Singer et Ulmer ([SUl93a, SUl93b]), les auteurs indiquent la borne $m = 36$ pour le degré des semi-invariants car ils recherchent des semi-invariants correspondant à des solutions liouvilliennes (une partie des bornes ci-dessus est néanmoins dans leur papier, et était sûrement dans leurs brouillons de travail) ; la proposition 53 ci-dessus montre que les bornes d'Ulmer ([Ulm92]) sur les degrés des semi-invariants peuvent être améliorées (au moins pour $n = 3$) si on cherche n'importe quel

semi-invariant. Il serait intéressant de comprendre si cette remarque se généralise à d'autres valeurs de n. $\diamond$

6.3. Une étude de cas : l'équation de Hurwitz

Reprenons l'équation de Hurwitz traitée en exemple dans la section 4 Nous avions trouvé un polynôme de Darboux M de degré 4, qui correspondait à une intégrale première polynomiale.

Calcul de toutes les intégrales premières.

Nous savons que l'algèbre des invariants de G_{168} est engendrée par quatre invariants I_i (où $i = 4, 6, 14, 21$ est le degré de I_i) et que l'on a :

$$I_6 = H(I_4), \qquad I_{14} = HB(I_4, I_6), \qquad I_{21} = J(I_4, I_6, I_{14}).$$

La seule donnée de M nous donne donc quatre intégrales premières polynomiales $M_1, \ldots, M_4$ (la quatrième est algébriquement dépendante des trois premières) et l'algèbre des intégrales premières de L est $C[M_1, \ldots, M_4]$.
Pour l'exemple, nous calculons le Hessien $H(M)$ de M, ce qui donne :

$$M_6 = 768288795144192\,x^8(4169775577723022868 48\,x^9 - 1609235974754285912064\,x^8 + 2451343920792170438016\,x^7$$
$$- 1894354537129381507329\,x^6 + 813642918118934193756\,x^5 - 208057880597320176192\,x^4 + 32609273287630751488\,x^3$$
$$- 3083517602215550976\,x^2 + 161870210692055040\,x - 3628410392018944)(x-1)^6\,Y_0{}^6$$
$$+ (580826329129009152\,x^9(7487812485248974848\,x^8 - 24614585201902288896\,x^7 + 31329905250090756312\,x^6$$
$$- 19867296082375501965\,x^5 + 6894676920718797228\,x^4 - 1380662630255650112\,x^3 + 159840819841876992\,x^2$$
$$- 9962284506746880\,x + 259172170858496)(x-1)^7\,Y_1 + 1138419605092857937 92\,x^{10}(10968475320188928\,x^7$$
$$- 29778327211327488\,x^6$$
$$+ 28843935870264813\,x^5 - 12580277320833786\,x^4 + 2888214594249600\,x^3 - 365664583564672\,x^2$$
$$+ 24265104367616\,x - 661153497088)(x-1)^8\,Y_2)Y_0{}^5$$
$$+ (182960293675637882880\,x^{10}(134329969353424896\,x^8 - 499098520184610816\,x^7 + 743138610953518008\,x^6$$
$$- 571752307040090751\,x^5 + 246003643278431964\,x^4 - 60426627026350144\,x^3 + 8402693565181440\,x^2$$
$$- 615996038590464\,x + 18512297918464)(x-1)^7\,Y_1{}^2 + 5122888222917860720640\,x^{11}(2753403269677056\,x^7 - 8654584196745216\,x^6$$
$$+ 1027871434424394 9\,x^5 - 5834151121526388\,x^4 + 1700370604049992\,x^3 - 263945818708992\,x^2 + 20853080070144\,x - 661153497088)(x-1)^8\,Y_2\,Y_1$$
$$+ 35860217560425025044480\,x^{12}(56422198149120\,x^6 - 145068071122944\,x^5 + 127614420012825\,x^4$$
$$- 46495274571612\,x^3 + 8206885648192\,x^2 - 703817999360\,x + 23612624896)(x-1)^9\,Y_2{}^2)Y_0{}^4$$
$$+ (30737329337507164323840\,x^{11}(2407347121029120\,x^7 - 7568228441161728\,x^6 + 9436973454104562\,x^5$$
$$- 5996995036750215\,x^4 + 2070064169813240\,x^3 - 383938605540672\,x^2 + 35846133098496\,x - 1322306994176)(x-1)^8\,Y_1{}^3 + 25819356643506018032$$

$$+60373515556143\,x^4-26864778520995\,x^3+5816794627168\,x^2-599174659328\,x+23612624896)(x-1)^9\,Y_2\,{Y_1}^2+180735496504542126224179 20\,x^{}$$

$$+1317297143997\,x^3-346322425064\,x^2+39875039680\,x-1686616064)(x-1)^{10}\,{Y_2}^2\,Y_1+16868646340423931780923392 0\,x^{14}(10339716096\,x^4-147$$

$$+5039680653\,x^2-659866144\,x+30118144)(x-1)^{11}\,{Y_2}^3)Y_0{}^3$$

$$+(290467762239442702860288 0\,x^{12}(43094485499904\,x^7-153945538910208\,x^6+224392668901164\,x^5-171923919956365\,x^4+7392580922814 4$$

$$+(102477026518075385569109606 4\,x^{13}(110075314176\,x^6-330322043520\,x^5+404712363768\,x^4-257183189255\,x^3+88277634240\,x^2-1515451$$

$$+307431079554226156707328819 2\,x^{14}(13759414272\,x^6-47188863360\,x^5+67452060628\,x^4-51436637851\,x^3+22069408560\,x^2-5051506432\,x$$

$$+258242106825549971634156208128\,x^{15}(281346048\,x^5-804027852\,x^4+919370737\,x^3-525781344\,x^2+150386880\,x-17210368)(x-1)^{10}\,Y_2\,Y_1$$

$$+90384737388942490071954672844 80\,x^{16}(-4298112\,x+5750784\,x^4-13146820\,x^3+11273973\,x^2+614656)(x-1)^{11}\,{Y_2}^2\,{Y_1}^4$$

$$+16871817645935931480098205597696 0\,x^{17}(117504\,x^3-201457\,x^2+115166\,x-21952)(x-1)^{12}\,{Y_2}^3\,{Y_1}^3$$

$$+17715408528232728054103115877580 80\,x^{18}(-2743\,x+784+2400\,x^2)(x-1)^{13}\,{Y_2}^4\,{Y_1}^2$$

$$+69444401430672293972084214240116736\,x^{19}\,(7\,x-4)\,(x-1)^{14}\,{Y_2}^5\,Y_1$$

$$+23148133810224097990694738080038912\,x^{20}\,(x-1)^{15}\,{Y_2}^6$$

Bien sur, cette expression est horrible à voir. Mais sa grande qualité est qu'elle se calcule très vite : avec MAPLE, il nous a fallu quelques secondes pour calculer ce Hessien et deux heures pour calculer le même polynôme de Darboux par la méthode directe. Nous verrons plus bas qu'il est illusoire pour l'instant d'espérer calculer les autres intégrales premières autrement que par ce moyen.
Comme les trois premiers invariants sont algébriquement indépendants ([Spr77]), toute solution y de L est caractérisée par la donnée de trois constantes c_i $(i = 1..3)$ telles que $M_i(y) = c_i$. Toute solution non-singulière* du système $\{M_i(y) = c_i, i = 1..3\}$ est une solution algébrique de L (et ses conjuguées sont solutions du même système).
Si on se donne 9 constantes arbitraires $c_{i,j}$, les relations $M_i(y_j) = c_{i,j}$ définissent 3 solutions algébriques (non conjuguées) de L ; comme l'extension $k\langle y_1, y_2, y_3\rangle$ est algébrique, elle ne contient pas de nouvelle constante : les solutions non-singulières du système $\{M_i(y_j) = c_{i,j}(i, j = 1..3), Wr(y_1, y_2, y_3) \neq 0\}$ engendrent donc une extension de Picard-Vessiot pour L.

SOLUTIONS ALGÉBRIQUES DE L'ÉQUATION DE HURWITZ.

Bâtissant sur les travaux de Singer et Ulmer, W. Fakler a donné la décomposition du polynôme minimal d'une solution algébrique pour les équations d'ordre 3 dont le groupe de Galois est G_{168} (voir [Fak94]). Il n'est néanmoins pas arrivé à calculer effectivement le polynôme minimal de l'équation de Hurwitz, et pour cause : l'équation $L^{\circledS 21}(y) = 0$ qu'il faut résoudre pour exprimer les coefficients du polynômes est d'une taille telle qu'elle en devient inconstructible (l'équation est d'ordre 253 et les coefficients sont des polynômes de degré environ 250 dont les coefficients comportent environ 500 chiffres**

* c'est à dire qu'il existe i tel que $\frac{\partial M_i}{\partial y'^t} \neq 0$

** Pour $L^{\circledS 14}$, la situation est a peine meilleure : l'équation est d'ordre 120 et les coefficients ont environ 240 chiffres. J'ai arrêté une tentative de calcul après 3 jours C.P.U (sur une machine "rapide" DEC alpha à 64 bits et 300 Mo de mémoire

Nous avons vu plus haut que pour G_{168}, si l'on connaît l'expression de l'invariant (dans $C[y_i]$) I_1 de degré 4, alors on construit $I_2 = H(I_1)$ de degré 6, $I_3 = HB(I_1, I_2)$ de degré 14, et $I_4 = Jac(I_1, I_2, I_3)$ de degré 21. Ces quatre invariants engendrent l'algèbre des invariants Le problème, ici, est que l'on connaît la *valeur* de I_1 (comme élément de $\mathbb{C}(x)$) mais qu'on ne peut pas en déduire la valeur de I_2. Pour appliquer notre méthode, nous notons que $Tr(A^*) = \frac{7x-4}{x(x-1)} = f'/f$ avec $f = x^4(x-1)^3$. Nous pouvons calculer l'intégrale première M_1 de degré 4 de (A^*). Le coefficient de y_1^4 dans M_1 est nul et nous en déduisons que $I_1 = 0$ (ceci a déjà été remarqué par plusieurs auteurs, e.g [SUl93c]). Nous calculons[§] $H(M_1)$; par la proposition 50, $M_2 := f^2 H(M_1)$ est encore une intégrale première de (A^*) de degré 6. Examinant le coefficient de y_1^6, nous en déduisons que $I_2 = \frac{1}{x^4(x-1)^3}$. Continuant le processus, nous calculons $M_3 := f^2 HB(M_1, M_2)$ et $M_4 := fJ(M_1, M_2, M_3)$; nous en déduisons que $I_3 = \frac{1}{x^9(x-1)^7}$ et $I_4 = \frac{1}{x^{14}(x-1)^{10}}$. En substituant dans les expressions données par Fakler, on peut en déduire le polynôme minimal d'une solution algébrique.

De cette manière, le calcul est passé de "absolument impossible pour l'instant" à une heure ; en effet, les expressions de M_3 et M_4 sont gigantesques et les calculs de déterminant deviennent très long. On peut là encore accélérer nettement les choses de la manière suivante : le seul coefficient dont on ait besoin dans les M_i est le premier. Il est donc inutile de calculer les autres. Si on ne prend que les termes en $y_1^1, \ldots, y_1^4$ dans M_1, que les termes en y_1^4, y_1^5, y_1^6 dans M_2, et que les termes en y_1^{13}, y_1^{14} dans M_3, alors on obtient toujours les invariants cherchés mais l'ensemble du calcul (calcul de M_1 compris) prend une petite dizaine de minute, ce qui devient raisonnable.

Remarque. - Cette méthode donne aussi un moyen* d'obtenir des solutions liouvilliennes d'équations différentielles d'ordre 3 de manière "directe" : comme les intégrales premières polynomiales M_1 et M_2 associées à I_1 et I_2 ont une solution non-triviale en commun, le résultant en Y_3 de M_1 et M_2 est non-nul. Comme ce résultant appartient à l'idéal (algébrique) engendré par M_1 et M_2, une solution commune de $M_1(y) = 0$ et $M_2(y) = 0$ annule le résultant. On obtient donc une relation homogène (de degré 24) entre Y_1 et Y_2 qui fournit à son tour le polynôme minimal d'une solution de l'équation de Riccati.
Notons, néanmoins, que cette méthode est nettement moins rapide que la méthode de Singer-Ulmer si on lui apporte les améliorations indiquées ci-dessus. ⋄

6.4. Conditions nécessaires

S'il est difficile de calculer des solutions rationnelles de puissances symétriques, on peut donner de bonnes conditions nécessaires d'existence de telles solutions : l'existence de so-

interne, le calcul occupait alors plus de 120 Mo). A ma connaissance, personne a ce jour n'est arrivé à calculer $L^{\circledS 14}$ pour cette équation et, même si c'était possible, je ne suis pas sur que le résultat serait utilisable.

§ Par calcul direct de Hessien, on ne résout pas de nouveau système différentiel

* Ce moyen est un peu lourd, mais le résultat est de toute façon intrinsèquement épouvantable

lutions rationnelles (ou radicales) de puissances symétriques dépend de relations combinatoires entre les exposants aux singularités (e.g [SUl94, SUl93c]) ; d'un point de vue pratique, il est donc préférable de commencer par là.

Une autre observation est la suivante : calculer la matrice $S^m(A)$ est très simple et très rapide (même pour de 'grandes' valeurs de m et n). Les difficultés commencent quand on se met à utiliser un vecteur cyclique ; nous ne connaissons toujours pas de critère, pour l'instant qui permette de choisir un 'bon' vecteur cyclique (au sens où l'équation produite n'ait pas de trop gros coefficients par rapport à la taille des coefficients de l'équation initiale). La question trouble qui se profile derrière cela est que l'utilisation d'un vecteur cyclique est (pour l'instant) l'algorithme le plus efficace que l'on connaisse pour calculer les solutions rationnelles d'un système. Cela pose une double question algorithmique :

Question 54. :
1. Peut-on trouver un algorithme de recherche des solutions rationnelles (ou exponentielles) d'un système différentiel linéaire qui soit significativement plus efficace que le vecteur cyclique ?
2. Peut-on déterminer un "bon" vecteur cyclique, c'est à dire un vecteur qui minimise la taille de l'équation produite ?

7. Questions de degré

A ce stade, nous disposons d'une procédure pour calculer des polynômes de Darboux si leur degré est donné ; nous en avons de plus des interprétations intéressantes en termes de théorie de Galois. Il nous reste maintenant à borner leur degré ce qui, nous l'avons vu, est le plus difficile. Grâce au théorème 38, nous savons que cela se ramène à borner le degré des semi-invariants du groupe de Galois différentiel G (c'est à dire borner le degré des générateurs du semi-groupe multiplicatif formé par les invariants ou, au moins, borner le degré d'un semi-invariant de degré minimal). Nous ne savons pas complètement résoudre ce problème (voir l'annexe 2, pour un rapide état de l'art et des pointeurs sur la littérature), mais nous donnons dans cette section de nombreux éléments de réponse.

Lemme 55. *Soit $Y' = AY$ un système différentiel linéaire homogène. Alors, $G \subset SL_n(C)$ si et seulement si il existe $f \in k$ tel que $f'/f = Tr(A)$.*

Preuve. - C'est un résultat probablement classique dont la preuve est similaire à celle donnée par Kaplansky ([Kap57] page 41) pour le cas d'une équation d'ordre n. Il suffit de noter que, en posant $Z = e^{-\int \frac{Tr(A)}{n}} Y$, Z vérifie $Z' = BZ$ où B est à coefficients *dans* k et $Tr(B) = 0$; si U est une matrice fondamentale de solutions pour (B), on a $\det(U)' =$

$Tr(B)\det(U) = 0$ et la preuve de Kaplansky s'étend en remplaçant le Wronskien par $\det(U)$. □

Si $f'/f = Tr(A)$ mais que $f \notin k$, nous savons que D admet un polynôme de Darboux sur $k(f)$ si et seulement si elle en admet sur k ; comme le groupe de Galois d'une extension de Picard-Vessiot de $k(f)$ est unimodulaire, nous pouvons supposer que $G \subset SL_n(C)$; nous faisons cette hypothèse dans ce qui suit.

Un autre résultat simple donne un borne théorique sur le degré des générateurs de l'algèbre des intégrales premières.

Lemme 56. *Si G est réductif, l'algèbre des intégrales premières est finiment engendrée.*

Preuve. - le corollaire 43 donne un isomorphisme d'algèbre entre la C-algèbre engendrée par les intégrales premières polynomiales et la C-algèbre engendrée par les invariants. Le lemme découle alors du théorème de finitude de Nagata ([Spr77, Die70]) qui montre que l'algèbre des invariants d'un groupe réductif est finiment engendrée. □

7.1. Le cas irréductible

Soit L une équation différentielle linéaire homogène irréductible unimodulaire de groupe de Galois $G \subset SL_n(C)$. Une condition nécessaire (mais non suffisante) pour que G admette un semi-invariant est que, pour un certain entier m, G n'agisse pas transitivement sur $S^m(V)$ (un semi-invariant correspond à un sous-espace 1-dimensionel de $S(V)$ stable sous G). Beukers, Brownawell, et Heckmann ont donné un critère pour décider si G agit transitivement sur $S^m(V)$ pour tout m (voir le théorème 2.2 page 88 dans [BBH88]) :

Lemme 57 [BBH88]. *Soit L une équation différentielle linéaire homogène irréductible unimodulaire de groupe de Galois $G \subset SL_n(C)$, et soit V son espace de solutions. S'il existe un entier m tel que G n'agit pas transitivement sur $S^m(V)$, alors soit $G/Z(G)$ est un groupe fini soit $S^2(V)$ contient un sous-espace propre stable sous G.*

Si G agit transitivement sur $S^m(V)$ pour tout m, alors on dit que L (ou le système associé) est *Siegel normale* ([BBH88]). Si $G/Z(G)$ est un groupe fini (où $Z(G)$ désigne le centre de G, [BBH88] page 88), alors L admet une solution liouvillienne ; Si L admet une solution liouvillienne, elle admet au moins un semi-invariant et on peut borner le degré de ce semi-invariant (voir [Sin81, Ulm92, SUl93b], l'annexe 3, ou le chapitre suivant). D'autre part, on peut tester si $S^2(V)$ est réductible ([BrP94],[Sin94],[Gri90]) ; le critère ci-dessus est donc effectif.

Pour étudier la réciproque, nous pouvons faire l'observation suivante. Notons G° la composante connexe de l'identité de G. On sait (e.g [Sin89]) que G° est le groupe de Galois d'une extension de Picard-Vessiot pour L d'une extension algébrique finie k_1 de k. Comme l'existence de polynômes de Darboux sur k_1 implique l'existence de polynômes de Darboux sur k, nous pouvons supposer *dans cette section* que G *est connexe*. Les groupes connexes irréductibles n'ayant pas d'invariants ont donné lieu à une classification sophistiquée (voir l'appendice 2), que nous ne savons pas (pour l'instant) tester de manière effective pour n'importe quelle équation.

On peut citer de nombreux cas d'existence d'intégrales premières que l'on peut tester effectivement. Par exemple :

Pour $n = 2, 3$, le lemme 57 donne un critère effectif de décision* (voir la section précédente).
Si G est résoluble, il y a des solutions liouvilliennes et la réponse est affirmative aussi ([Sin81, Kol48a] ou le corollaire 45)
Si n est premier, alors** G est résoluble (au moins) quand G est imprimitif (car G est monomial dans ce cas, [Ulm92]) ou primitif fini.
Si $n < 7$ et qu'il existe une relation polynomial homogène $P(y_{1,1}, \cdots, y_{1,n}) = 0$ à coefficients dans k entre les solutions de L, alors il y a une solution liouvillienne et un semi-invariant ([Sin86, Com94]).
Si $G \subset O_n(C)$ (le groupe orthogonal), alors Goldman a montré ([Gol58], théorème 4 page 574) que L admet une intégrale première et un invariant de degré 2 (cela tient au fait que $G = G^*$ dans ce cas).

Remarque. - Dans [Gol58], Goldman montre que, pour $G = O(n, C)$ ou $G = SO_n(C)$, cette intégrale première est le polynôme différentiel minimal des solutions de L sur k ; or, la dimension de $O(n, C)$ (i.e le degré de transcendance de l'extension de Picard-Vessiot correspondante) est $\frac{1}{2}n(n-1)$, ce qui illustre le fait que, même si l'ordre du polynôme différentiel minimal de chaque solution est $n-1$, il peut y avoir des relations d'ordre plus petit que $n-1$ entre les solutions de L (par exemple, ici, il y a une relation d'ordre 0 et degré 2). En d'autres termes, l'ordre du polynôme différentiel minimal des solutions donne

* Dans [Mar98], Marotte donne une classification de groupes (connexes) pour $n = 4$ qui laisse entrevoir une réponse positive aussi. Néanmoins, les papiers de cette époque méritent une vérification approfondie car plusieurs notions -notamment la notion de groupe - n'étaient pas encore bien fixées. La thèse de Marotte est parfois impressionnante d'actualité.

** Note postérieure à la remise de ce travail aux rapporteurs : si n est premier et que $G \subsetneq SL_n(V)$ est irréductible, alors G admet un semi-invariant. Soit G^o la composante connexe de l'identité dans G. Si G^o agit de manière réductible sur V, alors un théorème de Clifford montre que, comme n est premier, V est une somme d'espace 1-dimensionels stables sous G^o ([BBH88], appendice), donc G admet un semi-invariant. Enfin, Gabber a donné la liste complète des groupes linéaires algébriques connexes unimodulaires d'ordre premier qui agissent irréductiblement sur V ([Beu92]) ; en étudiant cette liste, on voit que tous les groupes qui la composent (sauf SL_n) admettent un invariant, d'où le résultat. Le critère de Beukers, Brownawell, et Heckmann nous donne donc une procédure pour décider si un système d'ordre premier admet un polynôme de Darboux.

une borne sur la dimension du groupe de Galois mais ne donne certainement pas sa valeur (sauf exceptionnellement, par exemple quand le groupe est fini). ⋄

7.2. Le cas réductible

Supposons maintenant que L est réductible (ceci peut se tester effectivement, voir par exemple [BrP94, Sin94, Hoe95, Gri90]). Cela signifie que L, vue comme opérateur, peut se factoriser en $L = L_1 L_2$. Pour un système (A), cela signifie que (A) est de même type que (B), où B est triangulaire inférieure par blocs (et les blocs de la diagonale sont irréductibles, i.e ils ne peuvent plus subir de telle réduction) ; (A) est complètement réductible (et G est réductif) si et seulement si B peut être choisie diagonale par blocs.

Nous avons le résultat préliminaire suivant :

Lemme 58. *Supposons que $L = L_1 L_2$ et que L admet un polynôme de Darboux M. Alors, ou bien L_2 a un polynôme de Darboux, ou bien M appartient à l'idéal différentiel $[L_2]$ engendré par L_2.*

Preuve. - Soit M un polynôme de Darboux pour L avec $DM = \alpha M$. Réduisons (au sens de Ritt) M par L_2 (qu'on suppose unitaire). On obtient $M = \sum_{i=0}^{n-1-r} q_i L_2^{(i)} + R$. Si $R = 0$, alors $M \in [L_2]$; Supposons que $R \neq 0$. Rappelons nous que, pour tout $P \in k[y, \cdots, y^{(n-1)}]$, on a $P' = DP + \frac{\partial P}{\partial y_{n-1}} L$. Il en découle que :

$$DM = q_{n-1-r} L + \sum_{i=0}^{n-r} \tilde{q}_i L_2^{(i)} + R' = \alpha \sum_{i=0}^{n-1-r} q_i L_2^{(i)} + \alpha R.$$

Il en découle que, pour toute solution z de $L_2(z) = 0$, on a $R(z)' = \alpha R(z)$ et R est donc bien un polynôme de Darboux pour L_2. □

Exemple. - Considérons $L = (\partial^2 - x)(\partial^2 - x) = \partial^4 - 2x\partial^2 - 2\partial + x^2$. On peut vérifier que L admet une intégrale première polynomiale (voir plus loin). Or, $L_1 = \partial^2 - x$ a pour groupe de Galois $SL_2(C)$ (cf. [Kap57]) et n'admet donc pas de semi-invariant. Il en découle que $M \in [\partial^2 - x]$. De fait, le polynôme $M = (L_1' - y)L_1' + (y' - xL_1)L_1$ vérifie $DM = 0$. ⋄

Si L n'est pas complètement réductible, le fait que L_2 admette un polynôme de Darboux n'implique pas que L en admette un. Par exemple, si l'on prend $L = (\partial^2 - x)(x\partial - 1)$, alors $L_2 = x\partial - 1$ admet un polynôme de Darboux de degré 1 (en l'occurrence : y) mais on peut montrer que L n'en admet pas (L^* n'a pas de solution rationnelle). Néanmoins, on a le résultat utile suivant :

Lemme 59. *Supposons que $L = L_1 L_2$ et que L_1 admet un polynôme de Darboux M_1. Alors L admet un polynôme de Darboux.*

Preuve. - Soient A_1 et A_2 les matrices des systèmes correspondant à L_1 et L_2. L'équation $L(y) = 0$ se réécrit en le système $\{L_1(z) = 0, L_2(y) = z\}$. Donc, L est équivalente au système $Y' = AY$ suivant (où c dénote le coefficient dominant de L_2) :

$$A = \left(\begin{array}{ccc|c} & & & \\ & A_1 & & 0 \\ - & - & - & - \ - \ - \\ \vdots & & & \\ 0 & & & A_2 \\ 1/c & 0 & \cdots & \end{array}\right).$$

Sous cette forme, tout Darboux pour A_1 est immédiatement un Darboux pour A. □

Remarque. - En termes d'équations, si M_1 est un polynome de Darboux pour L_1, alors on vérifie que $M = M_1(L_2(y))$ est un polynôme de Darboux pour L. Cela tient au fait que L_2 est un morphisme de $Sol(L)$ dans $Sol(L_1)$ ⋄

Remarque. - On a le résultat similaire suivant : Soit $Y' = AY$ un système complètement réductible avec

$$A = \left(\begin{array}{ccc} A_1 & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & \cdots & A_r \end{array}\right).$$

Si l'un des sous-systèmes admet un semi-invariant, alors D admet un polynôme de Darboux. ⋄

Le cas réductible et complètement réductible.

Si le système est réductible et complètement réductible (ce qui peut se tester effectivement, [Sin94]), le lemme 56 montre que le degré des générateurs de l'algèbre des intégrales premières polynomiales est - au moins théoriquement - borné.

De par la complète réductibilité, on est ramené à étudier les sous-systèmes obtenus par factorisation. En effet, on a alors $L = ppcmg(L_1, \ldots, L_r)$ avec les L_i irréductibles (où la notation *ppcmg* représente le plus petit commun multiple à gauche des deux opérateurs) ; de même, on a $V = V_1 \oplus \ldots \oplus V_r$, l'action de G se décompose sur chaque V_i, et chaque $g \in G$ est donc diagonal par blocs. On en déduit que $G \subset G_1 \times \ldots \times G_r$ (où G_i est le groupe de Galois des L_i). Si l'un des G_i admet un semi-invariant, alors c'est aussi un semi-invariant pour G (car les actions de G et G_1 coïncident sur $S(V_1)$).

Supposons que aucun des G_i n'admet de semi-invariant. Nous devons maintenant chercher quelles "relations entre les solutions" donnent lieu à des polynômes de Darboux. Nous aurons besoin de la définition suivante.

Définition 60. Soient $Y' = A_1Y$ et $Y' = A_2Y$ deux systèmes de taille n, soient U_1, U_2 deux matrices fondamentales de solutions, et V_1, V_2 leurs espaces de solutions. On dit que (A_1) et (A_2) sont *cogrédients* s'il existe une matrice P inversible et f exponentiel sur k tels que $U_1 = fPU_2$. On dit que (A_1) et (A_2) sont *contragrédients* si (A_1) est cogrédient avec (A_2^*).
Par abus de langage, on emploie ces mêmes termes pour V_1 et V_2.

Le fait que deux systèmes soient cogrédients ou contragrédients peut se tester de manière effective (voir [Sin94] où un test, dû probablement à Ore, est donné pour les équations) Notre premier résultat est le suivant :

Lemme 61. *Soit $G \in GL(V)$ et supposons que $V \supset V_1 \oplus V_2$, où les V_i sont stables sous l'action de G. Si V_1 est G-isomorphe à V_2^*, alors G admet un invariant de degré 2. Si V est l'espace solution d'un système différentiel et que V_1 et V_2 sont contragrédients, alors G admet un semi-invariant de degré 2.*

Preuve. - Posons $W = V_1 \oplus V_2$. On sait que $(V_1 \times V_1^*)^G \simeq End_G(V_1)$ et* donc $\dim_C(V_1 \times V_1^*)^G \geq 1$ (car $End_G(V_1)$ contient au moins l'identité). Or, $S^2(W) \simeq S^2(V_1) \oplus S^2(V_2) \oplus (V_1 \otimes V_2)$. Comme $V_1 \otimes V_2$ est par hypothèse G-isomorphe à $V_1 \otimes V_1^*$, on en déduit que $\dim_C (S^2(W))^G \geq 1$ et il y a donc au moins un invariant de degré 2. Le résultat sur les systèmes contragrédients découle du lemme 31 □

Exemple. - Soient $L_1 = L_2 = (\partial^2 - x)$ et $L = L_1L_2$, c'est à dire

$$L(y) = \frac{d^4}{dx^4}y(x) - 2\,x\frac{d^2}{dx^2}y(x) - 2\,\frac{d}{dx}y(x) + x^2y(x)$$

On peut vérifier que cette équation est complètement réductible et que toute factorisation s'écrit (voir [BrP94]) $L = L_3L_4$ avec

$$\begin{aligned} L_3 &= -\frac{(c^4x^3 - 8b^2c^2x^2 + 2bxc^3 + 16b^4x + c^4 - 8b^3c)\,y(x)}{(c^2x - 4b^2)^2} + \frac{c^2\frac{d}{dx}y(x)}{c^2x - 4b^2} + \frac{d^2}{dx^2}y(x) \\ L_4 &= -\frac{(c^2x^2 - 4b^2x - 2bc)\,y(x)}{c^2x - 4b^2} - \frac{c^2\frac{d}{dx}y(x)}{c^2x - 4b^2} + \frac{d^2}{dx^2}y(x) \end{aligned}$$

où b, c sont des constantes arbitraires. De plus, le théorème d'unicité de factorisation de

* La notation $End_G(V_1)$ dénote les endomorphismes de V_1 qui commutent avec tous les éléments de G

Loewy (voir [Sin94]) montre que, comme $Gal(L_1) = Gal(L_2) = SL_2(C)$, toute factorisation est de la forme L_3L_4 avec $Gal(L_3) = Gal(L_4) = SL_2(C)$. Comme $L_1 = L_1^*$, on obtient $L_2 \sim L_4^*$ et il y a donc un invariant de degré 2. De fait, si on calcule le carré symétrique de L (car $L = L^*$), on obtient :

$$x^3\partial^{10} - 3x^2\partial^9 + \left(6x - 12x^4\right)\partial^8 + \left(-6 - 30x^3\right)\partial^7 + \left(84x^2 + 48x^5\right)\partial^6 + \left(-168x + 288x^4\right)\partial^5$$
$$+ \left(-64x^6 + 168 + 116x^3\right)\partial^4 + \left(-480x^5 - 180x^2\right)\partial^3 + \left(360x - 720x^4\right)\partial^2 + \left(-360 - 120x^3\right)\partial$$

Il n'a pas de terme en y et admet donc la solution $y = 1$. On en déduit l'intégrale première

$$Y_3{}^2 - 2xY_3Y_1 - 3Y_3Y_0 - xY_2{}^2 + Y_2Y_1 + 2x^2Y_2Y_0 + x^2Y_1{}^2 + 2xY_1Y_0 + \left(-x^3 + 2\right)Y_0{}^2.$$

Remarquons dans cet exemple que, d'après le lemme 58, M appartient aux idéaux différentiels engendrés respectivement par L_2 et par L_4 (pour toute valeur de b et c) ; Si $V = V_2 \oplus V_4$, il en découle que, pour tout $y \in V_2$ ou tout $y \in V_4$, on a $M(y) = 0$. Néanmoins, si y est somme de deux vecteurs de V_2 et V_4 respectivement, il se peut que $M(y) \neq 0$. $\diamond$

Ceci conduit bien à se poser la question suivante : Soit $G \in GL(V)$ et supposons que $V = V_1 \oplus V_2$, où les V_i sont stables sous G. Si V_1 est G-isomorphe à V_2 (ou si V_1 et V_2 sont cogrédients), alors G admet-il toujours un semi-invariant ?

Malheureusement, la réponse est 'non' ; par exemple, on peut vérifier que $SL_3(C) \times SL_3(C)$ admet une orbite dense, donc n'a pas d'invariants ([PV94] ou appendice 2).

À l'opposé, nous pouvons encore adapter un joli critère de Beukers,Brownawell, et Heckmann ([BBH88], théorème 2.3) pour décider si un système n'a pas de polynôme de Darboux :

Corollaire 62. *Soit (A) un système complètement réductible diagonal par blocs et V son espace de solutions ; soit $V = \oplus V_i$ une décomposition de V en sous-espaces irréductibles et (A_i) les sous-systèmes correspondants (les blocs de A). Si les trois conditions suivantes sont vérifiées, alors (A) n'admet pas de polynôme de Darboux :*

1 Aucun des A_i n'admet un polynôme de Darboux.
2 Il n'existe pas de couple d'entiers (i, j) tels que V_i et V_j soient contragrédients
3 Il n'existe pas de couple d'entiers (i, j) tels que V_i et V_j soient cogrédients

Le cas réductible non complètement réductible.

Dans le cas réductible et non-complètement réductible (par exemple l'opérateur $L = (\partial^2 - x)(x\partial - 1)$ mentionné plus haut), nous n'avons pas d'autre résultat positif que nos deux lemmes 58 et 59.

Pour le cas où $k = C$, on peut se reporter à [Now94] (ou aux articles de Nowicki) où divers résultats de finitude (par exemple le théorème de Weitzenböck) sont étudiés ;

Pour $k = C(x)$, nous avons le résultat négatif suivant :

Proposition 63. *Il existe un opérateur linéaire sur $\mathbb{C}(x)$ dont l'algèbre des intégrales premières polynomiales n'est pas finiment engendrée.*

Preuve. - Le contre-exemple de Nagata au $14^{\text{ième}}$ problème de Hilbert est un sous groupe linéaire algébrique réductible (mais non réductif) de $GL_{32}(\mathbb{C})$ (voir e.g [Die70]) dont l'anneau des invariants n'est pas finiment engendré. Le résultat de Tretkoff et Tretkoff ([TT79]) montre qu'il existe un opérateur L_{32} à coefficients dans $\mathbb{C}(x)$ admettant ce groupe pour groupe de Galois différentiel. Le théorème 38 montre alors que l'opérateur L_{32}^* a une algèbre d'intégrales premières polynomiales non finiment engendrée. □

8. Conclusion

Il ressort de ce chapitre que la stratégie de calculer des intégrales premières s'avère très intéressante quand le groupe de Galois est de "petite dimension" (fini, ou à composante connexe résoluble) ou de "grande dimension" (par exemple, le groupe orthogonal ou bien $PSL_2(C)$, où une intégrale première caractérise le polynôme différentiel minimal d'une solution).
En matière de théorie de Galois différentielle, il reste de grands problèmes ouverts comme : déterminer la dimension d'une extension de Picard-Vessiot, déterminer le groupe de Galois, caractériser le groupe de Galois (c'est à dire l'idéal des relations qui lui confèrent une structure de groupe algébrique) ... Notre approche ne donne pas une réponse complète à ces questions mais elle contribue à éclairer la situation pour un système donné.

Le travail que nous avons mené dans ce chapitre peut se comprendre comme une étape vers une compréhension complète (i.e une version effective) du théorème de Chevalley ([MRa89, Ber86, Spr81]) qui caractérise le groupe de Galois par les constructions sur V qu'il laisse stables. Nous avons exploré les puissances symétriques (et leur duaux) en cherchant à tirer un maximum d'information des invariants polynomiaux (i.e les éléments de $S(V)$ qui sont fixés par G). Il serait maintenant intéressant de comprendre quelles autres constructions peuvent nous apporter des informations (un tel travail est actuellement mené par E. Compoint [Com95a]) et quels autres types d'invariants on peut-être amenés à considérer. Cette idée est similaire à celles qui sont menées en théorie de Galois classiques (voir [AVB93, Col95]) où l'on caractérise les groupes de Galois par de "bonnes" résolvantes (ce qui serait, pour nous, de "bonnes" constructions sur V).

L'ensemble de cet chapitre aurait pu être écrit dans le langage des connections (voir

[MRa89, Ber86, Mor94]) et s'y traduit très facilement. Ce formalisme a plusieurs avantages : par exemple, il permet d'étendre nos résultats à des situations méromorphes plus vastes (voir e.g [MRa89, LRi91] et les références à une multitude de travaux intéressants qu'on y trouve), il donne des résultats intrinsèques et raccourcit parfois les preuves. Nous avons choisi de ne pas utiliser ce formalisme pour essentiellement deux raisons. La première est que les résultats s'expriment bien dans le formalisme utilisé sans qu'il soit nécessaire d'en introduire un nouveau. La deuxième (et principale) est que, pour les calculs effectifs, on cherche des *valeurs* des coefficients et surtout des valeurs des invariants ; pour pouvoir calculer effectivement ces valeurs (par exemple pour le théorème 52), il nous faut savoir exactement dans quelle base nous sommes et la formulation non-intrinsèque s'impose dans ce cas.

En matière d'efficacité, il nous reste encore des problèmes car la taille des systèmes croit vite et le vecteur cyclique produit des équations dont la taille des coefficients explose. Il y a peut-être un espoir d'amélioration en utilisant des calculs locaux ou modulaires. Une autre idée raisonnable est de changer la structure de données et de représenter nos coefficients par des programmes d'évaluation ; cette stratégie a été menée avec succès en théorie de l'élimination (e.g [GHe91]).

Enfin, si nous considérons des systèmes à paramètres et que nous cherchons pour quelles valeurs des paramètres le système admet des intégrales premières, nous sommes ramenés à chercher pour quelles valeurs des paramètres une équation différentielle admet des solutions rationnelles. Ce problème introduit des problèmes diophantiens délicats (les paramètres peuvent apparaître comme degrés de polynômes à déterminer) et nous ne serions pas surpris qu'ils s'avèrent indécidables du point de vue algorithmique. Néanmoins, l'utilisation de conditions nécessaires ([DLR92, SUl94, Ulm94]) ou de méthodes "transcendantes" (e.g [Mit95, LRi91] et références incluses) permet souvent de répondre à la question ; ces méthodes ne donnent pas (ou pas encore) lieu, me semble-t-il, à des algorithmes complets, mais donnent suffisamment d'information pour qu'on puisse 'terminer' le travail avec une boite à outils informatique. Pour le problème des paramètres et pour le traitement de gros systèmes, ces approches semblent s'imposer, et ouvrent la voie à de très notables avancées dans la compréhension effective des groupes de Galois différentiels.

CHAPITRE III

Équations différentielles linéaires du second ordre

Il existe des algorithmes pour déterminer les solutions liouvilliennes d'équations différentielles linéaires homogènes du second ordre (voir [Kov86, SUl93a]). Dans ce chapitre, nous montrons comment, en combinant finement les techniques de ces articles, on peut trouver toutes les solutions liouvilliennes d'une équation différentielle linéaire irréductible du second ordre en ne calculant que des solutions rationnelles d'équations associées (les produits symétriques). Le résultat est une version rationnelle simplifiée et très aisée à implanter de l'algorithme de Kovacic.

Par rapport aux notions du chapitre précédent, cela revient à calculer des intégrales premières directement plutôt que des polynômes de Darboux. Ce chapitre reprend l'article [UWe94], écrit en commun avec Félix Ulmer.

Ce chapitre reprend l'article [UWe94], écrit en commun avec Félix Ulmer*. La première partie sert essentiellement à fixer les notations et permet de lire ce chapitre indépendamment des précédents. Les résultats de la deuxième partie sont très proches des résultats de la partie précédente; de cette manière, l'algorithme présenté dans la troisième partie peut aussi se comprendre comme un algorithme de calcul d'intégrale première (à multiplication par y^m près, un polynôme de Darboux pour l'équation de Riccati est un polynôme de Darboux pour L, cf [Wei94] partie 5). À la fin de ce chapitre, nous montrons comment nos techniques permettent aussi de décider très simplement si une équation de Riccati admet des solutions par radicaux.

1. Differential Galois Theory

The material presented in this section is well known and has been included to make the exposition self contained. We refer to [Kap57, Kol48a, Sin89] for further details about this section.

* Pour des raisons historiques, les polynômes de Darboux sont appelés polynômes spéciaux dans l'article [UWe94]. Nous avons corrigé cette notation ici, de manière à maintenir une cohérence avec les parties précédentes

1.1. Introduction

A *differential field* (k, δ) is a field k together with a derivation δ on k. We also write $y^{(n)}$ instead of $\delta^n(y)$ and $y', y'', \ldots$ for $\delta(y), \delta^2(y), \ldots$. The field of constants $\{c \in k | c' = 0\}$ is denoted $\mathcal{C}$. Unless otherwise stated, a differential equation $L(y) = 0$ over k always means an ordinary homogeneous linear differential equation

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0 \qquad (a_i \in k).$$

In the following we will look at solutions of $L(y) = 0$ in a differential field extension of k. A *differential field extension* of (k, δ) is a differential field (K, Δ) such that K is a field extension of k and Δ is an extension of the derivation δ of k to a derivation on K. The differential Galois group $\mathcal{G}(K/k)$ of a differential field extension K of k is the set of k-automorphisms of K which commute with the derivation of K. There is a unique way to extend the derivation of k to an algebraic extension of k making any algebraic extension of k into a differential extension.

Definition 64. A differential field extension (K, Δ) of (k, δ) is a *Liouvillian extension* if there is a tower of fields

$$k = K_0 \subset K_1 \subset \cdots \subset K_m = K,$$

where K_{i+1} is a simple field extension $K_i(\eta_i)$ of K_i, such that one of the following holds:

i) η_i is algebraic over K_i, or
ii) $\delta(\eta_i) \in K_i$ (extension by an integral), or
iii) $\delta(\eta_i)/\eta_i \in K_i$ (extension by the exponential of an integral).

A solution of $L(y) = 0$ which is contained in

1 k, the coefficient field, will be called a *rational* solution,
2 an algebraic extension of k will be called an *algebraic* solution,
3 a Liouvillian extension of k will be called a *Liouvillian* solution

A solution z of $L(y) = 0$ is called *exponential** if z'/z is in the coefficient field k. In the following we will have to compute rational and exponential solutions of $L(y) = 0$. For this reason we always assume that k is a differential field over which such solutions can be computed (e.g. $\mathcal{C}(x), \frac{d}{dx}$)). The computation of an exponential solution is usually much more difficult than the computation of a rational solution.

* Note that the exponential solutions of $L(y) = 0$ do not form a ring.

For $k = \mathcal{C}(x)$ and a differential equation $L(y) = 0$ with coefficients in k, (an) algorithms to compute

1 rational solutions is given in [Lio33]. More recent algorithms for more general coefficient fields are presented in [Br92b, Sin91].
2 algebraic solutions of a second order equation $L(y) = 0$ are given in [Fuc78, Pep62]. The study of the third order case is started in [Jor78], a general algorithm was given by Boulanger (cf. [Sin80]) and rediscovered in [Sin80].
3 Liouvillian solution of a second order equation is given in [Kov86]. A general procedure for equations of arbitrary order is presented in [Sin81]. The third order case is treated in details in [SUl93a].

Definition 65. Let $L(y) = 0$ be a homogeneous linear differential equation of order n with coefficients in k. A differential field extension K of k is a Picard-Vessiot extension (PVE) of k for $L(y) = 0$ if

1 $K = k < y_1, \ldots, y_n >$, the *differential* field extension of k generated by $y_1, \ldots, y_n$ where $\{y_1, \ldots, y_n\}$ is a fundamental set of solutions of $L(y) = 0$.
2 K and k have the same field of constants.

A PVE extension plays the role of a splitting field for $L(y) = 0$. A PVE exists and is unique up to differential isomorphisms if the field of constants of k is algebraically closed*. However, this in of characteristic 0 (cf. [Kap57] p.21 and [Kol48b]). In the sequel we will always assume that the coefficient field is algebraically closed of characteristic 0. By definition the differential Galois group $\mathcal{G}(L)$ of $L(y) = 0$ is the differential Galois group of K/k, where K is a PVE of k for $L(y) = 0$. If we choose a fundamental set of solutions $\{y_1, y_2, \ldots, y_n\}$ of the equation $L(y) = 0$, then for each $\sigma \in \mathcal{G}(L)$ we get $\sigma(y_i) = \sum_{j=1}^{n} c_{ij} y_j$, where $c_{ij} \in \mathcal{C}$. This gives a faithful representation of $\mathcal{G}(L)$ as a subgroup of $GL(n, \mathcal{C})$. Different choices of bases $\{y_1, y_2, \ldots, y_n\}$ give equivalent representations. In the sequel we always consider this equivalence class of representation as *the* representation (module) of $\mathcal{G}(L)$. In fact $\mathcal{G}(L)$ is a linear algebraic subgroup of $GL(n, \mathcal{C})$ (cf. [Kov86]). We can limit our considerations to differential equations with $\mathcal{G}(L) \subseteq SL(n, \mathcal{C})$:

Theorem 66 (Kaplansky, [Kap57] p. 41). *The differential Galois group of a differential equation of the form*

$$L(y) = y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0 \qquad (a_i \in k) \tag{1.1}$$

* Epstein also developed in [Eps55] a Picard-Vessiot theory in the case of a non-algebraically closed constant field. However, this induces unnecessary complications for our purposes and it is better to assume that the constant field is algebraically closed, even though we usually won't use this assumption in practice

is a unimodular group (i.e. $\mathcal{G}(L) \subseteq SL(n,\mathcal{C})$) if and only if $\exists W \in k$, such that $W'/W = a_{n-1}$.

In particular for a differential equation of the form

$$L(y) = y^{(n)} + a_{n-2}y^{(n-2)} + \cdots + a_1 y' + a_0 y = 0 \tag{1.2}$$

we have $\mathcal{G}(L) \subseteq SL(n,\mathcal{C})$. Using the variable transformation $y = z \cdot e^{\left(-\frac{\int a_{n-1}}{n}\right)}$ it is always possible to transform a given differential equation $L(y)$ into an equation $L_{SL}(y)$ of the form (1.2) without altering the Liouvillian character of the solutions. This transformation is always performed in [Kov86]. The algorithm presented in this chapter works independently of this particular form and avoids unnecessary transformations.

1.2. Properties of the differential Galois group

Properties of the equation $L(y) = 0$ are reflected by properties of the group $\mathcal{G}(L)$. To the equation (1) we associate a linear differential operator:

$$p(\delta) \quad = \quad a_n\delta^n + a_{n-1}\delta^{(n-1)} + \cdots + a_0$$

The set of differential operators forms a ring $k[\delta]$ where multiplication is defined by $\delta a = a\delta + \delta(a)$. The ring $k[\delta]$ is a right and left euclidian ring in which a right (resp. left) least common multiple of differential operators can be computed (cf [Ore33]). The factorization of differential operators in $k[\delta]$ is not unique but we have:

Theorem 67 ([Kol48a, Sin89, Sin94]). *The linear differential equation $L(y)$*

1. *factors as a linear differential operator, if and only if $\mathcal{G}(L) \subseteq GL(n,\mathcal{C})$ is a reducible linear group.*
2. *is the least common left multiple of irreducible operators if and only if $\mathcal{G}(L) \subseteq GL(n,\mathcal{C})$ is a completely reducible linear group.*

Another property of $L(y) = 0$ that can be characterized by a property of $\mathcal{G}(L)$ is the solvability in terms of Liouvillian solutions. Note that if a second order equation has a Liouvillian solution, then another Liouvillian solution can be found using the d'Alembert reduction method. Thus a second order equation has either no Liouvillian solutions or only Liouvillian solutions.

Theorem 68 (see e.g. [Kol48a]). *A differential equation $L(y) = 0$ with coefficients in k has only Liouvillian solutions over k if and only if the component of the identity $\mathcal{G}(L)^\circ$ of $\mathcal{G}(L)$ in the Zariski topology is solvable. In this case $L(y) = 0$ has a solution whose logarithmic derivative is algebraic over k.*

This gives the following algorithm to compute Liouvillian solutions of a linear differential equation $L(y) = 0$. First, $\mathcal{G}(L)^\circ$ is of finite index in $\mathcal{G}(L)$; if $\mathcal{G}(L)^\circ$ is solvable, then it can be put simultaneously in triangular form (Lie-Kolchin Theorem, cf, [Kol48a]) and thus has a common eigenvector z. In particular z'/z is in the fixed field of $\mathcal{G}(L)^\circ$. Using the Galois correspondence between algebraic subgroups $\mathcal{G}(L)$ of and differential subfields of a PVE, we get that z'/z is algebraic over k of degree at most $[\mathcal{G}(L) : \mathcal{G}(L)^\circ]$. In [Sin81] it is shown that the algebraic degree of the logarithmic derivative z_1'/z_1 of *a particular* solution z_1 can be bounded independently of the equation $L(y) = 0$ (cf. [Sin81, Ulm92]). The next step is to compute the coefficients of the minimal polynomial of $u_1 = z_1'/z_1$. Since all conjugates u_i of u_1 are also logarithmic derivatives of solutions z_i, the minimal polynomial $P(u)$ of u_1 can be written as

$$P(u) = \prod_{i=1}^{m} \left(u - \frac{\delta(z_i)}{z_i} \right) \tag{1.3}$$

$$= u^m - \frac{\delta\left(\prod_{i=1}^m z_i\right)}{\prod_{i=1}^m z_i} u^{m-1} + \ldots + (-1)^m \prod_{i=1}^{m} \frac{\delta(z_i)}{z_i} \tag{1.4}$$

In particular, the coefficient of u^{m-1} is a negative logarithmic derivative of a product of m solutions of $L(y) = 0$. It is possible to construct a differential equation whose solutions are the products of length m of solutions of $L(y) = 0$:

Definition 69. Let $L(y) = 0$ be a linear differential equation of degree n and fundamental system of solutions $\{z_1, \cdots, z_n\}$; the differential equation $L^{\circledS m}(y)$ whose solution space is spanned by the homogeneous forms of degree m in $z_1, \cdots, z_n$ is called the m-th symmetric power of $L(y) = 0$.

To construct the equation $L^{\circledS m}(y)$ one starts with $Y = \prod_{i=1}^m z_i$, where z_i are arbitrary solutions of $L(y) = 0$. Taking derivatives of Y and replacing derivatives of order m of the y_i on the right hand side by lower oder derivatives using $L(y) = 0$ gives a linear differential equation for Y of order at most $\binom{n+m-1}{n-1}$ (cf. [SUl93b]). The group $\mathcal{G}(L)$ operates on the solutions space of $L^{\circledS m}(y)$ which is a $\mathcal{G}(L)$-module. This gives another representation of $\mathcal{G}(L)$.

From (1.4) we get that the coefficient of u^{m-1} in the minimal polynomial $P(u)$ is an exponential solution of $L^{\circledS m}(y)$.

Example. - Let $L(y) = y'' + \frac{3}{16x^2}y$ and $k = \mathcal{C}(x)$. This equation has a solution whose logarithmic derivative is a solution of

$$P(u) = u^2 - \frac{1}{x}u + \frac{3}{16x^2}$$

The coefficient of u is the negative logarithmic derivative of the solution x of

$$L^{\circledS 2}(y) = y''' + \frac{3}{4x^2}y' - \frac{3}{4x^3}y$$

In this case the exponential solution is even rational. $\diamond$

In general the order of $L^{\circledS m}(y)$ can be less than $\binom{n+m-1}{n-1}$. For second order equations, the order is always $m+1$ (cf. [SUl93b], Lemma 3.5) and the solution space of $L^{\circledS m}(y)$ is isomorphic to the m^{th} symmetric power $\mathcal{S}^m(V)$ (c.f., [Lan92] , p. 586) of the solution space V of $L(y) = 0$. In particular the character χ_m of the representation of $\mathcal{G}(L)$ on the solution space of $L^{\circledS m}(y)$ is the symmetrization of the character χ of the representation of $\mathcal{G}(L)$ on the solution space of $L(y) = 0$. One can compute χ_m from χ (see e.g. [SUl93b]).

Definition 70 (see e.g [Stu94]). Let V be a $\mathcal{C}$ vector space with basis $\{y_1, \ldots, y_n\}$ and $G \subseteq SL(V)$ a linear group. Define an action of $g \in G$ on $\mathcal{C}[y_1, \ldots, y_n]$ by $g \cdot (p(y_1, \ldots, y_n)) = p\left(g(y_1), \ldots, g(y_n)\right)$. A polynomial with the property that

$$\forall g \in G, \quad g\left(p(y_1, \ldots, y_n)\right) = \psi_p(g) \cdot \left(p(y_1, \ldots, y_n)\right), \text{ with } \psi(g) \in \mathcal{C}$$

is called a *semi-invariant* of G. If $\forall g \in G$ we have $\psi_p(g) = 1$, then $p(y_1, \ldots, y_n)$ is called an *invariant* of G.

Clearly ψ_p must be a character of degree one. By differential Galois theory, since an invariant I of degree m of $\mathcal{G}(L)$ is left fixed by $\mathcal{G}(L)$, it must belong to k and thus equals a rational solution of $L^{\circledS m}(y) = 0$. In this chapter we will identify the invariants with this rational solution and by *computing an invariant* we always mean *computing the corresponding rational solution.* Similarly a semi-invariant of degree m corresponds to an exponential solution of $L^{\circledS m}(y) = 0$ and thus, if it is not 0, to a right factor of order one of $L^{\circledS m}(y)$.

If $L(y) = 0$ is a second order equation, then any semi-invariant S of degree m of $\mathcal{G}(L)$ is a non-trivial exponential solution of $L^{\circledS m}(y) = 0$. To this semi-invariant corresponds a character of degree 1 in the decomposition of χ_m (the character of the representation of $\mathcal{G}(L)$ on the solution space of $L^{\circledS m}(y)$). The existence of a non-trivial semi-invariant of degree m can be deduced from the existence of a character of degree 1 in the decomposition of χ_m into irreducible characters.

Using this terminology, we see from (1.4) that the coefficient of u^{m-1} in $P(u)$ is a semi-invariant of degree m of $\mathcal{G}(L)$. One of the results of this chapter is that to any semi-invariant

of $\mathcal{G}(L)$ corresponds a unique polynomial $P(u)$ whose irreducible *factors* are all minimal polynomials of logarithmic derivatives of some solutions of $L(y) = 0$ (Section 2).

Example. - Let $L(y) = y'' + \dfrac{3}{16x^2}y$ and $k = \mathcal{C}(x)$. we choose the two exponential solutions

$$y_1 = e^{\int \frac{1}{4x}} = x^{\frac{1}{4}} \quad , \quad y_2 = e^{\int \frac{3}{4x}} = x^{\frac{3}{4}}$$

as a basis of the solution space of $L(y) = 0$. A PVE of k for $L(y) = 0$ is the algebraic extension $\mathcal{C}(x)(x^{\frac{1}{4}})$ and $\mathcal{G}(L)$ is cyclic of order 4. The group $\mathcal{G}(L)$ is an abelian group and has four characters of degree one: the trivial character $\mathbf{1}$, a character $\psi_{1,1}$ of order 2 (i.e. $(\psi_{1,1})^2 = \mathbf{1}$) and two characters $\psi_{1,2}$ and $\psi_{1,3}$ of order 4. In the basis $\{y_1, y_2\}$, the group $\mathcal{G}(L)$ is generated by:

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

From the above form we get that $\chi = \psi_{1,2} + \psi_{1,3}$ and thus that $\mathcal{G}(L)$ has two linearly independent semi-invariants $S_{1,1} = x^{\frac{1}{4}}$ and $S_{1,2} = x^{\frac{3}{4}}$ of degree one corresponding to the characters $\psi_{1,2}$ and $\psi_{1,3}$. To the logarithmic derivatives of $S_{1,1}$ and $S_{1,2}$ correspond two minimal polynomials $\left(u - \frac{1}{4x}\right)$ and $\left(u - \frac{3}{4x}\right)$ of solutions of $Ri(u) = 0$.
A basis of the solution space of $L^{\circledS 2}(y) = 0$ (cf. previous example) is given by:

$$(y_1)^2 = x^{\frac{1}{2}} \quad , \quad y_1 y_2 = x \quad , \quad (y_2)^2 = x \cdot x^{\frac{1}{2}}$$

In the basis $\{(y_1)^2, y_1 y_2, (y_2)^2\}$, the group $\mathcal{G}\left(L^{\circledS 2}\right)$ is generated by:

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

From the above form we get that $\chi_2 = \mathbf{1} + 2\psi_{1,1}$ and thus that $\mathcal{G}(L)$ has an invariant $I_2 = y_1 y_2 = x$ of degree 2 and two linearly independent semi-invariants $S_{2,1} = y_1^2 = x^{\frac{1}{2}}$ and $S_{2,2} = y_2^2 = x \cdot x^{\frac{1}{2}}$ of degree 2 corresponding both to the character $\psi_{1,1}$. To the logarithmic derivative $\frac{1}{x}$ of I_2 corresponds the polynomial $\left(u^2 - \frac{1}{x}u + \frac{3}{16x^2}\right)$. This polynomial is not irreducible, but is the product of the above polynomials of degree one corresponding to $\psi_{1,2}$ and $\psi_{1,3}$. We will show in this chapter that this factorisation corresponds to the factorisation $\mathbf{1} = \psi_{1,2} \cdot \psi_{1,3}$. $\diamond$

Since exponential solutions (semi-invariants) are usually more difficult to compute than rational solutions (invariants), we want to compute whenever possible the minimal polynomials corresponding to rational solutions (invariants) and, if necessary, factor the corresponding polynomial $P(u)$. In particular we will show that for irreducible second order equations this will always be possible.

1.3. Second order equation

Let $L(y) = y'' + a_1 y' + a_0 y$ be a second order equation with coefficients in k and unimodular Galois group $\mathcal{G}(L) \subset SL(2, \mathcal{C})$. The logarithmic derivatives of the solutions are precisely the solutions of the associated Riccati equation $Ri(u) := u' + a_0 + a_1 u + u^2 = 0$. The possible groups $\mathcal{G}(L)$ are the linear algebraic subgroups of $SL(2, \mathcal{C})$ which can be classified (up to conjugacy) as follows (cf. [Kov86, SUl93a]):

1 The reducible non-reductive groups, where a non-trivial G-invariant subspace has no complementary G-invariant subspace.
2 The diagonal linear algebraic subgroups of $SL(2, \mathcal{C})$.
3 The imprimitive subgroups of $SL(2, \mathcal{C})$ which is either a finite group $D_n^{SL_2}$ of order $4n$ (a central extension of the dihedral groups D_n) and generated by:

$$\begin{pmatrix} e^{\frac{\pi i}{n}} & 0 \\ 0 & e^{-\frac{\pi i}{n}} \end{pmatrix} \text{ and } \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

or the infinite group:

$$D_\infty = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 0 & -a \\ a^{-1} & 0 \end{pmatrix} \right\} \qquad \text{where } a \in \mathcal{C}^*$$

4 A primitive finite subgroup of $SL(2, \mathcal{C})$ which is isomorphic to the tetrahedral, octahedral or icosahedral group which we denote respectively $A_4^{SL_2}$, $S_4^{SL_2}$ and $A_5^{SL_2}$. A definition for these groups is given in [Kov86, SUl93a].
5 The group $SL(2, \mathcal{C})$.

In order to bound the degree of an algebraic solution of $Ri(u) = 0$, we compute the index of a maximal 1-reducible subgroup H_z, i.e. a subgroup having a common eigenvector z (see [Ulm92]). The group H_z is the stabiliser of z'/z and thus, if the index is finite, the minimal polynomial of z'/z will be of degree $[\mathcal{G}(L) : H_z]$. For a second order equation, the possible groups H_z are the reducible subgroups of $\mathcal{G}(L)$.

Lemma 71. *Let H be a finite reducible subgroup of $SL(2, \mathcal{C})$ which is not contained in the center $Z(SL(2, \mathcal{C}))$ of $SL(2, \mathcal{C})$. Then H is cyclic and there exists up to multiples a unique basis in which H is a diagonal subgroup of $SL(2, \mathcal{C})$.*

Proof. - Since H is finite, Maschke's theorem shows that any invariant subspace has a complementary invariant subspace. Thus, we can put the elements of H simultaneously in diagonal form. Since $H \subset SL(2, C)$ the diagonal entries will be given by characters χ and χ^{-1}. Therefore the map $h \in H \mapsto \chi(h)$ is an isomorphism of H onto a finite (and therefore

cyclic) subgroup of C. The result now follows from the linear independence of characters ([Lan92]). □

Lemma 72. *Let $L(y) = 0$ be an irreducible second order equation over k whose differential Galois group $\mathcal{G}(L)$ is a finite unimodular group. Let $Z(\mathcal{G}(L))$ be the center of $\mathcal{G}(L)$. Then, the number of irreducible minimal polynomials of degree $m < [\mathcal{G}(L) : Z(\mathcal{G}(L))]$ of algebraic solutions of $Ri(u) = 0$ is equal to $2/m$ times the number of maximal cyclic subgroups (i.e. not contained in a larger cyclic subgroup) of index m of G. In particular, this number is always finite. All other zeroes of the Riccati are algebraic of degree $[\mathcal{G}(L) : Z(\mathcal{G}(L))]$.*

Proof. - Let w be an algebraic solution of $Ri(u)$; then, the degree m of the minimum polynomial of w equals the index $[\mathcal{G}(L) : H_1]$ of the stabilizer $H_1 = Stab_{\mathcal{G}(L)}(w)$ of w in $\mathcal{G}(L)$. Note that $Stab_{\mathcal{G}(L)}(w)$ always contains $Z(\mathcal{G}(L))$. If $m < [\mathcal{G}(L) : Z(\mathcal{G}(L))]$ then, by the above Lemma, H_1 is a non-central cyclic group having up to multiples a unique basis $\{y_1, y_2\}$ in which it is a diagonal group.
Denote z_1 the solution of $L(y) = 0$ such that $z_1'/z_1 = w$. Then z_1 spanns an H_1-invariant subspace, which by Maschke's Theorem has a complementary subspace spanned by some solution z_2. Since H_1 is also diagonal in the basis $\{z_1, z_2\}$, z_1 must be a multiple of y_1 or y_2, say y_1. The cyclic group H_1 cannot be contained in a larger cyclic subgroup of $\mathcal{G}(L)$: from Lemma 71 such a group would also be diagonal in the (unique up to multiples) basis $\{y_1, y_2\}$ and thus would be contained in H_1, the stabiliser of $w = y_1'/y_1$. In particular H_1 is also the stabiliser of y_2'/y_2 which must be algebraic of the same degree as y_1'/y_1.
It follows that the stabilizer of any algebraic solution of degree $m < [\mathcal{G}(L) : Z(\mathcal{G}(L))]$ of $R_i(u) = 0$ is a maximal cyclic subgroup, and each maximal cyclic subgroup of index $m < [\mathcal{G}(L) : Z(\mathcal{G}(L))]$ is the stabilizer of exactly two algebraic solutions of degree m of $R_i(u) = 0$. If there are N maximal cyclic subgroups of index $m < [\mathcal{G}(L) : Z(\mathcal{G}(L))]$, there are exactly $2N$ solutions of $R_i(u) = 0$ which are algebraic of degree m, and we must have exactly $2N/m$ minimum polynomials of degree m for these solutions. □

Using for example the group theory system CAYLEY one gets:

Corollary 73. *Let $L(y) = 0$ be a second order equation over k. For the possible minimal polynomials of the algebraic solutions of the Riccati equation we get:*

If $\mathcal{G}(L) \cong D_2^{SL_2}$ (quaternion group), there are exactly three minimal polynomials of degree 2 and all the others are of degree 4.
If $\mathcal{G}(L) \cong A_4^{SL_2}$ (tetrahedral group), there are exactly two minimal polynomials of degree 4, one of degree 6, and all the others are of degree 12.
If $\mathcal{G}(L) \cong S_4^{SL_2}$ (octahedral group), there is exactly one minimal polynomial of degree 6, one of degree 8, one of degree 12, and all the others are of degree 24.

If $\mathcal{G}(L) \cong A_5^{SL_2}$ (icosahedral group), there is exactly one minimal polynomial of degree 12, one of degree 20, one of degree 30, and all the others are of degree 60.

This gives a partial proof of the following theorem which is the basis of the Kovacic algorithm:

Theorem 74 ([Kov86, SUl93a]). *Let $L(y) = 0$ be a second order linear differential equation with $\mathcal{G}(L) \subseteq SL(2, \mathcal{C})$.*

1. *$\mathcal{G}(L)$ is a reducible linear group if and only if the differential operator associated to $L(y)$ factors. In this case $L(y) = 0$ has an exponential solution.*
2. *If the previous case does not hold, then $\mathcal{G}(L)$ is an imprimitive linear group if and only if $L(y) = 0$ has a solution whose logarithmic derivative is algebraic of degree 2.*
3. *If the previous cases do not hold, then $\mathcal{G}(L)$ is a primitive finite linear group if and only if $L(y) = 0$ has a solution whose logarithmic derivative is algebraic of degree 4, 6 or 12.*
4. *If the previous cases do not hold, then $\mathcal{G}(L) = SL(2, \mathcal{C})$ and $L(y) = 0$ has no Liouvillian solution.*

In the above result only the minimal degrees of an algebraic logarithmic derivative is mentioned. In this chapter, we will consider also other solutions, where the minimal polynomial is of higher degree, in order to use invariants instead of semi-invariants of $\mathcal{G}(L)$.

2. Algebraic solutions of the first order Riccati equation and the semi-invariants

Let $L(y) = y'' + a_1 y' + a_0 y$ be a second order equation with coefficients in k, and $Ri(u) = u' + a_0 + a_1 u + u^2 = 0$ be the associated Riccati equation. We saw in Section 1.2 that, in order to compute a Liouvillian solution of $L(y) = 0$, one can compute the minimal polynomial $P(u) = u^m + b_{m-1}u^{m-1} + \ldots + b_0$ of an algebraic solution of $Ri(u) = 0$. The main reason for the efficiency of the Kovacic algorithm is the fact that, for $k = \mathcal{C}(x)$ and $a_1 = 0$, the coefficients of $P(u)$ are given by a linear recursion from the knowledge of b_{m-1} (cf. [Kov86, DLR92]). In this section we give a proof of this fact without assuming that $\mathcal{G}(L)$ is unimodular or that $k = \mathcal{C}(x)$. The proof applies also to reducible polynomials, which will be fundamental to our approach.

Definition 75. Let $P \in k[u]$ and D be a derivation on $k[u]$. The polynomial P is called a Darboux polynomial for D if P divides $D(P)$ in $k[u]$.

Using the following two derivations on $k[u]$:

$$\begin{aligned}\partial_k\left(\sum_{i=0}^{m} b_i u^i\right) &= \sum_{i=0}^{m} \delta(b_i) u^i \\ \frac{\partial}{\partial u}\left(\sum_{i=0}^{m} b_i u^i\right) &= \sum_{i=0}^{m} i b_i u^{i-1}\end{aligned}$$

We define a new derivation $\mathcal{D}_{L,k}$ on $k[u]$ by:

$$\mathcal{D}_{L,k}\left(P(u)\right) = \partial_k\left(P(u)\right) - (a_0 + a_1 u + u^2)\frac{\partial}{\partial u}\left(P(u)\right)$$

A differential extension $k\{u\}$ of k by a differential variable u is obtained by adjoining to k a variable u and new variables u_i for the i-th derivative of u. A derivation Δ on $k\{u\}$ is defined by $\Delta(a) = \delta(a)$ for $a \in k$ and $\Delta(u) = u_1$, $\Delta^2(u) = u_2, \ldots$. The derivative of a polynomial $P(u) = \sum_{i=0}^{m} b_i u^i \in k[u] \subset k\{u\}$ by Δ is:

$$\begin{aligned}\Delta\left(P(u)\right) &= \partial_k\left(P(u)\right) + u'\frac{\partial P}{\partial u}(u) \\ &= \partial_k\left(P(u)\right) - (a_0 + a_1 u + u^2)\frac{\partial P}{\partial u}(u) + \left(u' + u^2 + a_0 + a_1 u\right)\frac{\partial P}{\partial u}(u) \\ &= \mathcal{D}_{L,k}\left(P(u)\right) + Ri(u)\cdot\frac{\partial P}{\partial u}(u)\end{aligned}$$

Lemma 76. *All zeroes of $P \in k[u]$ are solutions of the Ricatti equation if and only if P is Darboux for $\mathcal{D}_{L,k}$.*

Proof. - Suppose that P is Darboux and pick any irreducible factor P_1 which must again be Darboux (Lemma 12). Since P_1 divides $\mathcal{D}_{L,k}(P_1)$, we have that $P_1 = 0$ implies $\mathcal{D}_{L,k}(P_1) = 0$. Since P_1 is prime, it can not divide $\frac{\partial}{\partial u}\left(P_1\right)$. From

$$\Delta\left(P_1(u)\right) = \mathcal{D}_{L,k}\left(P_1\right)(u) + Ri(u)\cdot\left(\frac{\partial}{\partial u}P_1\right)(u), \tag{2.1}$$

we finally get that if $P_1(u) = 0$, then $Ri(u) = 0$. Since any zero of P is a zero of an irreducible factor, the result follows.
Conversely, suppose that all zeroes of $P(u)$ are zeroes of $Ri(u)$. Pick an irreducible factor $P_1(u)$ of $P(u)$; then, reasoning as above, we get from (2.1) that, since $Ri(u) = 0$, all zeroes of P_1 are zeroes of $\mathcal{D}_{L,k}(P_1)$ and thus that P_1 is Darboux. Since all irreducible factors of $P(u)$ are Darboux for $\mathcal{D}_{L,k}$, $P(u)$ is Darboux for $\mathcal{D}_{L,k}$ (Lemma 12). □

A polynomial $P(u) = u^m + b_{m-1}u^{m-1} + \ldots + b_0$ is Darboux if and only if $\mathcal{D}_{L,k}\left(P(u)\right)$ is divisible by $P(u)$. Performing the division and setting the remainder equal to 0 gives the following system $(\sharp)_m$ for the coefficients b_i:

$$\begin{cases} b_m = 1 \\ b_{i-1} = \dfrac{-b_i' + b_{m-1}b_i + a_1(i-m)b_i + a_0(i+1)b_{i+1}}{m-i+1}, \quad m-1 \geq i \geq 0 \\ b_{-1} = 0 \end{cases} \tag{2.2}$$

Note that $P(u)$ is Darboux if and only its coefficients b_i satisfy the above system. The last equation $b_{-1} = 0$ plays a central role in [Kov86] but is almost not used in our proofs. From the form of the system we see that the coefficients b_i are all determined from the knowledge of the coefficient b_{m-1}. A Darboux polynomial is thus uniquely determined by its degree m and by its coefficient b_{m-1}: we may say that such a b_{m-1} solves the system $(\sharp)_m$. Note that, if $P_1 = u^m + b_{m-1}u^{m-1} + \ldots$ and $P_2 = u^n + \beta_{n-1}u^{n-1} + \ldots$ are Darboux, then $P_1P_2 = u^{m+n} + (b_{m-1} + \beta_{n-1})u^{m+n-1} + \ldots$ is also Darboux and so $b_{m-1} + \beta_{n-1}$ solves the system $(\sharp)_{n+m}$. Our next step is to characterize the elements b_{m-1} of k which solve the system $(\sharp)_m$ and thus give a Darboux polynomial of degree m.

Theorem 77. *Let $L(y) = y'' + a_1y' + a_0y$ be a second order equation with $a_i \in k$, then all zeroes of $P(u) = u^m + \sum_{i=0}^{m-1} b_iu^i$ with $b_i \in k$ are solutions of the Riccati equation $Ri(u) = 0$ if and only if b_{m-1} is the negative logarithmic derivative of an exponential solution (over k) of $L^{\circledS m}(y) = 0$, i.e. b_{m-1} is the negative logarithmic derivative of a semi-invariant of $\mathcal{G}(L) \subseteq GL(2, \mathcal{C})$.*

Proof. - Suppose that $P(u) \in k[u]$ is Darboux. From Lemma 76 we get that all zeroes of $P(u) = 0$ are solutions of $Ri(u) = 0$. From relation (1.4) we get that b_{m-1} is an exponential solution of $L^{\circledS m}(y) = 0$.
We now show that any exponential solution z of a $L^{\circledS m}(y) = 0$ yields a Darboux polynomial of degree m. Consider the polynomial $P(u) = u^m + \sum_{i=0}^{m-1} b_iu^i$, where $b_{m-1} = z'/z$ and where the other coefficients $b_{m-2}, \ldots, b_0$ are given according to the recursion $(\sharp)_m$. Since $b_{m-1} \in k$, all b_i will also be in k and thus $P(u) \in k[u]$. Let y_1, y_2 be a fundamental system of solutions of $L(y) = 0$ and (K, Δ) be a PVE of (k, δ) for $L(y) = 0$. Since z is a semi-invariant of degree m of $\mathcal{G}(L)$, it can be written as a homogeneous form $z = F(y_1, y_2)$ of degree m in y_1, y_2 over $\mathcal{C}$. As $\mathcal{C}$ is algebraically closed, $F(y_1, y_2)$ can be factored over K as a product of m linear forms: $F(y_1, y_2) = \prod_{i=1}^{m}(\beta_iy_1 - \alpha_iy_2)$ with $\beta_i, \alpha_i \in \mathcal{C}$. We note that $u_i = \Delta(\beta_iy_1 - \alpha_iy_2)/(\beta_iy_1 - \alpha_iy_2)$ is a solution of $Ri(u) = 0$. Thus all zeros of the polynomial $Q(u) = \prod_{i=1}^{m}(u - u_i) \in K[u]$ are solutions of $Ri(u) = 0$. The polynomial $Q(u) = 0$ must be Darboux for $\mathcal{D}_{L,K}$ (Lemma 76) and its coefficients must satisfy $(\sharp)_m$. In particular, since $z'/z = b_{m-1} = \prod_{i=1}^{m} u_i$, the coefficients of $Q(u) = 0$ are in k. Since $P(u)$ and $Q(u)$ are of the same degree and are both constructed from z'/z and $(\sharp)_m$, we have $P(u) = Q(u)$. The polynomial $P(u) = Q(u)$ is Darboux for $\mathcal{D}_{L,K}$ and has coefficients in k. By Lemma 14, $P(u)$ is also Darboux for $\mathcal{D}_{L,k}$. From Lemma 76 we get that all roots of $P(u) = 0$ are solutions of $Ri(u) = 0$. □

This gives a bijection between monic polynomials of degree m over k whose roots are solutions of the Riccati equation and exponential solutions of $L^{\circledS m}(y) = 0$, i.e. semi-invariants of degree m of $\mathcal{G}(L)$. In particular, if z_1 and z_2 are two semi-invariants, then the Darboux polynomial associated with the product $z_1 z_2$ is the product of the Darboux polynomials associated with z_1 and z_2 respectively. In the sequel, we will use this remark without further mention.

For higher order linear differential equations, the minimum polynomial of an algebraic solution of the Riccati equation is no longer Darboux, and the bijection does not exist any more.

3. The algorithm for second order equations

In this section, we will always assume that $L(y)$ is a second order equation with $\mathcal{G}(L) \subseteq SL(2, \mathcal{C})$. The previous section shows that there is a bijection between exponential solutions of $L^{\circledS m}(y) = 0$ and polynomials of degree m whose zeroes are solutions of the Riccati. We now propose an algorithm where rational solutions of $L^{\circledS m}(y) = 0$ are used as much as possible instead of exponential solutions.

The proposed algorithm can be outlined as follows:

1 Test if $L(y)$ has a non-trivial rational (and thus Liouvillian) solution.
2 Test if $L^{\circledS 2}$ has a non-trivial rational solution. If it is the case, then $\mathcal{G}(L)$ is a reducible subgroup of $SL(2, \mathcal{C})$.
   (a) If the space of rational solutions of $L^{\circledS 2}$ is of dimension 3, then $\mathcal{G}(L) = \{id, -id\}$ and any Darboux polynomial $P(u)$ of degree 2 associated to a non-trivial rational solution of $L^{\circledS 2}$ is reducible. A factor of $P(u)$ gives a Liouvillian solution.
   (b) If the previous case does not hold, then $\mathcal{G}(L)$ is a completely reducible group if and only if the Darboux polynomial $P(u)$ of degree 2 associated to a non-trivial rational solution of $L^{\circledS 2}$ factors but is not a square. The two factors of $P(u)$ give two exponential solutions.
   (c) If the above cases do not hold, then the Darboux polynomial $P(u)$ of degree 2 associated to a non-trivial rational solution of $L^{\circledS 2}$ is either a square or is irreducible. In both cases a Liouvillian solution is found.
3 Test if $L(y) = 0$ has a non trivial exponential (and thus Liouvillian) solution. Such a solution must then be unique and gives a right factor of order one of $L(y)$.
4 Test if $L^{\circledS 4}$ has non-trivial rational solutions. The Darboux polynomial $P(u)$ associated to an arbitrary non-trivial rational solution of $L^{\circledS 4}$ is either the square of an irreducible Darboux polynomial of order 2 or is irreducible.
5 Test for increasing $m \in \{6, 8, 12\}$ if $L^{\circledS m}$ has a non trivial rational solution. The corresponding Darboux polynomial will be irreducible.

6 Conclude that $L(y) = 0$ has no Liouvillian solution.

The steps have to be performed in the given order and the algorithm terminates as soon as a solution is found in one of the cases. The third step is the only one where instead of some rational solution one has to compute an exponential solution of $L(y)$ (which is however known to be unique in this case). We note that it is not difficult to test if a Darboux polynomial $P(u)$, known to be either irreducible or a square, is a square. This is the case if and only if $Q(u) = GCD\left(P(u), \frac{d}{du}P(u)\right)$ is not constant in u, in which case, under the given assumption, $(Q(u))^2 = P(u)$

In the remainder of this section we prove that the proposed algorithm is correct and compute examples in each case.

3.1. The reducible case

If $L(y) = 0$ has a non-trivial rational solution, then this is a Liouvillian solution of $L(y) = 0$ (cf. [SUl93b] Proposition 4.2 for a description of the reducible Galois groups in this case).

Lemma 78. *Let $L(y)$ be a second order equation with $\mathcal{G}(L) \subseteq SL(2,\mathcal{C})$ having no non-trivial rational solutions. If $L^{\circledS 2}(y) = 0$ has a non-trivial rational solution, then $\mathcal{G}(L)$ is a reducible subgroup of $SL(2,\mathcal{C})$.*

1 *If the space of rational solutions of $L^{\circledS 2}$ is of dimension 3, then $\mathcal{G}(L) = \{id, -id\}$ and any Darboux polynomial $P(u)$ associated to a non-trivial rational solution of $L^{\circledS 2}$ factors.*
2 *If the previous case does not hold, then $\mathcal{G}(L)$ is a completely reducible group if and only if the Darboux polynomial $P(u)$ associated to a non-trivial rational solution of $L^{\circledS 2}$ factors but is not a square. The two factors of $P(u)$ give two exponential solutions which are linearly independent over $\mathcal{C}$.*
3 *If the above cases do not hold, then the Darboux polynomial $P(u)$ associated to a non-trivial rational solution of $L^{\circledS 2}$ is either a square or is irreducible. In both cases a Liouvillian solution is found.*

Proof. - We first note that if $\mathcal{G}(L) \subseteq SL(2,\mathcal{C})$ is irreducible (i.e. primitive or imprimitive), then $L^{\circledS 2}$ has no non-trivial rational solution because there is no invariant of degree 2 in those cases (cf. proofs of Lemmas 79 and 80). Thus, if $L^{\circledS 2}(y) = 0$ has a non-trivial rational solution, then $\mathcal{G}(L) \subseteq SL(2,\mathcal{C})$ is reducible.
Assume that $\mathcal{G}(L)$ is completely reducible. For a basis denoted $\{y_1, y_2\}$ all elements g of

$\mathcal{G}(L)$ must be of the form $g = \begin{pmatrix} a_g & 0 \\ 0 & a_g^{-1} \end{pmatrix}$. In particular y_1 and y_2 are semi-invariants and $y_1 y_2$ is an invariant of $\mathcal{G}(L)$.

1 If $\mathcal{G}(L)$ has another linearly independent invariant of degree two, say $F(y_1, y_2) = \alpha(y_1)^2 + \beta(y_2)^2$. Then, for $g \in \mathcal{G}(L)$, we have $g \cdot F(y_1, y_2) = a_g^2 \alpha(y_1)^2 + a_g^{-2} \beta(y_2)^2$. Thus $\forall g \in \mathcal{G}(L)$, $a_g^2 = 1$. Thus $\mathcal{G}(L) = \{id, -id\}$. In this case any homogeneous form of degree 2 is invariant and $L^{\circledS 2}(y) = 0$ has a rational solution space of dimension 3. Any solution of $L(y) = 0$ is an exponential solution and thus any polynomial $P(u)$ factors into two linear polynomials.

2 If $\mathcal{G}(L)$ has no other linearly independent invariant of degree two, then any rational solution of $L^{\circledS 2}(y) = 0$ is a multiple of $y_1 y_2$ and factors. The polynomial $P(u)$ associated to a non-trivial rational solution of $L^{\circledS 2}(y) = 0$ will be the product of the distinct minimal polynomials associated to the semi-invariants y_1 and y_2. In particular, $P(u)$ is not a square.

Suppose that $P(u)$ factors but is not a square, then each factor is a Darboux polynomial of order one corresponding to a different logarithmic derivative z_1'/z_1 and z_2'/z_2. The corresponding solutions z_1 and z_2 must be linearly independent over $\mathcal{C}$. In the basis $\{z_1, z_2\}$, the group $\mathcal{G}(L)$ is diagonal and thus completely reducible.
The only case left is that $P(u)$ is a square or is irreducible over $k[u]$. In this case, by the above, $\mathcal{G}(L)$ cannot be completely reducible. □

Remark. - The fact that factorization of differential operators is easier in the completely reducible case is used by Singer in [Sin94]. ◇

An example of a completely reducible group is the example given in Section 1.2 which we now summarize:

Example. - Let $L(y) = y'' + \dfrac{3}{16x^2} y$. This equation has no non-trivial rational solution, and the equation $L^{\circledS 2}(y) = 0$ has a one dimensional space of rational solutions generated by x. Thus $\mathcal{G}(L) \subseteq SL(2, \mathcal{C})$ is a reducible group and $L(y) = 0$ factors. Since the rational solution space of $L^{\circledS 2}(y) = 0$ is not of dimension 3, we have $\mathcal{G}(L) \neq \{id, -id\}$. The Darboux polynomial obtained from the logarithmic derivative $1/x$ of x is

$$u^2 - \frac{1}{x} u + \frac{3}{16x^2}$$

which factors into $\left(u - \frac{1}{4x}\right)\left(u - \frac{3}{4x}\right)$. Since $P(u)$ is not a square, $\mathcal{G}(L) \subseteq SL(2, \mathcal{C})$ is a completely reducible group. From the factorisation of $P(u)$ we get the following two Liouvillian solutions of $L(y) = 0$:

$$y_1 = e^{\int \frac{1}{4x}} \quad , \quad y_2 = e^{\int \frac{3}{4x}}$$

The equation $L(y) = 0$ is the least common left multiple of $y' - \frac{1}{4x}y$ and $y' - \frac{3}{4x}y$. $\diamond$

In the following example, we deal with a reducible but not completely reducible linear group:

Example. - Consider $L(y) = y'' + \left(\frac{3}{16\,x^2} + \frac{1}{4\,(x-1)^2} - \frac{1}{4\,x\,(x-1)}\right) y$. The equation $L^{\circledS 2}(y) = 0$ has no non-trivial rational solution and thus $\mathcal{G}(L) \subseteq SL(2,\mathcal{C})$ has no invariant of degree 2. In this case the exponential solution $e^{\int \frac{3x-1}{4x(x-1)}}$ is a semi-invariant of degree one, but there exists no other linearly independent semi-invariant of degree one. We thus get a unique polynomial $P(u) = u - \frac{3x-1}{4x(x-1)}$ of degree one. The group $\mathcal{G}(L) \subseteq SL(2,\mathcal{C})$ is reducible but not completely reducible.
We note that even if no invariant of degree two exists, there could exists other invariants of higher degree. In this example $L^{\circledS 4}$ has a one-dimensional rational solution space generated by $x\,(x-1)^2$.
The example shows that, even if no invariant of degree 2 exists, the equation $L(y)$ could be reducible, and that in order to proceed in the algorithm, one must look for exponential solutions of $L(y) = 0$ at this stage. $\diamond$

3.2. The imprimitive case

In this case we show that the computation of a Liouvillian solution of a second order equation $L(y) = 0$ is reduced to the computation of a rational solution of $L^{\circledS 4}(y) = 0$ and that the Darboux polynomial associated to the logarithmic derivative is either a square or irreducible. In this section we need to assume that $L(y) = 0$ is an irreducible equation.

Lemma 79. *Let $L(y) = 0$ be an irreducible second order equation over K whose Galois group $\mathcal{G}(L)$ is unimodular. Then $\mathcal{G}(L)$ is an imprimitive subgroup of $SL(2,\mathcal{C})$ if and only if $L^{\circledS 4}$ has a rational solution q. The Darboux polynomial obtained from the logarithmic derivative of q is then*

1 *The square of a unique Darboux polynomial of degree 2 if $L^{\circledS 4}$ has a one dimensional rational solution space.*

2 *Either the square of a Darboux polynomial of degree 2 or is irreducible if $L^{\circledS 4}$ has a two dimensional rational solution space, in which case $\mathcal{G}(L) \cong D_2^{SL_2}$.*

Proof. - Denote $\{y_1, y_2\}$ a basis in which all $g \in \mathcal{G}(L) \subseteq SL(2,\mathcal{C})$ are simultaneously in the form $\begin{pmatrix} a_g & 0 \\ 0 & a_g^{-1} \end{pmatrix}$ or $\begin{pmatrix} 0 & -a_g \\ a_g^{-1} & 0 \end{pmatrix}$ (cf. Section 1.3). Since $\forall g \in \mathcal{G}(L)$ we have $g(y_1y_2) = \pm y_1y_2$, we get that y_1y_2 is a semi-invariant of degree 2 and that $y_1^2y_2^2$ is an invariant of degree 4 of $\mathcal{G}(L)$. Since $L^{\circledS 4}(y) = 0$ has no rational solution if $\mathcal{G}(L)$ is primitive subgroup of $SL(2,\mathcal{C})$ (cf. character decompositions of the finite primitive groups in the next subsection and [Spr77] for $SL(2,\mathcal{C})$), we get the first assertion (this result is also proven in [SUl93b] Theorem 4.1 or [Kov86] p.20).
If the space of rational solutions of $L^{\circledS 4}$ is one dimensional then, up to a constant multiple, this rational solution is the square of y_1y_2. Thus, the (unique) Darboux polynomial corresponding to the (unique) logarithmic derivative of a rational solution $y_1^2y_2^2$ of $L^{\circledS 4}$ will be the square of the Darboux polynomial associated with the semi-invariant y_1y_2. Note that the Darboux polynomial associated with y_1y_2 must be irreducible, since $\mathcal{G}(L)$ is irreducible and thus has no semi-invariants of degree 1. Since for second order equations there is a bijection between rational solutions and invariants and we now look at the ring of invariants to see if the $\mathcal{C}$-subspace of invariants of degree 4 is of dimension 1. The ring of invariants of $D_n^{SL_2}$ is generated by (cf. [Spr77], p. 95)

$$I_1 = y_1^2y_2^2, I_2 = y_1^{2n} + (-1)^n y_2^{2n}, I_3 = y_1y_2(y_1^{2n} - (-1)^n y_2^{2n})$$

The group D_∞ has up to scalar multiples only one invariant $y_1^2y_2^2$ of degree 4. To see this one looks at the diagonal subgroup and, as in the proof of Lemma 78, shows that this diagonal subgroup would be of order at most 2 making D_∞ finite, a contradiction. Thus the group $D_2^{SL_2}$ is the only imprimitive group for which the space of rational solutions of $L^{\circledS 4}$ is of dimension 2 and not 1.
The group $D_2^{SL_2}$ has 5 irreducible characters, the trivial one denoted $\mathbf{1}$, 3 characters $\zeta_{1,1}$, $\zeta_{1,2}$, $\zeta_{1,3}$ of degree one and one character ζ_2 of degree two. The non trivial characters of degree one have the property that the product $\zeta_{1,i}\zeta_{1,j}$ is $\mathbf{1}$ for $i = j$ and different from $\mathbf{1}$ otherwise. If a second order equation $L(y) = 0$ has Galois group $\mathcal{G}(L) \cong D_2^{SL_2}$, then the corresponding character of $\mathcal{G}(L)$ will be ζ_2. The character χ_m of $\mathcal{G}(L^{\circledS m})$ can be computed according to the formula given in [SUl93b] p. 15:

$$\chi_2 = \zeta_{1,1} + \zeta_{1,2} + \zeta_{1,3}, \qquad \chi_3 = 2\zeta_2, \qquad \chi_4 = 2 \cdot \mathbf{1} + \zeta_{1,1} + \zeta_{1,2} + \zeta_{1,3}$$

this shows that there are 3 semi invariants S_i associated to the characters $\zeta_{1,i}$ ($i \in \{1,2,3\}$) whose squares are rational. The products S_1S_2, S_1S_3 and S_2S_3 are not invariants (i.e. do not correspond to a rational solution) since the products of the associated characters are not the trivial character. Thus a rational solution is either the square of a semi-invariant S_i of order 2, in which case the associated Darboux polynomial will be a square, or it is not the product of semi-invariants and the associated Darboux polynomial will be irreducible. □

Example. - Consider the irreducible equation

$$L(y) = y'' - \frac{2}{2x-1}y' + \frac{(27x^4 - 54x^3 + 5x^2 + 22x + 27)(2x-1)^2}{144x^2(x-1)^2(x^2-x-1)^2}y = 0.$$

It is unimodular because $\frac{2}{2x-1}$ is the logarithmic derivative of $2x-1$. The equation $L^{\circledS 4}(y) = 0$ has a one dimensional space of rational solutions generated by $-x(x-1)\left(x^2-x-1\right)^2$. The Darboux polynomial associated with the logarithmic derivative $\dfrac{(2x-1)\left(3x^2-3x-1\right)}{\left(x^2-x-1\right)(x-1)x}$ is

$$\begin{aligned}
&u^4 - \frac{(2x-1)\left(3x^2-3x-1\right)}{\left(x^2-x-1\right)(x-1)x}\,u^3 \\
&+\frac{(2x-1)^2\left(243x^4-486x^3+77x^2+166x+27\right)}{72x^2(x-1)^2\left(x^2-x-1\right)^2}\,u^2 \\
&-\frac{\left(81x^4-162x^3+23x^2+58x+9\right)(2x-1)^3\left(3x^2-3x-1\right)}{144x^3(x-1)^3\left(x^2-x-1\right)^3}\,u \\
&+\frac{\left(81x^4-162x^3+23x^2+58x+9\right)^2(2x-1)^4}{20736x^4(x-1)^4\left(x^2-x-1\right)^4}
\end{aligned}$$

which is the square of:

$$u^2 - \frac{(2x-1)\left(3x^2-3x-1\right)}{2x(x-1)\left(x^2-x-1\right)}\,u + \frac{\left(81x^4-162x^3+23x^2+58x+9\right)(2x-1)^2}{144x^2(x-1)^2\left(x^2-x-1\right)^2}$$

Since $L^{\circledS 6}$ also has a rational solution $x^2(x-1)^2\left(x^2-x-1\right)^2$, we get from the above proof that $\mathcal{G}(L)$ is $D_3^{SL_2}$ $\diamond$

The next example has a Galois group $\mathcal{G}(L) \cong D_2^{SL_2}$

Example. - Consider the irreducible equation

$$L(y) = y'' - \frac{2}{2x-1}y' + \frac{3(2x-1)^2\left(x^4-2x^3+x+1\right)}{16x^2(x-1)^2\left(x^2-x-1\right)^2}y$$

The fourth symmetric power has a two dimensional rational solution space generated by $J_0 = x(x-1)\left(x^2-x-1\right)$ and $J_1 = -x(x-1)\left(x^2-x+1\right)\left(x^2-x-1\right)$. Thus, $\mathcal{G}(L)$ is the quaternion group and we get the following two Darboux polynomials:

$$\begin{aligned}
&u^4 - \frac{(2x-1)\left(2x^2-2x-1\right)}{x(x-1)\left(x^2-x-1\right)}\,u^3 + \frac{(2x-1)^2\left(11x^4-22x^3+11x+3\right)}{8x^2(x-1)^2\left(x^2-x-1\right)^2}\,u^2 \\
&-\frac{(2x-1)^3\left(2x^2-2x-1\right)\left(3x^4-6x^3+3x+1\right)}{16x^3(x-1)^3\left(x^2-x-1\right)^3}\,u \\
&+\frac{\left(3x^4-6x^3+3x+1\right)^2(2x-1)^4}{256x^4(x-1)^4\left(x^2-x-1\right)^4}
\end{aligned}$$

and

$$u^4 - \frac{(2x-1)\left(3x^4-6x^3+3x^2-1\right)}{x(x-1)\left(x^2-x+1\right)\left(x^2-x-1\right)}\,u^3$$

$$+\frac{3(2x-1)^2\left(9x^6-27x^5+19x^4+7x^3-8x^2+1\right)}{8x^2(x-1)^2\left(x^2-x-1\right)^2\left(x^2-x+1\right)}u^2$$
$$-\frac{(2x-1)^3\left(27x^8-108x^7+117x^6+27x^5-86x^4+x^3+21x^2+x-1\right)}{16x^3(x-1)^3\left(x^2-x-1\right)^3\left(x^2-x+1\right)}u$$
$$+\frac{(2x-1)^4\left(81x^{10}-405x^9+621x^8-54x^7-572x^6+204x^5+231x^4-55x^3-48x^2-3x+1\right)}{256x^4(x-1)^4\left(x^2-x-1\right)^4\left(x^2-x+1\right)}$$

From the theorem, we know that each polynomial is either a square or is irreducible. In this example, the first polynomial is a square and the second is irreducible. ⋄

3.3. The primitive case

The following shows that for the primitive case it is always possible to look only for rational solutions of symmetric powers. However the algebraic solution of the Riccati found this way will not be of lowest algebraic degree for $A_4^{SL_2}$.

Lemma 80. *Let $L(y)=0$ be a second order equation whose differential Galois group G is a finite primitive subgroup of $SL(2,\mathcal{C})$.*

If $G\cong A_4^{SL_2}$, then the unique Darboux polynomial obtained from the logarithmic derivative of a non-trivial rational solution of $L^{\circledS 6}$ is irreducible.

If $G\cong S_4^{SL_2}$, then the unique Darboux polynomial obtained from the logarithmic derivative of a non-trivial rational solution of $L^{\circledS 8}$ is irreducible. Also the unique Darboux polynomial obtained from the logarithmic derivative of a non-trivial rational solution of $L^{\circledS 12}$ is the square of a unique Darboux polynomial of degree 6.

If $G\cong A_5^{SL_2}$, then the unique Darboux polynomial obtained from the logarithmic derivative of a non-trivial rational solution of $L^{\circledS 12}$ is irreducible.

In all cases, it is the Darboux polynomial of lowest order one can construct using rational *solutions of symmetric powers of $L(y)$.*

Proof. - The (abstract) group $A_4^{SL_2}$ has seven irreducible characters, the trivial one denoted **1**, two characters $\zeta_{1,1}$ and $\zeta_{1,2}$ of degree 1, two characters $\zeta_{2,1}$ and $\zeta_{2,2}$ of degree 2 (where the trace of an element of order 3 is different from one and thus the representation is not in $SL(2,\mathcal{C})$), another character ζ_2 of degree two (corresponding to a representation in $SL(2,\mathcal{C})$) and a character ζ_3 of degree 3. If a second order equation $L(y)=0$ has Galois group $\mathcal{G}(L)\cong A_4^{SL_2}$, then the corresponding character of $\mathcal{G}(L)$ will be $\chi=\zeta_2$. The character

χ_m of $\mathcal{G}(L^{\circledS m})$ can be computed according to the formula given in [SUl93b] p. 15:

$$\begin{array}{lll} \chi_2 = \zeta_3 & \chi_4 = \zeta_{1,1} + \zeta_{1,2} + \zeta_3 & \chi_6 = \mathbf{1} + 2\zeta_3 \\ \chi_3 = \zeta_{2,1} + \zeta_{2,2} & \chi_5 = \zeta_{2,1} + \zeta_{2,2} + \zeta_2 & \end{array}$$

Since there are no semi-invariants of degree 2 or 3, the unique Darboux polynomial obtained from the logarithmic derivative of a rational solution of $L^{\circledS 6}$ cannot be the product of Darboux polynomials of lower order.
The proof in the other cases are similar and can be deduced from the decompositions that follow:

The (abstract) group $S_4^{SL_2}$ has eight irreducible characters, the trivial one $\mathbf{1}$, another characters $\zeta_{1,1}$ of degree 1, one characters ζ_2 of degree 2 which is not faithful, two (conjugated) character $\zeta_{2,0}$ and $\zeta_{2,1}$ of degree 2 (corresponding to representations in $SL(2,\mathcal{C})$), two character $\zeta_{3,1}$ and $\zeta_{3,2}$ of degree 3 and a character ζ_4 of degree 4. For $\zeta_{2,i}$ we set $j \equiv i+1 \pmod 2$ and get:

$$\begin{array}{lll} \chi_2 = \zeta_{3,1} & \chi_5 = \zeta_{2,j} + \zeta_4 & \chi_8 = \mathbf{1} + \zeta_2 + \zeta_{3,1} + \zeta_{3,2} \\ \chi_3 = \zeta_4 & \chi_6 = \zeta_{1,1} + \zeta_{3,1} + \zeta_{3,2} & \chi_{12} = \mathbf{1} + \zeta_{1,1} + \zeta_2 + \zeta_{3,1} + 2\zeta_{3,2} \\ \chi_4 = \zeta_2 + \zeta_{3,2} & \chi_7 = \zeta_{2,i} + \zeta_{2,j} + \zeta_4 & \end{array}$$

In the above case we note that the character χ_{12} as a unique trivial summand and thus that $L^{\circledS 12}(y) = 0$ has a one dimensional rational solution space and thus that (up to multiples) there is a unique invariant of degree 12. But this invariant must be the square of the semi-invariant of degree 6 since the one dimensional character $\zeta_{1,1}$ is of order 2. The Darboux polynomial associated to the invariant of degree 12 must be the square of the unique Darboux polynomial of degree 6.
The (abstract) group $A_5^{SL_2}$ has 9 irreducible characters, the trivial one $\mathbf{1}$, two (conjugated) character $\zeta_{2,0}$ and $\zeta_{2,1}$ of degree 2 (corresponding to two representations in $SL(2,\mathcal{C})$), two character $\zeta_{3,1}$ and $\zeta_{3,2}$ of degree 3, two character $\zeta_{4,1}$ and $\zeta_{4,2}$ of degree 4, a character ζ_5 of degree 5 and a character ζ_6 of degree 6. For $\zeta_{2,i}$ we set $j \equiv i+1 \pmod 2$ and get:

$$\begin{array}{lll} \chi_2 = \zeta_{3,i} & \chi_6 = \zeta_{3,j} + \zeta_{4,2} & \chi_{10} = \zeta_{3,1} + \zeta_{3,2} + \zeta_5 \\ \chi_3 = \zeta_{4,1} & \chi_7 = \zeta_{2,j} + \zeta_6 & \chi_{11} = \zeta_{2,i} + \zeta_{4,1} + \zeta_6 \\ \chi_4 = \zeta_5 & \chi_8 = \zeta_{4,2} + \zeta_5 & \chi_{12} = \mathbf{1} + \zeta_{3,i} + \zeta_{4,2} + \zeta_5 \\ \chi_5 = \zeta_6 & \chi_9 = \zeta_{4,1} + \zeta_6 & \end{array}$$

Example. - Consider the irreducible equation

$$L(y) = y'' - \left(-\frac{3}{16\,x^2} - \frac{2}{9\,(x-1)^2} + \frac{3}{16\,x\,(x-1)} \right) y$$

This equation is studied in [Kov86] p. 23, where a minimal polynomial of degree 4 of an algebraic solution of the Riccati equation is given. This minimal polynomial corresponds

to an exponential solution of $L^{\circledS 4}$ which is not rational, but which is the cube root of a rational function. The same equation is also studied in [SUl93a] p. 68 where the minimal polynomial of a solution (not of a logarithmic derivative) is computed.
Using our approach, since $L^{\circledS 4}$ has no rational solution we know that $\mathcal{G}(L)$ is a primitive subgroup of $SL(2,\mathcal{C})$. Since $L^{\circledS 6}$ has a rational solution $x^2(x-1)^2$, we get that $\mathcal{G}(L)$ is the tetrahedral group and that the Darboux polynomial associated with the logarithmic derivative $\dfrac{4x-2}{x^2-x}$ will be irreducible. This gives the following minimal polynomial for an algebraic solution of the Riccati:

$$
\begin{aligned}
&u^6 - 2\,\frac{(2\,x-1)}{x\,(x-1)}u^5 + \frac{5\,(64\,x^2-63\,x+15)}{48\,x^2\,(x-1)^2}u^4 \\
&-\frac{5\,(512\,x^3-745\,x^2+351\,x-54)}{432\,x^3\,(x-1)^3}u^3 \\
&+\frac{5\,(4096\,x^4-7840\,x^3+5485\,x^2-1674\,x+189)}{6912\,x^4\,(x-1)^4}u^2 \\
&-\frac{(3645\,x-16254\,x^2+35781\,x^3-38720\,x^4+16384\,x^5-324)}{20736\,x^5\,(x-1)}u \\
&+\frac{-29889\,x+169209\,x^2-506331\,x^3+842008\,x^4+262144\,x^6-735232\,x^5+2187}{2985984\,x^6\,(x-1)^6}
\end{aligned}
$$

$\diamond$

4. Remarks on the rationality problem

In order to use differential Galois theory and in particular the existence of a PVE for $L(y)=0$, we needed to assume that the field of constants of the coefficient field is algebraically closed of characteristic 0. This implies that even if the coefficients of $L(y)=0$ belong to $\mathbb{Q}(x)$, the coefficient of a Darboux polynomial could be in $\overline{\mathbb{Q}}(x)$ but not in $\mathbb{Q}(x)$. In [HvP93, HvP94, Ulm94], the question of which algebraic extension of the constant field is needed to represent a Darboux polynomial is studied. The following result is trivial but useful, since it connects the approach used in this chapter to the rationality problem:

Lemma 81. *Let $L(y)=0$ be a linear differential equations whose coefficients belong to a differential field $k_0 \subseteq \mathcal{C}(x)=k$. If a Darboux polynomial $P(u)$ is obtained by an invariant of degree m corresponding to a solution in k_0 of $L^{\circledS m}(y)=0$, then the coefficients of $P(u)$ are in k_0, i.e. no algebraic extension is needed to represent the coefficients of this particular Darboux polynomial $P(u)$.*

To see how to use this result we note that:

1 The coefficient of any symmetric power $L^{\circledS m}(y)$ of $L(y)$ are obtained by solving a linear system over k_0 and thus also belong to k_0.
2 An invariant of degree m is a rational solution of $L^{\circledS m}(y) = 0$. By [Br92b], Theorem 9.1 there exists a basis of the rational solution space of $L^{\circledS m}(y) = 0$ in k_0 which can be computed*.
3 If the invariant and thus b_{m-1} is in k_0, then all other coefficients of $P(u)$ obtained by the recursion $(\sharp)_m$ will also be in k_0.

In what follows we assume (e.g. using the algorithm given in [Br92b], Theorem 9.1) that all computed invariants from now on are in k_0, the smallest field containing the coefficients. Thus, if a Darboux polynomial can be computed using an invariant of some degree (i.e. a rational solution), then this Darboux polynomial has also coefficients in k_0. Our results imply that this is possible in all cases except for the non-reductive reducible subgroups $\mathcal{G}(L) \subseteq SL(2, \mathcal{C})$. For non-reductive groups, there is a unique exponential solution, and so the result of [Ulm94, HvP93, HvP94] quoted above shows that no extension of the constant field is needed to express this solution. Thus, we can always compute *one* Darboux polynomial without increasing the constant field.

4.1. The reducible case

If we are in a non completely reducible case then, as seen just above, there a unique exponential solution and its logarithmic derivative lies in k_0.

In section 3.1, we showed that the Galois group $\mathcal{G}(L) \neq \{id, -id\}$ is reducible and completely reducible if and only if it has an invariant of degree 2 such that the corresponding Darboux polynomial factors but is not a square. In that case, an algebraic extension of degree 2 of the constant field may be needed to factor the Darboux polynomial, as shows this example:

Example. - Consider $L(y) = y'' + \dfrac{7}{16x^2}y$ whose coefficients belong to $k_0 = \mathbb{Q}(x) \subset \overline{\mathbb{Q}}(x) = k$. A rational solutions of $L^{\circledS 2}$ is x and we get the Darboux polynomial

$$u^2 - \frac{1}{x}u + \frac{7}{16x^2}.$$

This Darboux polynomial is irreducible over $\mathbb{Q}(x)$, but factors over $\mathbb{Q}(\sqrt{-3})(x)$ into

$$\left(u - \frac{2 - \sqrt{-3}}{4x}\right)\left(u - \frac{2 + \sqrt{-3}}{4x}\right)$$

* If $L(y) = 0$ has coefficients in $k_0 = \mathcal{C}_0(x)$ and V is the $\mathcal{C}_0$-space of solutions of $L(y) = 0$ in k_0, then $W = \overline{\mathcal{C}}_0 \otimes_{\mathcal{C}_0} V$ is the $\overline{\mathcal{C}_0}$-space of solutions of $L(y) = 0$ in $\overline{\mathcal{C}_0}k_0$. In particular, a $\mathcal{C}_0$-basis of V will be a $\overline{\mathcal{C}_0}$-basis of W.

We get the following two Liouvillian solutions of $L(y) = 0$:

$$y_1 = e^{\int \left(\frac{2-\sqrt{-3}}{4x}\right)} \quad , \quad y_2 = e^{\int \left(\frac{2+\sqrt{-3}}{4x}\right)}$$

◇

4.2. The irreducible case

For irreducible equations $L(y) = 0$ we showed how to construct an irreducible Darboux polynomial using an invariant. So, in this case, no algebraic extension of the coefficient field is needed to represent a solution. But, for the quaternion and the tetrahedral groups, the Darboux polynomial proposed is not of minimal degree. To construct the Darboux polynomial of minimal degree, an algebraic extension of k_0 is sometime necessary. In fact, there are exactly two cases when one may need to augment the constant field; we now detail them.

4.3. The group of quaternions

If $\mathcal{G}(L) \cong D_2^{SL_2}$ (the group of quaternions), we saw that there are three irreducible Darboux polynomials of degree 2 and all the other irreducible ones of degree 4. With our approach, one can also find the polynomials of degree 2. The idea, explained through the following example, is to choose the correct linear combination of invariants in order to guarantee that the corresponding Darboux polynomial is a square.

Example. - Consider the equation $y'' + \frac{27x}{8(x^3-2)^2}y = 0$ (from [HvP94]). Applying our algorithm, we find that $\mathcal{G}(L)$ has no invariant of degree less than 4 and that $L^{⊛4}(y) = 0$ has a basis of rational solutions given by $J_1 = (x^3 - 2)$ and $J_2 = x\,(-2 + x^3)$. Thus, $\mathcal{G}(L)$ is the quaternion group and we get the following two Darboux polynomials $P_1(u)$ and $P_2(u)$:

$$u^4 - 3\frac{x^2}{x^3-2}\,u^3 + \frac{3x\,(4x^3+1)}{4\,(x^3-2)^2}\,u^2 - \frac{8x^6+13x^3-4}{8\,(x^3-2)^3}\,u + \frac{27x^2\,(-1+2x^3)}{64\,(x^3-2)^4}$$

and

$$u^4 - 2\frac{(-1+2x^3)}{(x^3-2)\,x}\,u^3 + \frac{3x\,(8x^3-7)}{4\,(x^3-2)^2}\,u^2 - \frac{16x^6-19x^3+1}{4\,(x^3-2)^3}\,u$$
$$+\frac{(4x^3-3x-2)\,(16x^6+12x^4-16x^3+9x^2-6x+4)}{64\,(x^3-2)^4\,x}$$

A simple gcd computation shows that none of these is a square, so they both provide Liouvillian solutions. We now wish to compute the Darboux polynomials of minimal degree 2 using a linear combination $J_\lambda = J_0 + \lambda J_1$ and construct the Darboux polynomial

$P_\lambda(u)$ associated with J_λ. The results of section 3.2 show that there are exactly three values of λ such that P_λ is a square (and it is irreducible otherwise). Call R_u the resultant in u of $P_\lambda(u)$ and $\frac{\partial}{\partial u}P_\lambda(u)$; then, we must have $R_u(x,\lambda) = 0$ for all x. So, we compute the gcd of all coefficients in x and obtain $(2\lambda^3+1)^2$ (in fact, the resultant was $-115964116992\,(x^3-2)^{22}\,(1+2\lambda^3)^2\,(\lambda x+1)$). Call α a solution of $2\alpha^3+1=0$. Then, P_α is necessarily a square. Actually, we have $P_\alpha = Q_\alpha^2$, where $Q_\alpha(u)$ is:

$$u^2 - \frac{(2x^2+x\alpha^2-\alpha)}{(x^2+2x\alpha^2-2\alpha)\,(x-2\alpha^2)}\,u + \frac{(4x^3-3\alpha x-2)\,(x+\alpha^2)}{4\,(x^2+2x\alpha^2-2\alpha)^2\,(x-2\alpha^2)^2}$$

Note that there are 3 conjugate solutions of $2\alpha^3+1=0$ and thus we have three minimum polynomials of degree 2 given by the above relation. The above process can be applied to any equation with a quaternion Galois group. $\diamond$

4.4. The tetrahedral group

In the finite primitive cases, Kovacic already mentioned in [Kov86] that one could get the minimum Darboux polynomials by factoring Darboux polynomials obtained from invariants of degree 12. In the tetrahedral case, there is a 2-dimensional space of invariants. Taking the same notation as in the proof of Lemma 80, one can see this from:

$$\chi_{12} \;=\; 2\cdot\mathbf{1} + \zeta_{1,1} + \zeta_{1,2} + 3\zeta_3$$

Among those invariants of degree 12, two must be the square of the two semi-invariants of degree 4, since the corresponding linear characters $\zeta_{1,1}$ and $\zeta_{1,2}$ are of order 2.
One can proceed like for the group of quaternions and look for the linear combinations of the two invariants of degree 12 whose corresponding Darboux polynomials are the cubes of one of the two Darboux polynomials of degree 4. The linear combination may require an algebraic extension of the field of constants of k_0.

5. Résolubilité par radicaux

Dans la proposition 15 page 23, nous avons vu que, si D admet un polynôme de Darboux dans $K[u]$ (où K est une extension algébrique de k), on pouvait obtenir un polynôme de Darboux à coefficients dans k mais au prix d'une augmentation du degré. On peut alors se poser la question inverse: étant donné un polynôme de Darboux à coefficients dans k, peut-on en obtenir un de degré plus petit en se plaçant sur une extension algébrique de k ? Dans cette partie, nous montrons comment les développements précédents donnent une réponse positive pour les équations de Riccati. En fait, nous allons montrer comment, pour les équations de Riccati unimodulaires du premier ordre, on peut explicitement résoudre par radicaux quand le groupe n'est pas SL_2 ou $A_5^{SL_2}$. Ces résultats illustrent les théorèmes (non effectifs) 2.6 et 2.7 p.240 de Ulmer et Calmet dans [Ulm89].

5.1. Le principe

Soit $L(y) = 0$ une équation différentielle linéaire d'ordre 2 sur k et $Ri(u) = 0$ l'équation de Riccati associée; Soit G le groupe de Galois de L, c'est à dire le groupe de Galois d'une extension de Picard-Vessiot de k pour L ; nous supposons que $G \subset SL_2$. Nous allons passer en revue les sous-groupes (algébriques) de SL_2 autres que SL_2 et $A_5^{SL_2}$ et montrer comment, pour chacun, les techniques de ce chapitre donnent très simplement une résolution par radicaux de l'équation de Riccati.

Supposons d'abord que G est le groupe octaédral $S_4^{SL_2}$. Alors, d'après le paragraphe 3.3, Ri admet des solutions algébriques et le polynôme minimal d'une solution de degré minimal est de degré 6. L'équation $L^{\circledS 6}$ admet une solution δ_1 vérifiant $\delta_1^2 \in k$. Soit $k_1 = k(\delta_1)$ et cherchons quel est le groupe de Galois G_1 de L sur k_1 (c'est à dire le groupe de Galois d'une extension de Picard-Vessiot de k_1 pour L). Comme $L^{\circledS 6}(y) = 0$ admet une solution dans k_1, le groupe peut être réductible, imprimitif, ou alors $G_1 = A_4^{SL_2}$. Si G_1 est réductible, alors Ri admet une solution dans k_1 et donc Ri admet une solution algébrique de degré 2 sur k; comme le degré minimal d'une solution algébrique est 6, c'est impossible. De même, si G_1 est imprimitif, alors Ri admet une solution algébrique de degré 2 sur k_1 donc de degré 4 sur k, ce qui est aussi impossible. Il en découle que G_1 est le groupe tétraédral $A_4^{SL_2}$ et il y a un polynôme de Darboux de degré 4 sur k_1.

Comme $G_1 = A_4^{SL_2}$, l'équation $L^{\circledS 4}(y) = 0$ a deux solutions dont le cube est dans k_1. Il existe donc δ_2 avec $\delta_2^3 \in k$ tel que $L^{\circledS 4}(y) = 0$ a deux solutions dans $k_2 = k(\delta_1, \delta_2)$. Soit G_2le groupe de Galois de L sur k_2. Si G_2 était réductible, Ri aurait une solution algébrique de degré 3 sur k_1, ce qui est impossible, donc G_2 est le groupe des quaternions.

Comme G_2 est le groupe des quaternions, l'équation $L^{\circledS 2}(y) = 0$ admet trois solutions dont le carré est dans k_2. Il existe donc δ_3 avec $\delta_3^2 \in k$ tel que $L^{\circledS 2}(y) = 0$ ait trois solutions dans $k_3 = k(\delta_1, \delta_2, \delta_3)$. Soit G_3 le groupe de Galois de L sur k_3. Alors, $G_3 = \{Id, -Id\}$ ou bien $G_3 = \{Id\}$.

Si $G_3 = \{Id, -Id\}$, alors le carré de toute solution de L (dans l'extension de Picard-Vessiot de k_3) est rationnel et il existe δ_4 tel que $k_4 = k_3(\delta_4)$ contienne une base de solutions de $L(y) = 0$. Ce processus montre la réduction par radicaux du groupe de Galois pour les groupes $S_4^{SL_2}$, $A_4^{SL_2}$, quaternions, et $\{Id, -Id\}$.

Supposons maintenant que G est imprimitif et n'est pas le groupe des quaternions. Alors, $L^{\circledS 2}$ admet une unique solution δ_1 telle que $\delta_1^2 \in k$. Soit $k_1 = k(\delta_1)$ et G_1 le groupe de Galois de L sur k_1. Comme $L^{\circledS 2}$ a une solution (unique) dans k_1, G_1 est réductible et complètement réductible; il en découle que Ri a deux solutions dans k_1.

Enfin, le groupe tétraédral $A_5^{SL_2}$ ne se réduit pas et le mieux qu'on puisse obtenir est d'exprimer les solutions en fonction des racines d'un polynôme de degré 5.

Cette étude nous donne immédiatement un algorithme simple pour résoudre les équations de Riccati du premier ordre par radicaux.

5.2. Un exemple

Soit $k = \mathbb{Q}(x)$ avec la dérivation usuelle $\frac{d}{dx}$ et l'équation différentielle

$$L(y) = \frac{d^2}{dx^2}y(x) - \left(-\frac{3}{16\,x^2} - \frac{2}{9\,(x-1)^2} + \frac{3}{16\,(x-1)\,x}\right) y(x) = 0.$$

Soit $Ri(u) = 0$ l'équation de Riccati associée. L'équation L a pour groupe de Galois $G_k(L)$ (c'est à dire son groupe de Galois sur $\overline{\mathbb{Q}}(x)$) le groupe tétraédral $A_4^{SL_2}$. Nous calculons donc le polynôme P_3 (irréductible sur k) correspondant à la solution $x^2\,(x-1)^2$ de $L^{\circledS 6}(y) = 0$, ce qui donne:

$$\begin{aligned}
&2985984\,x^6\,(x-1)^6\,U^6 - 5971968\,x^5\,(2\,x-1)\,(x-1)^5\,U^5\\
&+311040\,x^4\left(15-63\,x+64\,x^2\right)(x-1)^4\,U^4\\
&-34560\,x^3\left(512\,x^3-745\,x^2+351\,x-54\right)(x-1)^3\,U^3\\
&+2160\,x^2\left(4096\,x^4-7840\,x^3+5485\,x^2-1674\,x+189\right)(x-1)^2\,U^2\\
&-144\,x\,(x-1)\left(16384\,x^5-38720\,x^4+35781\,x^3-16254\,x^2+3645\,x-324\right)U\\
&-29889\,x-506331\,x^3+842008\,x^4-735232\,x^5+169209\,x^2+262144\,x^6+2187
\end{aligned}$$

L'équation $L^{\circledS 4}(y) = 0$ admet les deux solution (radicales) $x\,(x-1)^{4/3}$ et $x\,(x-1)^{5/3}$. Elles s'expriment toutes deux en fonction d'un zéro α du polynôme $Z^3 - x + 1$. Alors, sur $k_1 = k(\alpha)$, le polynôme P_3 se factorise en $P_3 = Q_1 R_1$ avec:

$$\begin{aligned}
Q_1 = \quad & 20736\,x^4\,(x-1)^4\,U^4\\
&-3456\,x^3\,(x-1)^3\left(16\,x-\alpha+(\alpha)^2\right)U^3\\
&+864\,(x-1)^2\,x^2\left(64\,x^2+8\,x\,(\alpha)^2-63\,x-7\,x\alpha+15+3\,\alpha-3\,(\alpha)^2\right)U^2\\
&-24\,x\,(x-1)\,(1024\,x^3-144\,x^2\alpha+192\,x^2\,(\alpha)^2-1490\,x^2+702\,x-147\,x\,(\alpha)^2\\
&+123\,x\alpha+27\,(\alpha)^2-108-27\,\alpha)\,U\\
&+4096\,x^4+1024\,x^3\,(\alpha)^2-7840\,x^3-640\,x^3\alpha-1196\,x^2\,(\alpha)^2+818\,x^2\alpha+5485x^2\\
&+450\,x\,(\alpha)^2-1674\,x-360\,x\alpha+189-54\,(\alpha)^2+54\,\alpha
\end{aligned}$$

et

$$\begin{aligned}
R_1 = \quad & 144\,x^2\,(x-1)^2\,U^2 - 24\,x\,(x-1)\left(8\,x-(\alpha)^2+\alpha-4\right)U\\
&+15-63\,x+64\,x^2-16\,x\,(\alpha)^2+6\,(\alpha)^2-6\,\alpha+14\,x\alpha
\end{aligned}$$

Poursuivant le processus, on trouve ensuite que $L^{\circledS 2}(y) = 0$ admet la solution $y = \sqrt{(\alpha+1)\,x\alpha}$, ce qui permet de casser encore le polynôme et donne une solution par radicaux de l'équation de Riccati.

6. Conclusion

Nous ne prétendons pas que l'algorithme que nous avons présenté est systématiquement meilleur ou plus rapide que celui de Kovacic. Néanmoins, le fait de travailler avec des solutions rationnelles simplifie la présentation et rend l'algorithme beaucoup plus simple à implanter.

Notre méthode n'est pas limitée au cas $k = \mathcal{C}(x)$ et est valable pour toute équation du second ordre dont le groupe de Galois est unimodulaire (i.e la forme spéciale $p(x)y'' - q(x)y(x) = 0$ qu'utilise Kovacic n'est pas nécessaire). Le fait de (presque) tout ramener à la recherche de solutions rationnelles d'équations différentielles linéaires auxiliaires nous permet de travailler avec des singularités compliquées sans avoir besoin de factoriser sur $\overline{C}$. Notre implémentation est particulièrement intéressante pour des équations avec plusieurs singularités compliquées et des groupes finis (voir les exemples page 93 et 94) que les implantations connues de l'algorithme de Kovacic ont beaucoup de mal à résoudre ; en pratique, le seul cas qui peut encore s'avérer difficile est le cas non-réductif où l'équation de Riccati admet une unique solution rationnelle.

Les conditions nécessaires que donne Kovacic peuvent être aussi utilisées dans notre approche. Des conditions similaires (parfois plus fortes) ont été données par Singer et Ulmer dans [SUl94] ; Ulmer a donné des conditions nécessaires pour le groupe des quaternions dans [Ulm94].
Dans le cas d'un groupe fini, une alternative à notre approche est d'utiliser l'algorithme de Singer et Ulmer ([SUl93b]) pour calculer le polynôme minimal d'une solution algébrique de $L(y) = 0$.

CHAPITRE IV

Annexes

Annexe 1: Implantations

Les algorithmes décrits dans les parties II et III ont été implantés dans le logiciel de calcul formel MAPLE. Nous donnons ci-dessous quelques détails sur les choix d'implantation et des exemples de sessions de calcul. Les programmes sont accessibles auprès de l'auteur, ou sur le réseau Internet à l'adresse `http://medicis.polytechnique.fr/gage/weil.html`. Nous encourageons vivement tout lecteur intéressé à les utiliser.

1.1. INTÉGRALES PREMIÈRES: LA FONCTION *lfi*

la fonction *lfi*

Pour calculer des intégrales premières de systèmes différentiels linéaires, nous avons avons vu que notre fonction *lfi* devait passer par trois phases successives:

Construire le système $S^m(A)^*$.
Convertir ce système en une équation équivalente (ou plusieurs sous-systèmes).
Calculer les solutions rationnelles ou exponentielles de cette équation et en déduire les solutions du système initial.

La première phase est très simple à implanter et s'avère très efficace ; la raison en est que cette construction est tout à fait mécanique et ne demande aucun travail de résolution ou d'élimination.

La deuxième phase est de loin la plus compliquée (en termes de temps de calcul). La solution implantée ici est d'utiliser un vecteur cyclique. L'utilisateur peut spécifier un choix de vecteur s'il a des raisons de penser qu'il sera non-cyclique : comme nous l'avons vu, cela permet de découpler le problème en deux problèmes de taille plus petite.

Pour la troisième phase, on peut utiliser les algorithmes de recherche de solutions rationnelles ou exponentielles qui sont présent (à partir de la version $V.3$ de MAPLE). Pour les solutions rationnelles, nous avons préféré utiliser l'algorithme plus récent de M. Bronstein ([ABP95]) qui a deux avantages. D'une part, il apparaît dans la construction des singularités apparentes compliquées qui n'ont pas besoin d'être prises en compte (on sait à l'avance quelles singularités étudier) et ce programme permet de spécifier les singularités à

étudier ; d'autre part, il est nettement amélioré pour le calcul de la partie polynomiale des solutions, ce qui était le point le plus long pour l'instant. Disposer d'un bon programme est crucial à ce stade car les équations produites par la phase II peuvent être gigantesques.

Notre fonction *lfi(A, m)* effectue successivement ces trois étapes. Elle prend pour argument la matrice A et le degré m des intégrales premières à chercher ; l'utilisateur peut spécifier en troisième argument un vecteur qui servira de candidat vecteur cyclique dans la deuxième phase.

On peut aussi accéder à chaque étape séparément: la construction de $S^m(A)^*$ est effectuée par la fonction *dualsympower(A, m)**. Des fonctions *cyclic(M)* et *ratsolsys(M)* convertissent un système en équation ou calculent complètement ses solutions rationnelles

Alternatives

Il existe plusieurs alternatives à la deuxième phase. Plusieurs algorithmes de découplage (qui cherchent à "casser" le système en systèmes plus petits) sont apparus récemment ; notamment, l'algorithme de [AZ95] est très élégant et s'avère très efficace. Une alternative est d'utiliser l'algorithme de Berkowitz [Abd95] ; cette méthode, quoique théoriquement intéressante, n'est pas encore très bien adaptée à notre problème. Les travaux de [GHe91] donnent à penser qu'une meilleure structure de données pourrait significativement améliorer la méthode du vecteur cyclique ; ces travaux sont pour l'instant encore très théorique et nous n'avons pas d'indications sur leurs performances pratiques. Enfin, mentionnons que M. van Hoeij et l'auteur travaillent à une méthode qui évite la difficile conversion en équation et pourrait aussi améliorer significativement la puissance de l'algorithme.

Une session MAPLE

Pour illustrer (ou pour aider un utilisateur potentiel), nous donnons ci-dessous un exemple de session MAPLE.

D'abord, on charge les fonctions autour de *lfi* et la nouvelle fonction *ratlode* de M. Bronstein pour le calcul des solutions rationnelles d'équations différentielles linéaires.

```
> read(lfi);
> read(nratlode);
```

La matrice du système $Y' = AY$:

```
> A:=matrix(3,3,[0,1,0,0,0,1,2,4*x,0]);
```

* Nous avons aussi implanté une fonction *extpower(A, m)* qui calcule des puissances extérieures

$$A := \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 4\,x & 0 \end{bmatrix} \tag{1.1}$$

On calcule $S^2(A)^*$

```
> B:=dualsympower(A,2);
```

$$B := \begin{bmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ -8\,x & 0 & -1 & -2 & 0 & 0 \\ -4 & 0 & 0 & 0 & -1 & 0 \\ 0 & -4\,x & 0 & 0 & -1 & 0 \\ 0 & -2 & -4\,x & 0 & 0 & -2 \\ 0 & 0 & -2 & 0 & 0 & 0 \end{bmatrix} \tag{1.2}$$

Pour chercher s'il y a des solutions rationnelles, on prend un vecteur cyclique et on trouve effectivement une solution rationnelle.

```
> eq1:=cyclic(B,[0,0,0,0,0,1]);
```

$$eq1 := \left(\frac{\partial^6}{\partial x^6}\,\mathrm{y}(x)\right) + 64\,x^2\,\%1 - 22\,\left(\frac{\partial^3}{\partial x^3}\,\mathrm{y}(x)\right) + 128\,x\,\left(\frac{\partial}{\partial x}\,\mathrm{y}(x)\right) - 20\,x\,\left(\frac{\partial^4}{\partial x^4}\,\mathrm{y}(x)\right) - 128\,\mathrm{y}(x)$$

$$\%1 := \frac{\partial^2}{\partial x^2}\,\mathrm{y}(x)$$

```
> inv:=solutions_rationnelles(eq1,y,x);
```

$$inv := \_C_1\,x \tag{1.3}$$

Notons que, dans ce cas, on peut tomber sur un cas dégénéré:

```
> cyclic(B,[1,0,0,0,0,0]);
```

$$\left(\frac{\partial^5}{\partial x^5}\,\mathrm{y}(x)\right) + 64\,x\,\mathrm{y}(x) + 64\,x^2\,\left(\frac{\partial}{\partial x}\,\mathrm{y}(x)\right) - 30\,\left(\frac{\partial^2}{\partial x^2}\,\mathrm{y}(x)\right) - 20\,x\,\left(\frac{\partial^3}{\partial x^3}\,\mathrm{y}(x)\right)$$

La fonction lfi fait tout ce travail. Elle prend comme arguments la matrice A du système et le degré m de l'intégrale première cherchée.

```
> t:=time():sol:=lfi(A,2);time()-t;
```

$$sol := -\frac{1}{2}\,\_C_1\,y_2\,y_0 + \frac{1}{4}\,\_C_1\,{y_1}^2 + \_C_1\,x\,{y_0}^2 \tag{1.4}$$

$$.567 \tag{1.5}$$

On vérifie que c'est bien une solution en dérivant sol modulo $Y' = AY$:

```
> vfd(A,sol);
```

$$0 \tag{1.6}$$

On peut spécifier un candidat pour le vecteur cyclique si on le souhaite. Ici, on utilise le vecteur $[1,0,0,0,0,0]$ qui est non cyclique et, comme on l'a vu dans le chapitre II, ça accélère le calcul:

```
> t:=time():sol:=lfi(A,2,[1,0,0,0,0,0]);time()-t;
```

$$sol := -2\,\_t_1\,y_2\,y_0 + \_t_1\,{y_1}^2 + 4\,x\,\_t_1\,{y_0}^2 \tag{1.7}$$

$$.417 \tag{1.8}$$

Bien sur, le choix du vecteur cyclique peut aussi influer négativement sur le temps de calcul (mais pas sur le résultat!):

```
> t:=time():sol:=lfi(A,2,[0,1,0,x-1,0,1]);time()-t;
```

$$sol := 2\,\_C_0\,y_2\,y_0 - \_C_0\,{y_1}^2 - 4\,\_C_0\,x\,{y_0}^2 \tag{1.9}$$

$$2.366 \tag{1.10}$$

1.2. Équations du second ordre: la fonction *riccati-solve*

La fonction *riccati-solve*

L'implantation des résultats tels qu'ils sont présentés dans le chapitre III est immédiate pour deux raisons. La première raison est que, du fait qu'on n'a que deux variables, le calcul de l'équation $L^{\circledS m}$ ne requiert quasiment pas d'élimination : dans la transformation par le vecteur cyclique $[1,0,\ldots]$, on peut trianguláriser la construction au fur et à mesure qu'on construit la matrice P du chapitre II (on peut même pré-calculer ces puissances symétriques, mais les expressions sont larges et il est plus rapide de les re-calculer à chaque

fois - comme il est plus rapide de re-calculer un déterminant plutôt que d'utiliser une grosse formule)*. La deuxième raison est que les coefficients d'un polynôme de Darboux satisfont une récurrence très simple qui fait que, une fois $L^{\circledS m}$ construite et résolue, on n'a plus rien à faire.

La fonction *riccati-solve* que nous avons programmée prend comme paramètres une équation différentielle du second ordre, la fonction (y dans notre texte), et la variable (x dans notre texte).

Quand on la compare avec l'implantation de l'algorithme de Kovacic qui est fournie avec MAPLE, on constate qu'elle est un peu moins rapide sur les problèmes 'faciles', et montre tout son intérêt quand il y a des singularités compliquées, des polynômes de Darboux de degré élevé, ou qu'il faut augmenter le corps des constantes pour appliquer l'algorithme original de Kovacic (dans ce cas là, il arrive même que l'implantation fournie dans MAPLE fournisse une réponse fausse après un très long calcul). Notons que, non seulement notre méthode ne nécessite pas une telle extension des constantes, mais qu'elle permet même de prédire quelle serait la constante nécessaire à ajouter pour appliquer l'algorithme original de Kovacic.

Alternatives

Un complément intéressant à ce programme est de disposer d'outils d'analyse locale autour des singularités. Ceci peut permettre par exemple, pour une équation dépendant de paramètres, de donner des conditions nécessaires (mais pas suffisantes, en général) sur ces paramètres pour qu'elle admette une solution liouvillienne.

Une session *maple*

Voyons deux exemples simples de la fonction *riccati-solve*.

```
> read(riccati_solve):
```

Un premier exemple: les cas imprimitifs dans la liste d'équations hypergéométriques de Schwartz (voir [Poole]).

```
> lambda:=1/2:
> mu:=1/2:
> nu:=1/n:
> r:=(lambda^2-1)/(4*x^2)+(nu^2-1)/(4*(x-1)^2)+(1-nu^2+mu^2-lambda^2)/(4*x*(x-1)):
> deq:=diff(y(x),x$2)-r*y(x);
```

$$deq := \left(\frac{\partial^2}{\partial x^2}\,\mathrm{y}(\,x\,)\right) - \left(-\frac{3}{16}\,\frac{1}{x^2} + \frac{1}{4}\,\frac{\frac{1}{n^2}-1}{(\,x-1\,)^2} + \frac{1}{4}\,\frac{1-\frac{1}{n^2}}{(\,x-1\,)\,x}\right)\mathrm{y}(\,x\,) \tag{1.11}$$

* Pour le calcul de $L^{\circledS m}$, il existe aussi un programme de Thom Mulders en MAPLE, réalisé dans le cas du projet européen CATHODE.

```
> P:=riccati_solve(deq,y,x);
```

$$P := \_U^2 - \frac{1}{2}\,\frac{(3\,x-1)\,\_U}{x\,(x-1)} + \frac{1}{16}\,\frac{-6\,n^2\,x+9\,n^2\,x^2+n^2-4\,x}{n^2\,x^2\,(x-1)^2} \tag{1.12}$$

Un deuxième exemple (complètement réductible).

```
> deq:=eval(subs(y(x)=y(x)*x,diff(y(x),x$2)-c/16/x^2*y(x)));
```

$$deq := \left(\frac{\partial^2}{\partial x^2}\,\mathrm{y}(x)\right)\,x + 2\,\left(\frac{\partial}{\partial x}\,\mathrm{y}(x)\right) - \frac{1}{16}\,\frac{c\,\mathrm{y}(x)}{x} \tag{1.13}$$

```
> P:=riccati_solve(deq,y,x);
riccati_solve:   two solutions    _U-1/32*(16*x-8*x*(c+4)^(1/2))/x^2   _U-1/32*(16*x+8*x*
(c+4)^(1/2))/x^2
```

$$P := \_U + \frac{1}{4}\,\frac{2+\sqrt{c+4}}{x} \tag{1.14}$$

Si maintenant on souhaite exprimer la solution "explicitement":

```
> dsolve(diff(y(x),x)-solve(P,_U)*y(x),y(x)) ;
```

$$\mathrm{y}(x) = \frac{\_C1}{\sqrt{x}\,\left(x^{\left(\sqrt{c+4}\right)}\right)^{1/4}} \tag{1.15}$$

```
> expand(eval(subs(",deq)));
```

$$0 \tag{1.16}$$

Annexe 2: Quelques résultats utiles en théorie des invariants

Dans cet appendice, nous résumons rapidement les résultats de théorie des invariants nécessaires dans la fin du chapitre II. Notre description est schématique et nous renvoyons aux articles originaux pour des descriptions complètes Il y a énormément de références générales sur la théorie des invariants, notamment [Spr77, PV94, Stu94].

Soit C un corps algébriquement clos de caractéristique 0, V un C-espace vectoriel de dimension finie n, et G un groupe algébrique linéaire réductif agissant sur V de manière fidèle et irréductible. On appelle *invariants* de G les éléments de l'algèbre symmétrique $S(V)$ qui sont laissés fixes par G; l'ensemble des invariants est noté $S(V)^G$. Nous traitons deux problèmes: déterminer de tels groupes qui n'ont pas d'invariants, et borner le degré des générateurs de l'algèbre des invariants.

2.3. Les représentations qui n'ont pas d'invariants

La référence générale pour cette partie* est [PV94]. Si G n'a pas d'invariants, sa composante connexe de l'identité n'a pas non plus d'invariants; réciproquement, si la composante connexe a un invariant alors G a un semi-invariant. Pour les problèmes traités dans le chapitre II, nous pouvons donc supposer sans perte de généralité que G est *connexe* dans cette partie.

Soit Z la composante connexe de l'identité du centre de G. Nous avons deux possibilités: $Z = \{Id\}$ ou bien Z est de dimension 1 et agit sur V par multiplication scalaire (par le lemme de Schur, cf [Spr77] page 17). Dans ce dernier cas, l'action est non-triviale (car l'action de G sur V est fidèle). Donc, Z agit sur chaque $S^m(V)$ par des multiplications scalaires et il n'y a pas d'invariants.

Nous supposons donc maintenant que $Z = \{Id\}$, c'est à dire que G est semi-simple. Dans ce cas, on trouve dans [PV94] le critère suivant: Il n'y a pas d'invariant dans l'algèbre symmétrique $S(V)$ si et seulement s'il y a une orbite ouverte Zariski-dense sous G dans V.

Ce résultat se montre de la manière suivante. Comme G est semi-simple, le corps F des invariants dans le corps des fractions de $S(V)$ est le corps des fractions de $S(V)^G$. Or, le degré de transcendance de F est égal à $\dim V - \max_{v\in V} \dim G.v$. Donc, $S(V)^G = C$ si et seulement si $\dim V = \max_{v\in V} \dim G.v$, c'est à dire s'il y a une orbite dense dans V. □

Utilisant cette caractérisation (et les résultats de [AVE67]), on peut déduire des classifications données par Elashvili dans [Ela72a] la liste des groupes* G simples réductifs connexes n'admettant pas d'invariants**

$$SL_n,\ Sp_{2n},\ Spin_{10},\ \text{et}\ \Lambda^2\left(SL_{2n+1}\right).$$

Une classification analogue pour les groupes semi-simples est donnée dans [Ela72b] (voir aussi la table à la fin de [PV94]).

2.4. Bornes et calculs d'invariants

Une référence pour cette partie est [Kem1, Kem2]. Comme G est réductif, on sait que l'algèbre des invariants est finiment engendrée (voir par exemple [Spr77, Kem1]). Le degré des générateurs est donc théoriquement borné. Pour établir un algorithme de calcul d'invariants (ou d'intégrales premières, pour ce qui nous concerne), il nous faut une borne

* Ce qui suit est transcrit (librement) d'une lettre de V. Popov

* On les identifie à des *représentations* pour pouvoir parler d'invariants

** Les symboles SL_n, SP_n désignent les groupes algébriques simples correspondant dans leur plus simple représentation, $\Lambda^2(SL_{2n+1})$ désigne la représentation de SL_{2n+1} sur le carré extérieur, et $Spin_10$ désigne un revêtement universel de SO_{10} dans la représentation semi-spinorielle.

effective. Une telle borne existe si on connaît le groupe. Pour les groupes finis, une borne a été donnée par E. Noether (voir [Stu94]). Pour les groupes connexes (semi-simples), une borne a été donnée par Popov dans [Pop79] (voir aussi [Pop83]); sur cette base, Kempf donne dans [Kem1] une borne générale pour les groupes réductifs.

Notons que ces bornes supposent qu'on ait quelque donnée sur le groupe (par exemple, son algèbre de Lie et un tore maximal dans [Pop79]); ce n'est pas le cas dans la situation que nous étudions dans la partie II. Il n'est pas clair qu'une borne uniforme (i.e dépendant seulement de n) existe en général; pour le cas où G est résoluble, une borne sur le degré *d'un* semi-invariant a été donnée par Singer dans [Sin81] et améliorée par Ulmer dans [Ulm92].

Pour ce qui nous concerne dans la partie II, le mieux qu'on puisse faire (pour l'instant) est de se ramener, pour n donné, à des classifications de sous-groupes algébriques de SL_n et appliquer les résultats ci-dessus. Notons enfin que nous ne connaissons pas (pour l'instant) de borne sur le degré d'un invariant (ou semi-invariant) de degré *minimal* (sauf pour $n = 2, 3$), ce qui en fait nous suffirait pour avoir une complète procédure de décision dans la partie II.4.

Annexe 3: Solutions d'équations différentielles linéaires

Soit k un corps différentiel ordinaire (e.g $k = \mathbb{Q}(x)$ or $k = \mathbb{C}(x)$ avec la dérivation $\frac{d}{dx}$). Cet appendice résume quelques méthodes* utilisées pour résoudre l'équation $L(y) = a_n y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_0 y = 0$ (avec a_i dans k). Il est basé sur une rédaction (par l'auteur) d'un exposé de F. Ulmer à l'INRIA (Rocquencourt, projet ALGO) le 30 mai 1994. L'essentiel du contenu de cet appendice est rappelé dans le corps du texte ; nous l'incluons comme référence pour un lecteur non familier avec la résolution algorithmique des équations différentielles linéaires.

3.5. Classes of solutions

For effectivity and simplicity, we take $k = \overline{\mathbb{Q}}(x)$ in the sequel.

Rational solutions.

A solution is *rational* if it belongs to k. For example, the equation $a_2 y'' + xy' - y = 0$ has the solution $y = x$ which is in k. Algorithms for computing such solutions have been known for a long time. The first one is due to Liouville (1833). Some faster or more general versions have been given by Abramov and Bronstein [Abr91, Br92b, ABP95], and Singer ([Sin91], for the case when k contains a wider class of functions).

* Le lecteur attentif notera que certaines de ces méthodes sont améliorées dans les chapitres II et III.

If there is no rational solution, then one must perform a field extension to find a solution. Let K be a differential field which is an extension of k, and Δ be the derivation on K (resp δ on k). We say K is a differential field extension of k if Δ and δ coincide on k.

Algebraic solutions.

A solution of L is *algebraic* if it belongs to an algebraic extension of k. In other words, there is an irreducible polynomial P with coefficients in k such that $P(y) = 0$. For example, if we define y as a zero of the polynomial $y^2 - x$, then y is a solution of $2xy' = y$. Work on characterising such solutions has been performed for example by Pépin, Klein, Jordan, Fuchs, Baldassari & Dwork, Singer (see e.g [Sin81, SUl93a, Ulm92] for further references).

Liouvillian solutions.

A solution that is not algebraic is transcendental. An interesting class of solutions corresponds to the notion of "integrability by quadratures". A solution y of L is *Liouvillian* if it belongs to a field K such that:

1 $K = K_n \supseteq \ldots \supseteq K_1 \supseteq K_0 = k$;
2 $K_i = K_{i-1}(\eta_i)$ for $i = 1, \cdots, n$ and:
   (a) η_i is algebraic over K_{i-1}, or
   (b) $\eta_i' \in K_{i-1}$ (case of an integral), or
   (c) $\eta_i'/\eta_i \in K_{i-1}$ (case of exponential of an integral).

For example, if we take $L(y) = y'' - \frac{1}{2(x+1)}y' - (x+1)y = 0$, then $\{\exp[\int \sqrt{1+x}], \exp[-\int \sqrt{1+x}]\}$ forms a basis of liouvillian solutions.

Exponential solutions.

There is a very important subclass of the liouvillian solutions: we say that a solution y is *exponential* if its logarithmic derivative is in k, i.e $y'/y \in k$. For example, the equation $y'' - (2 + 4x^2)y = 0$ has the solution $y = e^{x^2}$ $(y'/y = 2x)$. Methods for computing such solutions have been given, for example, by Singer or Bronstein [Br92b, Sin91].

3.6. Differential Galois theory

The main known tool to compute liouvillian solutions of linear differential equations is differential Galois theory. Roughly, the idea is to look at the group of transformations that

send a solution of the equation to another solution of the equation; from the knowledge of this group, one can derive algebraic properties of the solutions. We now outline this formalism.

Picard-Vessiot extensions.

To a given vector space of solutions of L, one associates a field extension the following way. Since we work in a differential context, in order to adjoin an element y to k we must also add all its derivatives. We write $k\langle y\rangle := k(y, y', y'', \cdots)$. We say that $K \supset k$ is a *Picard-Vessiot extension* if $K = k\langle y_1, \cdots, y_n\rangle$, where $\{y_1, \cdots, y_n\}$ is a basis of the solution space of $L(y) = 0$, and K and k have the same field of constants C (elements with zero-derivative).

Then, we proceed as in classical Galois theory: The *differential Galois group* of L is the set $\mathcal{G}al(L)$ of the automorphisms of K that let k point-wise fixed and that commute with the derivation (this definition does not depend on K). As in classical Galois theory, an element is in k if and only if it is left fixed by $\mathcal{G}al(L)$; also, the subfields of K appear as fixed fields of some algebraic subgroup of $\mathcal{G}al(L)$.

Galois group.

Call V the vector space of solutions of L. As G acts on V, we can decompose its action on a basis of V. The image of a solution of L is still a solution of L, so the image of an element of K is completely characterised by the images of the y_i in the basis $\{y_1, \cdots, y_n\}$. This provides a faithful matrix representation of degree n of the Galois group: $\mathcal{G}al(L)$ can be viewed as a subgroup of $GL(n, C)$ (the group of invertible $n \times n$ matrices with entries in C).

In fact, $\mathcal{G}al(L)$ is a *linear algebraic group* (its entries are solutions of a set of polynomial equations). So, its entries have a structure of an algebraic variety. In particular, there is a component of this variety in which lies the origin; we denote it by $\mathcal{G}al(L)^\circ$. A key fact is that L has a liouvillian solution if and only if $\mathcal{G}al(L)^\circ$ is solvable (Picard-Vessiot, Kolchin). In this sense, finding liouvillian solutions is the differential analog of searching for solutions by radicals in the classical case. A theorem of Lie-Kolchin on triangularization of matrix groups implies that this happens if the elements of $\mathcal{G}al(L)^\circ$ have a common eigenvector y: $\forall \sigma \in \mathcal{G}al(L)^\circ, \exists c_\sigma \in C, \sigma(y) = c_\sigma y$. As a consequence $\sigma(\frac{y'}{y}) = \frac{\sigma(y')}{\sigma(y)} = \frac{c_\sigma y'}{c_\sigma y} = \frac{y'}{y}$, which means that y'/y is in the fixed field K° of $\mathcal{G}al(L)^\circ$. This in turn implies that y'/y is algebraic over k.

Ricatti equation.

As a consequence, there exists a $u = y'/y$ that is a solution of $P(u) = u^N + b_{N-1}u^{N-1} + \cdots + b_0 = 0$ (in other words, $y = \exp[\int u]$ is a solution of $L(y) = 0$). If we let $y' = uy$, then $y^{(i)} = R_i(u, u', \cdots)y$, with $R_i = R'_{i-1} + uR_{i-1}$. Replacing in L, we get that $\sum a_i R_i(u, u', \cdots) = 0$: this is a non-linear differential equation of order $n-1$ satisfied by u, called the *Ricatti equation*. For example, if $L = y'' - ry$, then the Ricatti equation is $u' + u^2 - r = 0$.

Finding a liouvillian solution is thus reduced to finding an algebraic solution of the Ricatti equation, which again splits into two subproblems: (1) find a bound for the degree N of P; (2) given N, compute the coefficients of a polynomial P such that its zeroes are logarithmic derivatives of zeroes of L.

Problem (1) is solved by group-theoretic considerations. It follows from works of Kovacic or Singer that there is a function $f(n)$ such that $N \leq f(n)$ (e.g, $f(2) = 60, f(3) = 360, f(4) \leq 5040, f(5) \leq 25920, f(6) \leq 604800, \cdots$). Recent works of Ulmer and Singer & Ulmer show that sharp bounds are $N \leq 12$ for $n = 2$ and $N \leq 36$ for $n = 3$. We shall come back to this point later and we now focus on the actual computation of the coefficients of the polynomial P.

3.7. Computing a solution

Symmetric powers.

Suppose for a moment that we work in an algebraic closure of k. There, P has N zeroes $u_1, \cdots, u_N$, and $P(u) = \prod (u - u_i)$. Since all zeroes of P are logarithmic derivatives of solutions of $L(y) = 0$, there are N solutions y_i such that:

$$P(u) = \prod (u - \frac{y'_i}{y_i}) = u^N - (\frac{y'_1}{y_1} + \cdots + \frac{y'_N}{y_N})U^{N-1} + \cdots + \prod \frac{y'_i}{y_i}.$$

So the coefficient b_{N-1} satisfies $b_{N-1} = \frac{y'_1}{y_1} + \cdots + \frac{y'_N}{y_N} = \frac{(y_1 \cdots y_N)'}{y_1 \cdots y_N}$. For any integer m, one can construct a linear differential equation $L^{\circledS m}$, called the *m-th symmetric power of L*, whose solution space is spanned by all monomials of degree m in the $y_1, \cdots, y_n$. In particular, b_{N-1} is the logarithmic derivative of a solution of $L^{\circledS N}$: our problem is now reduced to finding exponential solutions of $L^{\circledS N}$. Similar techniques yield the other coefficients (see [Sin81, SUl93b]).

Reducible operators.

Let $D = \frac{d}{dx}$. Then, $L(y)$ can be viewed as the action of the operator $\sum a_i D^i$ on y. Such operators form a non-commutative multiplicative ring $\mathcal{D} = k[D]$ in the following

way: for $a \in k$, we have $D(ay) = aD(y) + a'y$, so the multiplication on $\mathcal{D}$ follows from the rule $Da = aD + a'$ (precisely, $\mathcal{D}$ is called an Ore ring of type "derivation"). Before searching for solutions, one should first search if L factors in $\mathcal{D}$. For example, we have $D^2 = D.D = (D + 1/x)(D - 1/x)$.

In terms of solution space, $\mathcal{G}al(L)$ has an invariant subspace of dimension m if and only if L has a factor of order m. In that case, we say that $\mathcal{G}al(L)$ (resp L) is *reducible*. Algorithms for performing such factorizations (or detecting reducibility) exist on $\mathbb{C}(x)$. The classical algorithm dates back to Beke/Schlesinger (1895, see [BrP94] for a modern version); Grigor'ev [Gri90], Singer [Sin94], or Van Hoeij [Hoe95] have recently proposed alternative methods.

Irreducible operators.

Assume that $\mathcal{G}al(L)$ is irreducible. We say that $\mathcal{G}al(L)$ is an *imprimitive group* if V is a direct sum of subspaces that are permuted transitively under the action of $\mathcal{G}al(L)$. Otherwise, it is a *primitive group*. In general, if $\mathcal{G}al(L)$ is irreducible then: either $\mathcal{G}al(L)$ is imprimitive and $\exists y$ with$[k(y'/y) : k]$ small, or $\mathcal{G}al(L)$ is primitive finite and $\exists y$ with$[k(y'/y) : k]$ big, or $\mathcal{G}al(L)$ is primitive infinite and there is no liouvillian solution. This is made precise by the following theorems.

Théorème 82 Kovacic, 1986. *Let L be of order 2 and $\mathcal{G}al(L) \subseteq SL(2, \mathbb{C})$, then:*

1 $\mathcal{G}al(L)$ is reducible, or
2 $\mathcal{G}al(L)$ is imprimitive and then $\exists y$ with$[k(y'/y) : k] = 2$, or
3 $\mathcal{G}al(L)$ is primitive and $\exists y$ with$[k(y'/y) : k] = 4, 6, 12$, or
4 $\mathcal{G}al(L) = SL(2, \mathbb{C})$ and $L(y) = 0$ has no liouvillian solution.

Théorème 83 Singer-Ulmer, 1993. *Let L be of order 3 and $\mathcal{G}al(L) \subseteq SL(3, \mathbb{C})$, then:*

1 $\mathcal{G}al(L)$ is reducible and $L = L_1(L_2)$ or
2 $\mathcal{G}al(L)$ is imprimitive and then $\exists y$ with$[k(y'/y) : k] = 3$, or
3 $\mathcal{G}al(L)$ is primitive finite and $\exists y$ with$[k(y'/y) : k] = 6, 9, 21, 36$, or
4 Else, $L(y) = 0$ has no liouvillian solutions.

Algebraic solutions of L.

In general, it is difficult to compute y from the knowledge of y'/y (Abel's problem), but one can compute y directly in the case of a known finite primitive group because y is then

algebraic. It follows that y is algebraic over $k(y'/y)$, and one can show that there is an integer m such that $y^m \in k(y'/y)$. Thus, if d is one of the possible degrees for $[k(y'/y) : k]$, the minimum polynomial of y is of the form $P(y) = y^{m.d} + a_{d-1}y^{m.(d-1)} + \cdots + a_1 y^m + a_0$. This polynomial has the same number of coefficients as the minimum polynomial of an algebraic solution of the Ricatti equation. To show that the Ricatti equation had an algebraic solution, we showed that there was a subgroup of L with a common eigenvector. Such a subgroup is called *1-reducible*. To find the group or a solution, we must therefore find a 1-reducible subgroup H of $\mathcal{G}al(L)$ of minimal index. Suppose we have found such an H and let $\mathfrak{S} = \{\sigma_1, \cdots, \sigma_d\}$ be a system of representatives of $\mathcal{G}al(L)/H$. If y_0 is the eigenvector of H, then

$$P(y) = \prod_{\sigma \in \mathfrak{S}} (y^m - \sigma(y_0)^m).$$

Now, as the a_i are rational, they are invariant under $\mathcal{G}al(L)$. So, one can decompose the a_i in terms of invariants (or semi-invariants) of the group. Recall that a homogeneous polynomial $M(y_1, \cdots, y_n)$ is called an *invariant* of the group if it is left invariant under the action of the group ($\sigma(M)(y_i) = M(\sigma(y_i)) = M(y_i)$). Now, to detect if the group has invariants of degree m (resp. semi-invariants), one just has to search for rational solutions (resp. exponential solutions) of $L^{\circledS m}$, and we are almost done: as these solutions are given up to multiplication by constants, we just adjust the constants so as to really obtain the desired polynomials. Examples and more precise descriptions of this process are given in [SUl93b, SUl93a].

3.8. Symmetric powers

The whole philosophy was to reduce the computation of Liouvillian solutions to the computation of exponential (and sometimes rational) solutions of some symmetric powers of L. In fact, group-theoretic considerations show that one can reduce the presence of liouvillian solutions to the reducibility of some symmetric powers. Conversely, reducibility of some symmetric powers helps finding the Galois group of a given linear differential equation. This gives elegant criteria, as shown by this last result from [SUl93a]

Théorème 84 Singer-Ulmer. *Liouvillian solutions and symmetric powers are linked the following way:*

The equation $y'' - ry$ has a liouvillian solution if and only if $L^{\circledS 6}$ is reducible.
The equation $L(y) = y''' - a_1 y' - a_0 y = 0$ has a Liouvillian solution if and only if

1 $L^{\circledS 4}$ has order less than 5 or is reducible AND
2 (a) $L^{\circledS 2}$ has order 6 and is irreducible OR
(b) $L^{\circledS 3}$ has a factor of order 4.

Références

[Abd95] Abdeljaoued J *Sur l'algorithme de Berkowitz pour le calcul du déterminant dans un anneau commutatif arbitraire*, Prépublication, université de Besançon, 1995.

[Abr91] Abramov S.A, Kvashenko K.Yu *Fast algorithms for the rational solutions of linear differential equations with polynomial coefficients* Actes International Symposium on Symbolic and Algebraic Computation 91, ACM Press 1991.

[AZ95] Abramov S.A., Zima E.V *Ore polynomial rings and linear systems reduction.* Vestnik MGU, ser. 15, Computat. Maths. and Cybernetics **3**, 1995, pages 50-56.

[ABP95] Abramov S.A, Bronstein M & Petkovšek M *On polynomial solutions of linear operators* Proceedings of International Symposium on Symbolic and Algebraic Computation'95, ACM Press, 1995.

[AVE67] Andreev E.M, Vinberg E.B, & Elashvili A.G *Orbits of greatest dimensionality of semi-simple linear Lie groups* Funct. Anal. and Appl. **1** N° 4 (1967) pages 3-7

[AVB93] Arnaudies J.-M & Valibouze A *Résolvantes de Lagrange* Prépublication, rapport L.I.T.P 93.61, Institut Blaise Pascal (Paris), Décembre 1993.

[Artin] Artin M *Algebra* Prentice-Hall, 1991.

[Bar93] Barkatou A. *An algorithm for computing a companion block diagonal form for a system of linear differential equations*, Journal of Appl. Alg. in Eng. Comm. and Comp. , vol **4** (1993), pp. 185-195.

[Ber86] Bertrand D. *Théorie de Galois différentielle* Cours de DEA, Notes rédigées par R. Lardon, Université de Paris VI, 1986

[BBH88] Beukers F & Brownawell D & Heckmann G *Siegel Normality* Annals of Math, vol **127** (1988), pp. 279-308

[Beu92] Beukers F *Differential Galois theory* In: From Number Theory to Physics (Ed: Waldschmidt, Moussa, Luck, Itzykson), Springer 1992.

[Bia62] Bialynicki-Birula *On Galois theory of fields with operators* Amer. J. Math. **84** , 1962 pages 89-109

[Bou94] Boulier F *Algorithmes d'élimination en algèbre différentielle* Thèse, Université de Lille I, 1994.

[Bro90] Bronstein M *A unification of liouvillian extensions* Appl. Alg. in Eng. Comm. and Comp. journal **1** (1990) n^o 1, pp 5-24.

[Br92a] Bronstein M *Linear differential equations: breaking through the order two barrier* Actes International Symposium on Symbolic and Algebraic Computation 92, ACM Press 1992.

[Br92b] Bronstein M *Solutions of linear differential equations in their coefficient field* J.Symb.Comp **13**, 1992

[Bro93] Bronstein M *Symbolic integration* Livre a paraître.

[BrP94] Bronstein M & Petkovšek M *On the factorisation of skew-polynomials* Prépublication, 1994.

[Bui94] Buium A *Differential algebra and diophantine geometry* Hermann, Paris 1994.

[CM82] Cerveau D & Mattei J-F *Formes intégrales holomorphes singulières* Astérisque 97, Société Mathématique de France (1982), Paris.

[CLN91] Cerveau D & Lins-Neto A *Holomorphic foliations in $CP(2)$ having an invariant algebraic curve* Ann. Inst. Fourrier, **41**, 4 (1991), pp 883-903

[Chr94] Christophe *Les aventures du savant Cosinus* Réédition Armand Colin, 1994.

[Col95] Colin A *Formal computation of Galois groups with relative resolvants* Actes International symposium on Appl. Alg. in Eng. Comm. and Comp. 11 (Ed. M. Giusti & T. Mora), Lect. Notes in Comp. Sci. 948, Springer, 1995.

[Col93] Collins B *Algebraic invariant curves of polynomial vector fields in the plane* Prépublication, University of Waterloo, 1993

[Com94] Compoint E *Generalisation of a theorem of Fano-Singer* Comptes Rendus Acad. Sci. serie I, Paris, Mai 1994.

[Com95a] Compoint E *Équations différentielles et relations algébriques* Prépublication, Université de Paris 6, 1995.

[CLO92] Cox D., Little J., O'Shea D. *Ideals, varieties, and Algorithms* Undergraduate Texts in Math, Springer 1992

[Darboux] Darboux G *Mémoire sur les équations différentielles algébriques du premier ordre et du premier degré* Bull Sc Math, $2^{\text{ème}}$ série, **2** (1878), pages 60-96, 123-144, 151-200.

[DLR92] Duval A & Loday-Richaud M *Kovacič's algorithm and its application to some families of special functions* Appl. Alg. in Eng. Comm. and Comp. Journal **3**, 1992.

[DST87] Davenport,Siret,Tournier *Calcul formel* Masson, Paris 1987

[DDS93] Della Dora J & Stolovitch L *Normal forms* In *Computer Algebra and Differential Equations*, Ed. E. Tournier, Cambridge Press. (1994)

[Der93] Derksen H *The kernel of a derivation* J. Pure and Applied Algebra **84** (1993) 13-16 North-Holland

[DF93] Deveney J.K & Finston D.R *G_a actions on $\mathbb{C}^3$ and $\mathbb{C}^7$*, Prépublication, 1993.

[Die70] Dieudonne J.A & Carrell J.B *Invariant theory, Old and New* Academic Press, 1991.

[DLS95] Dobrovol'skii V.A & Lokot' N.V & Strelcyn J.M *Mikhail Nikolaevitch Lagutinskii (1871-1915), Un mathématicien méconnu* À paraître, Historia Mathematica.

[Dra37] Drach J *Sur la réduction de l'équation générale de Riccati* Comptes Rend. Acad. Sci **205** (1937) Paris pp 700-704 (Errata t.207 (1938) p.384)

[Ela72a] Elashvili A.G *Stationary subalgebras of points of the common state for irreducible Lie groups* Funct. Anal. and Appl. **6** N° 1 (1972), pages 44-53

[Ela72b] Elashvili A.G *Cannonical form and stationary subalgebras of points of general position for simple linear Lie groups* Funct. Anal. and Appl. **6** N° 2 (1972), pages 139-148

[Eps55] Epstein M *An existence theorem in the algebraic study of homogeneous linear ordinary differential equations* Proc. Amer. Math. Soc. **6** , 1955 pages 33-41

[Fah93] FAHIM A *Extensions Galoisiennes d'algèbres différentielles*, Publications IRMA vol.**31**, N° 10, 1993.

[Fak94] FAKLER W. *Algorithmen zur symbolischen lösung homogener linearer differentialgleichungen* Diplomarbeit, Universität Karlsruhe, Mai 1994.

[Fuc78] FUCHS L *Ueber die linearen Differentialgleichungen zweiter Ordnung, welche algebraische Integrale besitzen, zweite Abhandlung* J. für Math. (1878) **85**.

[FH91] FULTON W & HARRIS J *Representation theory, a first course* Graduate Texts in Math. **129**, Springer 1991.

[GHe91] GIUSTI M. & HEINTZ J. *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, Actes de "Computional Algebraic Geometry and Commutative Algebra", Cortona, Italie, Juin 1991.

[Gol58] GOLDMAN L *Lower order equation for zeroes of a linear differential polynomial* Illinois J. Math **2** (1958), pp 567-576

[Gor94] GORIELY A *Singularity analysis and integrability* PhD dissertation, Brussels, 1994.

[Gri90] GRIGORIEV Y *Complexity of testing reducibility of linear differential systems* Proceedings International Symposium on Symbolic and Algebraic Computation 90, ACM Press.

[HvP93] HENDRIKS P & VAN DER PUT M *A rationality result for Kovacič's algorithm* Actes International Symposium on Symbolic and Algebraic Computation 93, ACM press 1993.

[HvP94] HENDRIKS P & VAN DER PUT M *Galois action on solutions of a differential equation* À para^{ı}tre in: J. Symb. Comp, 1994.

[Hoe95] VAN HOEIJ M *Formal solutions and factorisation of differential operators with power series coefficients* Prépublication, Université de Nijmegen, 1995.

[Jor78] JORDAN C *Mémoire sur les équations différentielles linéaires à intégrale algébrique*, J. für Math. (1878) **84**.

[Jou79] JOUANOLOU J.P *Équations de Pfaff algébriques* Lect Notes in Maths 708, Springer-Verlag, 1979.

[Kap57] KAPLANSKY I *An introduction to differential algebra* Second edition, Hermann, Paris 1976.

[Kem1] KEMPF G.R *Computing invariants* in: Koh,S.S. (ed.) : Invariant theory, Lecture notes in mathematics 1278, Springer.

[Kem2] KEMPF G.R *More on computing invariants* in: Lecture notes in mathematics 1479, pages 87-93, Springer

[Kol48a] KOLCHIN E. R *Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations* Annals of Maths **49** , No 1, January 1948 pages 1-42

[Kol48b] KOLCHIN E. R *Existence theorems connected with the Picard-Vessiot theory of homogeneous linear ordinary differential equations* Bull.Amer.Math.Soc **54** , 1948 pages 927-932

[Kol68] KOLCHIN E. R *Algebraic groups and algebraic dependence* Amer. J. Math. **?** (1968) pp 1151-1164

[Kol73] Kolchin E. R *Differential algebra and algebraic groups* Academic Press, 1973.

[Kov86] Kovacič J *An algorithm for solving second order linear homogeneous differential equations* J.Symb.Comp **2** (1986) pp 3-43.

[Lan92] Lang S *Algebra* Third edition, Addison-Wesley, 1992.

[Lan83] Lang S *Fundamentals of diophantine geometry* Springer 1983

[Lev89] Levelt A.H.M *Differential Galois theory and tensor products* Indagationes mathematicae 1989.

[Lio33] Liouville J *Sur la détermination des intégrales dont la valeur est algébrique*, J. de l'École Polytechnique (1833) **22**.

[Lio38] Liouville J *Sur la classification des transcendantes* Journal de mathématiques pures et appliquées **4** , (1838)

[LP93] Lloyd & Pearson *Limit cycles and centres: an example* in: Differential Equations, Dynamical Systems and Control Science', ed. Elworthy, Everitt and Lee (Dekker, 1993)

[LRi91] Loday-Richaud M *Classification méromorphe locale des systèmes différentiels linéaires méromorphes: phénomène de Stokes et application* Thèse, Université d'Orsay, 1991

[Lut90] Lützen J. *Joseph Liouville 1809-1882 Master of pure and applied mathematics* Studies in the history of mathematics and physical science 15, Springer Verlag , 1990

[McM94] Mac Callum M & Man Y *A rational approach to the Prelle-Singer algorithm* Prépublication, August 94.

[Man94] Man Yu *Computing closed-form solutions of first-order ODEs using the Prelle-Singer procedure* J. Symb. Comp **16** N° 5 (1993), pages 423-444

[MMi95] Mansfield L & Milne A *Special integrals of ordinary differential equations* Prépublication, 1995

[Mar98] Marotte *Les équations différentielles linéaires et la théorie des groupes* Thèse, Annales École normale supérieure, Gauthier-Villard (1898), Paris

[MRa89] Martinet J & Ramis J.P *Généralités sur la théorie de Galois différentielle* In *Computer Algebra and Differential Equations*, Ed. E. Tournier, New York: Academic Press. (1990)

[Mag94] Magid A *Lectures on differential Galois theory*, to appear in the *University lectures series* of the A.M.S, 1995

[Mit95] Mitschi C *Differential Galois groups of confluent generalized hypergeometric equations: an approach using Stokes multipliers* à paraitre dans: Pacific J. Math.

[MSi95] Mitschi C & Singer M.F *Connected linear groups as Galois groups over $C(x)$*, Prépublication 1995.

[MoS90] Moulin-Ollagnier J & Strelcyn J.M *On first integrals of linear systems, Frobenius integrability theorem, and linear representations of Lie algebras* in: Lect Notes in Math 1455 (Ed. J.P Francoise et R Roussarie), Springer 1991.

[MOl92] Moulin-Ollagnier J *On liouvillian first integrals of homogeneous three-dimensional vector fields*, Prépublication 92-09, Université de Paris-Nord , 1992

[MNS93] Moulin-Ollagnier J & Nowicki A & Strelcyn J.M *On the non-existence of constants of derivations: the proof of a theorem of Jouanolou and is developpment* Bull. Sci. Math **119** (1995), p. 195-233.

[Mor94] Morales J.J *Non integrability of Hamiltonian systems and Stokes multipliers* Prépublication, University of Barcelona, april 94.

[Nag88] Nagata M & Nowicki A *Rings of constants for k-derivations in* $k[x_1, \cdots, x_n]$ J.Math.Kyoto Univ **28** (1988) 11-118

[Now94] Nowicki A *Polynomial derivations and their rings of constants* Uniwersytet Mikolaja Kopernika, Torun, 1994

[Nis89a] Nishioka K *General solutions depending algebraically on arbitrary constants* Nagoya Math. J. **113** 1989 pages 1-6

[Nis89b] Nishioka K. *On the transcendancy of Painlevé's first transcendant* Nagoya J. Maths. 1989

[Oll90] Ollivier F *Le problème de l'identifiabilité structurelle globale* , Thèse, Ecole Polytechnique 1990

[Ore33] Ore O *Theory of non-commutative polynomials*, Ann. of Math. (1933) **34**

[PGe95] Péladan-Germa A Testing identities of series defined by algebraic partial differential equations Actes International symposium on Appl. Alg. in Eng. Comm. and Comp. 11 (Ed. M. Giusti & T. Mora), Lect. Notes in Comp. Sci. 948, Springer, 1995.

[Pop79] Popov V.L *Constructive Invariant theory* in: Tableaux de Young et foncteurs de Schur, Aste'rique 87-88 pages 303-334.

[Pop82] Popov V.L *The constructive theory of invariants* Math USSR Izvest. **19** (1982) pp 359-376

[Pop83] Popov V.L *Homological dimension of algebras of invariants* J. Reine Angew. Math. **341** (1983) pp 151-173.

[Pop91] Popov V.L *Invariant theory* Amer. Math. Soc. Transl. **148**, 1991.

[PV94] Popov V.L & Vinberg E.B *Invariant theory* in: Encyclopaedia of Math. Sci, Algebraic Geometry IV, vol **55** (1994), pages 123-284, Springer-Verlag

[PSi83] Prelle M.J & Singer M.F *Elementary first integrals of differential equations* Trans. Amer. Math. Soc, **279** (1983) Number 1, pp 215-229.

[Pai97] Painlevé P *Lecons sur la theorie analytique des équations différentielles professées à Stockholm* , A.Hermann - Paris (Reprint in Oeuvre, CNRS 1972) , 1897

[Pep62] Pépin P.TH *Méthode pour obtenir les intégrales algébriques des équations différentielles linéaires du second ordre*, Atti dell' Accad. Pont. de Nuovi Lincei, XXXIV, p. 243-388 (1881)

[Poole] Poole E.G.C *Introduction to the theory of linear differential equations* Clarendon Press, Oxford, 1936 (reprint: Dover, 1960)

[Put95] van der Put M *Differential equations in characteristic p* À para^{ı}tre in Compositio math., special issue in honor of Frans Oort, 1995.

[Ram85] Ramis J-P *Théorèmes d'indice Gevrey pour les équations différentielles ordinaires*, Memoirs of the A.M.S **296** (1984).

[Ram91] Ramis J.P *About the solution of some inverse problems in differential Galois theory by Hamburger differential equations* Publication de l'Institut de Recherche Mathématique Avancée de Strasbourg, 1992.

[Rao94] Rao N.V *A generalization of the Liouville's theorem on elementary functions* Prépublication, University of Toledo Ohio, 1994.

[Rit40] Ritt J.F Trans.Amer.Math.Soc **48** , 1940 pages 542-552

[Rit50] Ritt J.F *Differential Algebra* AMS coll. Publications (or Dover, 1966) 1950.

[Rob90] Roberts P *An infinitely generated symbolic blow-up in a power series ring and a new counter-example to Hilbert's fourteenth problem*, J. Algebra **132** (1990), pp 461-473.

[Ros72] Rosenlicht M *Integration in finite terms* Amer.Math.Monthly, **79** (1972) pp 963-972.

[Ros73] Rosenlicht M *An analogue of L'hospital's rule* Amer.J.Math. **2** (1973) pp 369-374.

[Ros75] Rosenlicht M *Differential extension fields of exponential type* Pac. J. Math. **57** N° 1 (1975), pp 289-300.

[Ros76] Rosenlicht M *On Liouville's theory of elementary functions* Pac. J. Math. **65** N° 2 (1976), pp 485-492

[Sch93] Schlomiuk D *Elementary first integrals and algebraic invariant curves of differential equations* Expositiones Math **11** (1993), pp 433-454.

[Sei56] Seidenberg A *Contribution to the Picard-Vessiot theory of homogeneous linear differential equations* Amer. J. Math. **78** , 1956 pages 808-817

[SUl93a] Singer M.F & Ulmer F *Galois groups for second and third order linear differential equations* J.Symb.Comp **16 No. 1** , July 93

[SUl93b] Singer M.F & Ulmer F *Liouvillian and algebraic solutions of second and third order linear differential equations* J.Symb.Comp (1993) vol **16**, pp 37-73.

[SUl93c] Singer M.F. & Ulmer F. *On a third order equation whose differential Galois group is the simple group of 168 elements* Actes International symposium on Appl. Alg. in Eng. Comm. and Comp.10 (Porto-Rico) Ed. Mora & Moreno, Lecture Notes in Computer Science, Springer, 1994.

[SUl94] Singer M.F & Ulmer F *Necessary conditions for liouvillian solutions of (third order) linear differential equations* J. of Appl. Alg. in Eng. Comm. and Comp. vol **6** No 1 (1995) pp 1-22.

[Sin80] Singer M.F *Algebraic solutions of n^{th} order linear differential equations*, Actes 1979 Queens Conference on Number Theory, Queens Papers in Pure and Applied Mathematics (1980) **54**.

[Sin81] Singer M.F *Liouvillian solutions of n-th order homogeneous linear differential equations* Amer.J.Mat. **103** (1981) pp 661-682.

[Sin86] Singer M.F *Algebraic relations among solutions of linear differential equations: Fano's theorem* Amer. J. Math., **110**, (1986), pages 115-144.

[Sin89] Singer M.F *An outline of differential Galois theory* In *Computer Algebra and Differential Equations*, Ed. E. Tournier, New York: Academic Press. (1990)

[Sin91] Singer M.F *Liouvillian solutions of linear differential equations with liouvillian coefficients* J.Symb.Comp (1991) vol **11**, pp 251-273.

[Sin92] Singer M.F *Liouvillian first integrals of differential equations* Trans. Amer. Math. Soc, **333** (1992) Number 2, pp 673-687.

[Sin93] Singer M.F *Moduli of linear differential equations on the Riemann sphere with fixed Galois groups* Pac. J. Math **160** N° 2 (1993), pages 343-395

[Sin94] Singer M.F *Testing reducibility of linear differential operators: a group theoretic perspective* Prépublication, University of North Carolina, 1994. (À para^{ı}tre in J. of Appl. Alg. in Eng. Comm. and Comp.)

[Spr77] Springer T.A. *Invariant theory* Lect. Notes in Math. 585, Springer , 1977

[Spr81] Springer T.A. *linear algebraic groups* Progress in maths, Birkhaüser, 1981

[Sto88] Stockhamer R *Solving first order differential equations using the Prelle-Singer algorithm* Technical report 88-09, University of Delaware, 1998.

[Stu94] Sturmfels B *Algorithms in invariant theory* RISC series, Springer 1994

[TT79] Tretkoff & Tretkoff *Solution of the inverse problem of differential Galois theory in the classical case* Amer J. Math **101** (1979), pages 1327-1332

[Ulm89] Ulmer F & Calmet J *On liouvillian solutions of homogeneous linear differential equations*, Actes International Symposium on Symbolic and Algebraic Computation 90, ACM press 1990.

[Ulm92] Ulmer F *On liouvillian solutions of differential equations*, J. of Appl. Alg. in Eng. Comm. and Comp. (1992) **2**.

[Ulm94] Ulmer F *Linear differential equations of prime degree (the imprimitive case)* J. Symb. Comp. vol **18** No 4 (1994), pp 385-401

[UWe94] Ulmer F & Weil J.A *Note on Kovacič's algorithm* Prepublication IRMAR 94-13, Rennes Juillet 94 (to appear).

[Ves92] Vessiot E *Sur l'intégration des équations différentielles linéaires* Thèse, Annales de l'école normale supérieure, 1892.

[Ves15] Vessiot E *Méthodes d'intégration explicites* Encyclopédie du savoir mathématique 1915 (Edition Jacques Gabay, 1992)

[Weber] Weber H. *Traité d'algèbre supérieure* Gauthiers-Villard, Paris, 1898.

[Wei92] Weil J.A *De l'importance d'être constant* Note Informelle de Calcul Formel N° 41, École Polytechnique*, 1992.

[WGOS] Weil J.A, Germa-Péladan A, Ollivier F, et Shih J.A : *Quelques approches algébriques effectives des phénomènes différentiels* Images des Mathématiques 95* (Ed : F. Murat & J.L Colliot-Thelene), Éditions du CNRS, 1995.

[Wei94] Weil J.A *The use of the Special semi-groups for solving quasi-linear differential equations* Actes International Symposium on Symbolic and Algebraic Computation 94*, ACM press 1994.

* Disponible au laboratoire G.A.G.E de l'école polytechnique, ou à l'adresse `http://medicis.polytechnique.fr`

[Wei95] Weil J.A *First integrals and Darboux polynomials of homogeneous linear differential systems*, Actes International symposium on Appl. Alg. in Eng. Comm. and Comp. 11 (Ed. M. Giusti & T. Mora), Lect. Notes in Comp. Sci. 948, Springer, 1995.

[Wei85] Weisfeiler B *Comments on differential invariants* in "Infinite dimensional groups with applications" Ed V.Kac, Math Sci Research Inst Publi **4**, Springer 1985.

Résumé :
Gaston Darboux a montré que la recherche d'intégrales premières d'équations différentielles se ramenait au problème suivant : étant donné une dérivation D d'un anneau de polynômes, trouver des polynômes F et a tels que $DF = aF$; on dit alors que F est un *polynôme de Darboux*.
Dans un premier temps, nous rappelons et complétons l'état de l'art sur l'utilisation de polynômes de Darboux pour calculer des intégrales premières d'équations différentielles quasi-linéaires ou de champs de vecteurs. Nous montrons ensuite comment caractériser les polynômes de Darboux de systèmes différentiels linéaires en les liant bijectivement aux invariants du groupe de Galois différentiel. Enfin, nous appliquons ces idées au calcul de solutions algébriques ou liouvilliennes d'équations différentielles linéaires d'ordre 2 et 3.
Nos algorithmes ont été implantés dans le système de calcul formel MAPLE et nous décrivons en annexe les détails de cet aspect.

MOTS-CLÉS : Intégrales premières, Calcul formel, Théorie de Galois différentielle, Algèbre différentielle, Théorie des invariants, Groupes linéaires algébriques, Fonctions liouvilliennes.

Abstract :
Gaston Darboux showed that the search for first integrals of differential equations could be reduced to the following problem: given a derivation D of a polynomial ring, find polynomials F and a such that $DF = aF$; such an F is called a *Darboux polynomial*.
In a first part, we recall and complement the state of the art on the use of Darboux polynomials for computing first integrals of quasi-linear differential equations or vector fields. In a second part, we then show how to characterize the Darboux polynomials of linear differential systems by relating them bijectively with the semi-invariants of the differential Galois group. We then apply these ideas to the computation of algebraic or Liouvillian solutions of linear differential equations of order 2 and 3.
Our algorithms have been implemented in the computer algebra system MAPLE and we describe the details of this aspect.

KEY-WORDS : First integrals, Symbolic computation, Differential Galois theory, Differential algebra, Invariant theory, Linear algebraic groups, Liouvillian functions.

Index