CALCUL FORMEL
POUR LES ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES

par

Jacques-Arthur Weil

Mais il n'y a pas d'idéal dont le charme n'ait son péril, et pourtant on ne saurait priver la vie d'idéal sans la condamner à la platitude et au morne désespoir.
(J. Bedier, Tristan et Iseut)

Introduction

À la base, les systèmes de calcul formel savent essentiellement faire deux classes d'opérations : de l'algèbre linéaire, et de la manipulation de polynômes (algorithme d'Euclide, pgcd, résultants, etc). Dans la première partie de cet exposé (sections 1 et 2), nous allons montrer comment ramener l'intégration des fonctions usuelles à du calcul sur des polynômes. Dans la deuxième partie (sections 3 et 4), nous verrons comment, au prix d'une belle théorie mathématique (la théorie de Galois différentielle), on peut de même rechercher effectivement des solutions « explicites » d'équations différentielles linéaires (nous nous restreindrons ici au second ordre).

Ces notes sont essentiellement tirées d'un cours enseigné avec Driss Boularas à l'université de Limoges. Les deux sections sur l'intégration reprennent des présentations développées dans les articles **[17, 19, 32]** et les livres **[5, 9]** ; Les deux sections sur les équations différentielles sont principalement inspirées des articles **[29, 17, 24, 23, 14, 21, 22]**, ainsi que de passionnantes conversations avec Manuel Bronstein, Mark van Hoeij, Marius van der Put, Michael F Singer, et Felix Ulmer. Un certain nombre de résultats sont présentés sous forme d'exercices (élaborés avec Driss Boularas). L'histoire du sujet et son évolution récente sont remarquablement traités dans **[22]** qui contient de plus une très vaste bibliographie.

Dans ce qui suit, la lettre k désignera (sauf mention contraire) le corps $\overline{\mathbb{Q}}(x)$ (où $\overline{\mathbb{Q}}$ est la clôture algébrique de $\mathbb{Q}$). Tous les anneaux et corps considérés sont de caractéristique zéro.

1. Primitives des fractions rationnelles

1.1. Méthode naïve. Soit $f = p/q \in k$ une fraction rationnelle sous forme canonique[(1)]. Sur $\overline{\mathbb{Q}}$, le polynôme q se factorise en $q = \prod_{i=1}^{m}(x-a_i)^{n_i}$ et on peut en tirer une décomposition en éléments simples de f :

$$f = r + \sum_{i=1}^{m}\sum_{j=1}^{n_i}\frac{c(i,j)}{(x-a_i)^{n_j}}, \qquad r \in \overline{\mathbb{Q}}(x),\ c_{i,j} \in \overline{\mathbb{Q}}.$$

Comme on sait intégrer tous les éléments simples, on tire aisément de cette décomposition une primitive[(2)] de f :

$$\int f = \int r + \sum_{i=1}^{m} c(i,1)\ln(x-a_i) + \sum_{i=1}^{m}\sum_{j=2}^{n_i}\frac{-c(i,j)}{(j-1)(x-a_i)^{j-1}}. \tag{1}$$

Pour un système de calcul formel, il n'est pas simple (quoique possible) de manipuler séparément les zéros de q sur $\overline{\mathbb{Q}}$: ça introduit de nombreuses extensions algébriques inutiles. Dans la suite de cette partie, nous allons voir comment calculer une primitive de f sans factoriser q sur $\overline{\mathbb{Q}}$ en utilisant des pgcd et des résultants.

1.2. Factorisation sans carrés et décomposition partielle en éléments simples

Soit $f = p/q \in k$. On obtient facilement la partie entière de f par une division euclidienne donc, dans ce qui suit, nous supposons que $\deg(p) < \deg(q)$.

1.2.1. *Factorisation sans carré*

Définition 1. Soit $q \in \mathbb{Q}[x]$.

1. On dit que q est *sans carré* si $\mathrm{pgcd}(q, q') = 1$.
2. On appelle *factorisation sans carré* de q la décomposition $q = q_1 q_2^2 \cdots q_m^m$ où les q_i sont sans carré et $\mathrm{pgcd}(q_i, q_j) = 1$.

Cette décomposition peut se calculer en n'utilisant que des pgcd, comme on peut le voir dans l'exercice suivant :

***Exercice 1* (Algorithme de Yun).** On considère un polynôme P à coefficients dans $\mathbb{Q}$ et l'algorithme suivant :

$i := 1;\quad Q := 1;\quad C := \mathrm{PGCD}(P, P');\quad R := P/C;$
while $C \neq 1$ **do {**
$Y := \mathrm{PGCD}(C, R); Z := R/Y;$
$Q := Q.Z^i$; i := i+1 ;
$R := Y; C := C/Y$ **}**
$Q := Q \cdot R^i.$
return Q

(1) C'est à dire $\mathrm{pgcd}(p, q) = 1$ et q unitaire.
(2) Dans tout ce qui suit, on omettra les constantes d'intégration.

1. Soit $P = P_1 \cdot P_2^2 \cdot P_3^3$ une factorisation sans carrés de P. Lui appliquer cet algorithme.
2. Prouver que cet algorithme donne la factorisation sans carrés de tout polynôme à coefficients dans $\mathbb{Q}$.

1.2.2. *Décomposition partielle en éléments simples*

Lemme 1. *Soit $f = p/q$ avec $\deg(p) < \deg(q)$. En n'utilisant que des divisions euclidiennes, la factorisation sans carré de q permet d'obtenir la décomposition partielle en éléments simples de f suivante :*

$$\frac{p}{q} = \sum_{i=1}^{m} \sum_{j=1}^{i} \frac{p_{i,j}}{q_i^j}, \qquad \deg(p_{i,j}) < \deg(q_i), \mathrm{pgcd}(q_i, q_i') = 1. \tag{2}$$

Démonstration. Si $q = q_1 q_2$, avec $\mathrm{pgcd}(q_1, q_2) = 1$ et $\deg(p) < \deg(q)$, alors on peut calculer une décomposition de f de la manière suivante.

Comme $\mathrm{pgcd}(q_1, q_2) = 1$, l'algorithme d'Euclide étendu nous donne deux polynômes s_1 et s_2 tels que $s_1 q_1 + s_2 q_2 = 1$. On en déduit que

$$\frac{p}{q} = \frac{ps_1}{q_2} + \frac{ps_2}{q_1}. \tag{3}$$

Pour réduire un peu plus, nous obtenons par division euclidienne des polynômes t_i, u_i tels que $ps_2 = t_1 q_1 + u_1$ avec $\deg(u_1) < \deg(q_1)$ (et de même $ps_1 = t_2 q_2 + u_2$). Comme $\dfrac{p}{q}$ n'a pas de partie entière, on voit en reportant ces expressions dans (3) que $t_1 + t_2 = 0$ et on obtient la décomposition :

$$\frac{p}{q} = \frac{u_1}{q_1} + \frac{u_2}{q_2}, \qquad \deg(u_i) < \deg(q_j). \tag{4}$$

Si $q_1 q_2 \cdots q_m^m$ est une factorisation sans carré de q, l'itération du procédé ci-dessus nous donne une décomposition

$$\frac{p}{q} = \sum_{i=1}^{m} \frac{u_i}{q_i^i}, \qquad \deg(u_i) < \deg(q_i^i).$$

Procédant par divisions successives, on obtient ensuite des polynômes $p_{i,j}$ tels que $u_i = \sum_{j=1}^{i} p_{i,j} q_i^{i-j}$ et $\deg(p_{i,j}) < \deg(q_i)$; on en déduit la décomposition partielle en éléments simples de f :

$$\frac{p}{q} = \sum_{i=1}^{m} \sum_{j=1}^{i} \frac{p_{i,j}}{q_i^j}, \qquad \deg(p_{i,j}) < \deg(q_i), \quad \mathrm{pgcd}(q_i, q_i') = 1. \tag{5}$$

□

Exercice 2. Appliquer la méthode ci-dessus à $\dfrac{x^2+1}{x^3+2x^2+x}$ et en déduire une primitive.

1.3. Réduction de Hermite. La recherche de primitives de fractions rationnelles est donc ramenée à la recherche de primitives de p/q^i où q est sans carré et $\deg(p) < \deg(q)$.

Comme plus haut, on peut calculer des polynômes u, v tels que $p = uq + vq'$ avec $\deg(u) < \deg(q')$ et $\deg(v) < \deg(q)$. Si $i > 1$, on a donc

$$\int \frac{p}{q^i} = \int \frac{u}{q^{i-1}} + \int \frac{vq'}{q^i}.$$

En intégrant par partie, on en déduit :

$$\int \frac{p}{q^i} = \frac{v}{(1-i)q^{i-1}} + \int \frac{(1-i)u + v'}{(i-1)q^{i-1}}.$$

Itérant le procédé, on est ramené à chercher des primitives de p/q où q est sans carré et $\deg(p) < \deg(q)$. Ce procédé est souvent nommé « réduction de Hermite ».

1.4. Résultant de Rothstein-Trager. Pour mieux voir ce qui suit, revenons un instant au monde des idées. Soit q sans carré et $\frac{p}{q} = \sum \frac{\alpha_i}{(x - a_i)}$ la décomposition en éléments simples sur $\mathbb{C}$. De par l'unicité de la décomposition, la fraction $\frac{p}{\prod(x-a_i)} - \frac{\alpha_1}{(x-a_1)}$ n'a pas de pôle en a_1 : le polynôme $x - a_1$ est un facteur commun de $p - a_1 q'$ et q. Ce qui suit algébrise cette idée simple.

Si A est un anneau, rappelons que le *résultant en x* de deux polynômes $r, s \in A[x]$, noté $Res_x(r, s)$, est un élément de A qui est nul si et seulement si r et s ont un facteur commun. C'est de plus un objet effectif (c'est le déterminant de la matrice de Sylvester de r et s, voir **[5, 9]** ou tout livre d'algèbre générale). Le critère suivant, du simultanément à Rothstein et Trager, achève notre étude des primitives de fractions rationnelles.

Théorème 1*. Soit $f = \frac{p}{q} \in k$, avec q sans carré et $\deg(p) < \deg(q)$. Posons $R = Res_x(p - Yq', q) \in \overline{\mathbb{Q}}[Y]$. Soit α_i les zéros de R et $v_i = \mathrm{pgcd}(p - \alpha_i q', q)$. Alors*

$$\int \frac{p}{q} = \sum_{R(\alpha_i)=0} \alpha_i \ln(v_i).$$

Démonstration. Comme v_i divise q par construction, il est sans carré.

Supposons que v_i et v_j aient un facteur commun w. Alors $p - \alpha_i q' = r_i w$ et $p - \alpha_j q' = r_j w$. Par soustraction, $(\alpha_i - \alpha_j)q' = (r_i - r_j)w$. Comme $\alpha_i - \alpha_j \neq 0$, il en découle que w divise q'. Or w divise q (car v_i divise q) et q est sans carré donc $\mathrm{pgcd}(v_i, v_j) = w = 1$. Il en découle que $\prod v_i$ divise q.

Soit β un zéro de q. Alors $q'(\beta) \neq 0$ et $\mathrm{pgcd}(p - \dfrac{p(\beta)}{q'(\beta)}q', q) \neq 1$, donc $\dfrac{p(\beta)}{q'(\beta)}$ est un des α_i. Il en découle que tout zéro de q est zéro d'un des v_i et, comme q est sans carré, que $q = \prod v_i$.

Pour achever la preuve, il reste à montrer que le polynôme $S = p - \sum \alpha_i v_i' \dfrac{q}{v_i}$ est identiquement nul. On a $\deg(S) < \deg(q)$. De plus, pour tout $j \neq i$, on sait que v_i divise $v_j' \dfrac{q}{v_j}$. Or,

$$S = p - \alpha_i \sum_j v_j' \frac{q}{v_j} + \sum_{j \neq i} (\alpha_i - \alpha_j) v_j' \frac{q}{v_j} = p - \alpha_i q' + \sum_{j \neq i} (\alpha_i - \alpha_j) v_j' \frac{q}{v_j}.$$

donc v_i divise S. Comme les v_i sont premiers entre eux, on en déduit que q divise S. Et donc, comme $\deg(S) < \deg(q)$, on a $S = 0$. □

Il y a plusieurs variantes et raffinements des méthodes exposées ci-dessus. Le livre de Bronstein **[5]** en donne une description claire et détaillée.

2. Intégration en forme finie

Le problème de l'intégration en forme finie s'énonce (vaguement) de la manière suivante : étant donnée une fonction « usuelle », reconnaître si elle admet une primitive qui s'exprime l'aide des fonctions usuelles et, si oui, la calculer. Il nous faut pour ceci donner un sens précis à la notion de fonction usuelle (ce seront les fonctions élémentaires) ; d'autre part, on ne peut pas manipuler algébriquement des fonctions, mais on peut s'en donner un *modèle* algébrique. L'outil pour ce faire sera l'algèbre différentielle.

2.1. Un peu d'algèbre différentielle. On appelle dérivation sur un corps K un opérateur δ vérifiant les deux propriétés usuelles de $\dfrac{d}{dx}$:

$$\forall\, a, b \in K,\ \delta(a+b) = \delta(a) + \delta(b) \text{ et } \delta(ab) = \delta(a)b + \delta(b)a.$$

Nous dirons alors que K muni de δ est un *corps différentiel*. L'ensemble des éléments de K dont la dérivée est nulle est appelé le *corps des constantes* de K. On dit que (K_1, δ_1) est une extension différentielle de K si $K \subset K_1$ et si la restriction de δ_1 à K coïncide avec δ. Étant donné une infinité d'indéterminées Y_i indexées par $\mathbb{N}$, nous pouvons étendre la dérivation à $K[Y_i]_{i \in \mathbb{N}}$ en posant $\delta(Y_i) = Y_{i+1}$. Par abus de notation, nous écrirons $Y_1 = Y'$, $Y_i = Y^{(i)}$; on dit alors que Y est une *indéterminée différentielle*. L'anneau des *polynômes différentiels* en Y est $K\{Y\} = K[Y, Y', Y'', \dots]$. Pour construire des solutions d'équations différentielles, nous allons considérer des idéaux de cet anneau. Mais, quand une fonction est solution d'une équation différentielle, elle est aussi solution de toutes les équations obtenues par dérivations successives. Pour un polynôme différentiel P, nous appellerons donc *idéal* *différentiel engendré par P* l'ensemble des combinaisons $\sum_{i\geq 0} A_i P^{(i)}$ (où les A_i sont des polynômes différentiels et où les $P^{(i)}$ désignent les dérivées successives de P) : les solutions de $P = 0$ sont des solutions de toutes ces équations différentielles. Plus généralement, un idéal différentiel est un idéal de $K\{Y\}$ stable sous l'action de la dérivation.

À présent, il est aussi simple de « modéliser » $\exp x$ que d'ajouter $\sqrt{2}$ à $\mathbb{Q}$. Soit $I = [Y' - Y]$ l'idéal différentiel (premier) engendré par $Y' - Y$ et soit $\phi : \mathbb{C}(x)\{Y\} \mapsto \mathbb{C}(x)\{Y\}/[Y' - Y]$ le morphisme canonique. Si on pose $y = \phi(Y)$, alors $y' - y = 0$. Bien sur, cette construction ne donne pas *la* fonction exponentielle mais modélise toute la classe des solutions de $y' - y = 0$. Ce que nous avons construit est un corps qui « ressemble » à $\mathbb{Q}(x, \exp x)$, au sens où toute propriété vraie dans $\mathbb{Q}(x, y)$ est vraie pour $\mathbb{Q}(x, \exp x)$. Les fonctions obtenues de cette manière sont dites *différentiellement algébriques.*

Exercice 3. Soit $(K,')$ un corps différentiel tel que son corps de constantes, C, soit de caractéristique zéro et $y' = fy$, où $f \in K$ une équation différentielle qui n'admet pas de solution algébrique sur K. Soit T une indéterminée différentielle et t la solution construite comme image de T dans le quotient $k\{T\}/[T' - fT]$. Vérifier que $k[t]$ est un anneau différentiel.

Soit $P \in k[T]$ un polynôme unitaire irréductible tel que $P(t)$ divise $P(t)'$. Montrer que $P = T$.

2.2. Modèles algébriques des fonctions élémentaires. Nous pouvons maintenant donner une définition précise (et un modèle algébrique) des fonctions élémentaires. Le principe est d'empiler des extensions pour introduire une par une les fonctions intermédiaires dont on a besoin.

Définition 2. Soit k un corps différentiel. On dit que K est une *extension élémentaire* de k si $K = k(t_1, \ldots, t_n)$ avec :

$$\forall\ i = 1, \ldots, n;\ \exists\ a_i \in k(t_1, \ldots, t_{i-1}) \quad \text{tel que}$$
$$\begin{cases} t_i \text{ algébrique} & (t_i \text{ est algébrique sur } k(t_1, \ldots, t_{i-1})), \\ \text{ou } \ t_i' = a_i'/a_i & (t_i \text{ modélise } \log(a_i), \text{ le logarithme de } a_i), \\ \text{ou } \ t_i' = a_i' t_i & (t_i \text{ modélise } e^{a_i}, \text{ l'exponentielle de } a_i). \end{cases}$$

À l'étape i de la construction, l'élément t_i est introduit par le même passage au quotient que ce que nous avons fait plus haut pour l'exponentielle.

Dans la suite, nous appellerons (par abus de langage) *fonction élémentaire* tout élément d'une extension élémentaire de $\mathbb{C}(x)$. Elle sera représentée par une fraction rationnelle en $t_1, \ldots, t_n$. Rigoureusement, cette façon de procéder ne construit à chaque étape que des modèles de classes de fonctions ; mais on peut montrer que toute « fonction élémentaire » construite algébriquement de cette façon a une réalisation comme « vraie » fonction (i.e. méromorphe sur un ouvert, **[19]**).

Prenons quelques exemples. Pour construire $\log(\log(x))$, on introduit t_1 avec $t_1' = \frac{1}{x}$, puis t_2 avec $t_2' = \frac{1}{xt_1}$; le représentant de $\log(\log(x))$ est alors t_2. Pour introduire $\log(1+e^{\cos(x)})$, on introduit successivement $t_1' = it_1, t_2' = \left(\frac{t_1^2+1}{2t_1}\right)' t_2, t_3' = \frac{t_2'}{1+t_2}$ (et le représentant est alors t_3). Pour la tangente hyperbolique, on introduit $t_1' = t_1$, et alors le représentant de $\tanh(x)$ sera $\frac{t_1^2-1}{t_1^2+1}$.

2.3. Principe de Liouville et algorithme de Risch. Pour mieux comprendre ce qui suit, revenons un instant aux fractions rationnelles. Si $f \in \overline{\mathbb{Q}}(x)$, nous avons vu plus haut qu'on pouvait trouver des fonctions rationnelles $v_0(x), v_1(x), \ldots, v_m(x)$ et des constantes $c_1, \ldots, c_m$ telles que

$$\int f(x)dx = v_0(x) + \sum_{i=1}^{m} c_i \log(v_i(x)).$$

L'observation lumineuse de Liouville est que cette propriété s'étend aux autres fonctions élémentaires, ce qui l'a conduit à introduire le principe suivant (prouvé correctement en 1968 par Rosenlicht et par Risch) que nous admettrons :

***Théorème 2* (Risch-Liouville).** *Soit K une extension élémentaire de $\mathbb{C}(x)$, soit C son corps de constantes et $f \in K$ une fonction élémentaire. S'il existe une extension élémentaire E de K et $g \in E$ telle que $g' = f$, alors il existe $v \in K$, des constantes $c_1, \ldots, c_n$ algébriques sur C, et $u_1, \ldots, u_n \in K(c_1, \ldots, c_n)$ tels que*

$$f = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}.$$

L'interprétation de ce *théorème de structure* est que, s'il existe une primitive, alors elle sera d'une forme particulière, et on sait quel type de fonctions il faudra introduire pour exprimer une primitive. Risch en a déduit un algorithme d'intégration qui consiste à reconnaître cette forme particulière.

Le principe est de procéder récursivement. Soit $f \in \mathbb{C}(t_1, \ldots, t_n)$ une fonction élémentaire. Nous voulons « éliminer » t_n pour nous ramener à des calculs dans $\mathbb{C}(t_1, \ldots, t_{n-1})$. Risch montre que le calcul d'une primitive de f se ramène au calcul de primitives d'éléments de $\mathbb{C}(t_1, \ldots, t_{n-1})$ et à la recherche de solutions dans $\mathbb{C}(t_1, \ldots, t_{n-1})$ d'équations de la forme $y' + Ay = B$ avec $A, B \in \mathbb{C}(t_1, \ldots, t_{n-1})$ (Risch donne un algorithme pour traiter ce dernier problème). De façon récursive, on « élimine » ainsi les t_i pour se ramener finalement à des calculs de primitives de fractions rationnelles. L'algorithme est très sophistiqué dans sa version générale.

2.4. Application : intégration de fe^g. Pour comprendre quelques idées fondamentales de l'algorithme de Risch, on pourra regarder l'exemple suivant (adapté de **[19]**) :

Exercice 4. Soit $k = \mathbb{C}(x)$ avec $x' = 1$. Soit $f, g \in k$ tels que l'équation différentielle (E) : $y' = \left(\dfrac{f'}{f} + g'\right) y$ n'admette pas de solutions algébriques. On pose $K = k(t)$ où t est une solution de l'équation différentielle (E) construite comme dans l'exercice 3.

1. Montrer que fe^g admet une primitive élémentaire si, et seulement si, il existe $v_0 \in K, c_1, \ldots, c_n \in \mathbb{C}$ et $v_1, \ldots, v_n \in k[t]$, unitaires et irréductibles tels que

$$(*) \qquad t = v_0' + \sum c_i \frac{v_i'}{v_i}.$$

2. Supposons que $(*)$ soit vérifiée et soit P un facteur dans $k[t]$ du dénominateur de v_0. Montrer que P divise P' et en déduire que $(*)$ s'écrit $t = v_0'$ où v_0 est dans $k[t]$.
3. On pose $v_0 = \sum_{i=1}^{p} d_i t^i$. Montrer que d_1 satisfait l'équation $y' + g'y = f$.
4. En déduire le théorème (dû à Liouville) : fe^g *admet une primitive élémentaire si, et seulement si, l'équation* $y' + g'y = f$ *admet une solution rationnelle.*
5. Application : montrer que e^{x^2} n'admet pas de primitive élémentaire.

3. Solutions liouvilliennes d'équations différentielles linéaires d'ordre 2 : l'algorithme de Kovacic

Soit C un corps algébriquement clos (ici : $C = \overline{\mathbb{Q}}$ ou $C = \mathbb{C}$). Soit $k = C(x)$ muni de la dérivation $\dfrac{d}{dx}$. Nous utiliserons la notation usuelle $'$ pour les dérivations rencontrées dans ce qui suit.

3.1. Classes de solutions d'équations différentielles linéaires. Nous considérons l'équation :

$$(L) : a_n y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_0 y = 0, \quad a_i \in \mathbb{C}[x].$$

Dans cette partie, nous allons donner un sens précis au mot « résoudre », c'est-à-dire décrire les classes de fonctions dans lesquelles nous cherchons une solution (et quelques unes de leurs propriétés).

3.1.1. *Solutions rationnelles et exponentielles.* On dit qu'une solution y est *rationnelle* si $y \in k$. De nombreux algorithmes (rapides) existent pour décider si $L(y) = 0$ a des solutions rationnelles (ex : **[1, 4, 2]**).

On dit qu'une solution y est *exponentielle sur* k si $y'/y \in k$ (formellement, on devrait dire « exponentielle d'une intégrale »). Les algorithmes de calcul de solutions exponentielles procèdent par une étude locale des solutions au voisinage de singularités puis se ramènent au calcul de solutions rationnelles.

Soit y une solution de $L(y) = 0$. Si l'on pose $u = y'/y$, alors $y''/y = u' + u^2$ et, en itérant, $y^{(i)}/y$ est un polynôme différentiel en u. En injectant ces expressions dans la relation $L(y) = 0$, on obtient que u satisfait une équation différentielle (non-linéaire) d'ordre $n-1$ qu'on appelle *l'équation de Riccati* associée à L. Les solutions exponentielles de L sont exactement les solutions rationnelles de l'équation de Riccati ; plus généralement, toute solution de l'équation de Riccati est la dérivée logarithmique d'une solution de L (et réciproquement).

3.1.2. *Solutions liouvilliennes.* Dans ce qui suit, nous chercherons les solutions d'équations différentielles linéaires dans une classe de fonctions un peu plus générale que les fonctions élémentaires :

Définition 3. On dit qu'une solution de L est une *solution liouvillienne* si elle appartient à un corps $k(t_1, \ldots, t_n)$ avec

$$\forall\ i = 1, \ldots, n;\ \exists\ a_i \in k(t_1, \ldots, t_{i-1}) \quad \text{tel que}$$
$$\begin{cases} t_i \text{ algébrique} & (t_i \text{ est algébrique sur } k(t_1, \ldots, t_{i-1})), \\ \text{ou}\ \ t_i' = a_i & (t_i = \int a_i, \text{ extension par une intégrale}), \\ \text{ou}\ \ t_i' = a_i t_i & (t_i = e^{\int a_i}, \text{ extension par l'exponentielle d'une intégrale}) \end{cases}$$

Comme pour l'intégration, il y a un beau théorème de structure (probablement dû à Vessiot, mais correctement prouvé par Kolchin [**13**]) qui dit que l'équation $L(y) = 0$ admet une solution liouvillienne si et seulement si l'équation de Riccati correspondante admet une solution algébrique. Dans la suite, nous allons expliquer (pour les équations d'ordre 2) comment la théorie de Galois différentielle donne ce résultat et permet d'obtenir le polynôme minimal d'une solution algébrique de l'équation de Riccati en se ramenant au calcul de solutions rationnelles ou exponentielles d'équations différentielles linéaires auxiliaires. La théorie générale est bien expliquée dans [**21, 3, 12, 13, 22**].

Dans toute la suite, nous étudions l'équation

$$L(y) = y'' + a_1 y' + a_0 y = 0, \qquad a_i \in k.$$

3.2. Théorie de Galois différentielle

3.2.1. *Groupe de Galois*

Définition 4. Soit K une extension différentielle de k. On dit que K est une *extension de Picard-Vessiot* de k (pour L) si les deux conditions suivantes sont réalisées :

1. $K = k(y_1, y_1', y_2, y_2')$, où y_1, y_2 forment un système fondamental de solutions de $L(y) = 0$.
2. Le corps des constantes de K est égal au corps des constantes de k.

On peut montrer qu'une telle extension de Picard-Vessiot existe et est unique à isomorphisme différentiel près ([**13, 21**]). Dans ce qui suit, nous fixons une fois pour toutes une extension de Picard-Vessiot et appelons *solution* une solution de $L(y) = 0$ dans K.

Définition 5. On appelle *k-automorphisme différentiel* de K un automorphisme g de K qui laisse k fixe et qui commute avec la dérivation, c'est dire :

1. $\forall\, y \in K,\ g(y)' = g(y')$
2. $\forall\, y \in k,\ g(y) = y$

Le *groupe de Galois différentiel* de K, noté $G = Gal(K/k)$, est l'ensemble des k-automorphismes différentiels de K.

Soit V le C-espace vectoriel des solutions et y_1, y_2 la base utilisée pour construire l'extension de Picard-Vessiot. Soit y une solution et $g \in G$. Alors, $g(y)$ est aussi une solution. En effet, comme $a_i \in k$, on a $g(a_i) = a_i$ et :

$$\begin{aligned} L(g(y)) &= g(y)'' + a_1 g(y)' + a_0 g(y) \\ &= g(y'') + g(a_1) g(y') + g(a_0) g(y) \\ &= g(L(y)) = g(0) = 0. \end{aligned}$$

Comme toute solution est une combinaison linéaire de y_1 et y_2, on en déduit qu'il existe des constantes $c_{i,j} \in C$ telles que $g(y_1) = c_{1,1}y_1 + c_{2,1}y_2$ et $g(y_2) = c_{1,2}y_1 + c_{2,2}y_2$. Comme un automorphisme différentiel de K est complètement déterminé par son action sur y_1 et y_2, ceci nous donne une représentation fidèle de G comme sous-groupe du groupe $\mathrm{GL}(2, C)$ des matrices inversibles. En fait, on peut montrer (**[14, 3, 21]**) que G est un *groupe linéaire algébrique*, c'est-à-dire que les entrées des matrices satisfont des contraintes polynomiales (cela vient du fait que les éléments de G préservent toutes les relations différentielles satisfaites par les solutions). Dans ce qui suit, nous identifierons souvent G à cette représentation.

3.2.2. *Quelques propriétés essentielles.* Comme dans la théorie classique, on a une correspondance galoisienne entre les sous-groupes algébriques de G et les sous-corps différentiels de K. Nous admettrons ici une version faible de cette correspondance :

Théorème 3. *Soit K une extension de Picard-Vessiot de k, soit G son groupe de Galois différentiel, et soit $z \in K$. Alors :*

$$z \in k \quad \Longleftrightarrow \quad \forall\, g \in G,\ g(z) = z.$$

Les propriétés qui suivent sont des conséquences de ce théorème. Soit $\mathrm{SL}(2,\, C) \subset \mathrm{GL}(2, C,)$ le groupe des matrices de déterminant égal à 1.

Lemme 2 **([12])**. *Il existe $f \in k$ vérifiant $f'/f = -a_1$ si et seulement si $G \subset \mathrm{SL}(2,\, C)$.*

Démonstration. Soit $w = y_1' y_2 - y_1 y_2'$ le déterminant Wronskien de y_1, y_2. Un calcul simple montre que $w' = -a_1 w$. Soit $g \in G$ et σ sa matrice. Alors :

$$g(w) = \text{dét} \begin{pmatrix} g(y_1) & g(y_2) \\ g(y_1') & g(y_2') \end{pmatrix} = \text{dét} \left(\begin{pmatrix} y_1 & y_2 \\ y_1' & y_2' \end{pmatrix} .\sigma \right) = w\, \text{dét}(\sigma).$$

Si dét$(\sigma) = 1$, alors la correspondance galoisienne montre que w est une solution dans k de $f' = -a_1 f$. Réciproquement, si cette équation admet une solution dans k, alors $w \in k$ et $g(w) = w$ donc dét$(\sigma) = 1$. □

En appliquant le changement de variable $y = z \cdot e^{-\int a_1/2}$, on peut se ramener à une équation où $a_1 = 0$ sans altérer le caractère liouvillien des solutions. Dans ce qui suit, nous supposerons donc que $G \subset \mathrm{SL}(2, C)$

Proposition 1. *Toutes les solutions de $L(y) = 0$ sont algébriques si et seulement si G est un groupe fini.*

Démonstration. Supposons que G soit un groupe fini. Soit y une solution de $L(y) = 0$. Considérons le polynôme

$$P = \prod_{g \in G} (Y - g(y)) \in K[Y].$$

Bien sur, $P(y) = 0$ et il reste à montrer que les coefficients sont dans k. Soit $g_0 \in G$. Comme la multiplication à gauche par g_0 est une bijection de G, on a

$$\prod_{g \in G} (Y - g_0 \cdot g(y)) = \prod_{\tilde{g} \in G} (Y - \tilde{g}(y))\,.$$

Donc les coefficients de P sont tous fixés par le groupe. La correspondance galoisienne montre alors qu'ils sont dans k.

Réciproquement, soit y_1, y_2 une base de solutions algébriques de polynômes minimaux P_i ; les images des y_i sont aussi des zéros des P_i. Les y_i n'ont donc qu'un nombre fini d'images possibles et, comme un élément de G est entièrement déterminé par son action sur y_1 et y_2, il ne peut y avoir qu'un nombre fini d'éléments de G. □

En fait, nous venons même de prouver un résultat un peu plus fort. Si $z \in K$, on appelle orbite de z sous G l'ensemble $Orb_G(z) = \{g(z), g \in G\}$; notre preuve montre qu'un élément de K est algébrique sur k si et seulement si son orbite sous G est finie. Son degré (i.e le degré de son polynôme minimal) est le nombre d'éléments de l'orbite, ou encore l'indice dans G du stabilisateur de z.

Proposition 2. *L'équation $L(y) = 0$ admet une solution exponentielle $y \neq 0$ si et seulement si, pour tout $g \in G$, il existe une constante $c_g \in C$ telle que $g(y) = c_g \cdot y$.*

Démonstration. Soit y une solution non nulle de $L(y) = 0$. Alors :

$$\left(\frac{g(y)}{y}\right)' = \frac{g(y')}{y} - \frac{y'}{y^2} g(y) = \frac{g(y)}{y}\left(g(\frac{y'}{y}) - \frac{y'}{y}\right).$$

Donc, $g(y)/y$ est une constante pour tout $g \in G$ si et seulement si y'/y est fixé par tout $g \in G$. Par la correspondance galoisienne, ceci est bien équivalent au fait que $y'/y \in k$. □

Notons que, comme pour les solutions algébriques, nous venons en fait de prouver un résultat plus fort : un élément z de K est exponentiel sur k si et seulement si la droite vectorielle $C \cdot \langle z \rangle$ est globalement invariante sous l'action de G. L'existence d'une solution exponentielle est donc équivalente à l'existence d'un vecteur propre commun à toutes les matrices de G ; si y_1 est ce vecteur propre, alors les matrices sont triangulaires supérieures.

Exercice 5 **([17])**. On considère l'équation $y' = ay$ où $a \in \mathbb{C}(x)$.

1. Montrer que tout sous-groupe algébrique propre de $\mathbb{C}^*$ est fini et cyclique.
2. En considérant les groupes de Galois possibles, montrer que toute solution algébrique de l'équation $y' = ay$ vérifie $y^m = f$ où $f \in \mathbb{C}(x)$; en déduire que l'équation a une solution algébrique si et seulement si il existe un entier positif m tel que l'équation $f' = maf$ ait une solution $f \in \mathbb{C}(x)$.
3. Soit $a = p/q \in \overline{\mathbb{Q}}(x)$. Soit $R = Res_x(p - Yq', q)$ le résultant de Rothstein-Trager de a. Pour chaque zéro α_i de R, on pose $v_i = \mathrm{pgcd}(p - \alpha_i q', q)$. En reprenant les méthodes de la partie 1.4, montrer que l'équation $y' = ay$ admet une solution algébrique si et seulement si les conditions suivantes sont réalisées :
   (a) $\mathrm{pgcd}(q, q') = 1$ et $\deg(p) < \deg(q)$.
   (b) Tous les zéros α_i de R sont rationnels

3.3. Les sous-groupes de $\mathrm{SL}(2, C)$.

Les sous-groupes algébriques de $\mathrm{SL}(2, C)$ sont bien connus et classifiés. Nous allons maintenant voir comment, pour chaque groupe de cette classification(à conjugaison près), les propriétés précédentes permettent de déterminer la forme de la solution.

3.3.1. *Cas réductible*

Définition 6. Soit G un groupe agissant sur un espace vectoriel V. On dit que (l'action de) G est *réductible* s'il existe un sous-espace non trivial $W \subset V$ tel que $G(W) \subset W$.

Dans notre cas, $\dim(V) = 2$ donc W est nécessairement de dimension 1 et les matrices sont triangulaires. D'après la remarque suivant la proposition 2, ceci est équivalent à l'existence d'une solution exponentielle y_1 de $L(y) = 0$.

Si W admet un complémentaire stable sous G, on dit que G agit de manière *complètement réductible.* Les matrices sont alors diagonales. Ce cas est étudié dans l'exercice 7.

Si G n'agit pas de manière réductible, on dit qu'il est irréductible.

3.3.2. *Cas imprimitif*

Définition 7. Soit G un groupe irréductible agissant sur un espace vectoriel V. On dit que G est *imprimitif* s'il existe des sous-espaces V_i tels que $V = V_1 \oplus \cdots \oplus V_r$ et G permute transitivement les V_i :

$$\forall\, i = 1, \ldots, r\ \forall\, g \in G, \qquad \exists\, j \in \{1, \ldots, r\} : \ g(V_i) = V_j.$$

On dit alors que $V_1, \ldots, V_r$ forment un système d'imprimitivité pour G.

Dans notre cas, on a nécessairement $r = 2$ et $\dim(V_1) = \dim(V_2) = 1$. Les matrices sont de la forme

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix} \quad \text{avec} \quad a, b \in C^*.$$

Lemme 3. *Supposons que G est irréductible. Alors, l'équation de Riccati admet une solution algébrique de degré 2 si et seulement si G est imprimitif.*

Démonstration. Soit P le polynôme minimal d'une solution de Riccati algébrique de degré 2, et soient u_1, u_2 ses racines. Comme u_1, u_2 sont solutions de l'équation de Riccati, il existe des solutions y_i de $L(y) = 0$ telles que $y_i'/y_i = u_i$. Comme G permute les u_i, il permute les droites vectorielles $V_i = C \cdot \langle y_i \rangle$ et les V_i forment bien un système d'imprimitivité.

Réciproquement, soit $V_i = C \cdot \langle y_i \rangle$ un système d'imprimitivité. Si nous posons $u_i = y_i'/y_i$, alors G permute les u_i et, comme dans la remarque suivant la proposition 1, il sont donc algébriques de degré 2 et conjugués (on peut aussi vérifier directement que les fonctions symétriques en les u_i sont fixées par G). □

3.3.3. *Cas primitif*

Définition 8. Si G est irréductible et non imprimitif, on dit qu'il est primitif.

On peut montrer ([**24**]) qu'une équation dont le groupe de Galois est un sous-groupe primitif infini de $\mathrm{SL}(n, C)$ n'admet pas de solutions liouvilliennes ; et si le groupe est fini, alors toutes les solutions sont algébriques (proposition 1) donc liouvilliennes.

Dans le cas de $\mathrm{SL}(2, C)$, il y a trois groupes primitifs finis (voir [**23, 24**] pour une description de ces groupes) : le groupe du tétraèdre ($A_4^{SL_2}$) d'ordre 24, le groupe de l'octaèdre ($S_4^{SL_2}$) d'ordre 48, et le groupe de l'icosaèdre ($A_5^{SL_2}$) d'ordre 120. Dans les trois cas, toutes les solutions sont algébriques et donc les solutions de l'équation de Riccati sont également algébriques. En développant les idées présentées dans les propositions 1 et 2, l'étude de ces groupes ([**29, 14, 10**]) montre que :

- Pour $A_4^{SL_2}$: l'équation de Riccati admet des solutions algébriques de degrés 4, 6 ou 12.
- Pour $S_4^{SL_2}$: l'équation de Riccati admet des solutions algébriques de degrés 6, 8, 12, ou 24.
- Pour $A_5^{SL_2}$: l'équation de Riccati admet des solutions algébriques de degrés 12, 20, 30, ou 60.

Enfin, si $G = \mathrm{SL}(2, C)$, l'équation n'a pas de solutions liouvilliennes.

3.3.4. *Théorème de Kovacic.* Ce travail de classification est résumé dans le théorème suivant :

Théorème 4 **([14])**. *Soit $L(y) = 0$ une équation différentielle linéaire à coefficients dans k dont le groupe de Galois est contenu dans* $\mathrm{SL}(2, C)$. *Elle admet des solutions* *liouvilliennes si et seulement si elle admet des solutions de la forme $y = e^{\int u}$ où u est une solution algébrique de degré 1 (cas réductible), 2 (cas imprimitif), 4, 6 ou 12 (cas primitifs) de l'équation de Riccati associée.*

3.4. L'algorithme de Kovacic

3.4.1. *Puissances symétriques d'équations différentielles linéaires*

Soit $P = U^m + b_{m-1}U^{m-1} + \dots b_0$ le polynôme minimal d'une solution algébrique de l'équation de Riccati. Soit $u_1, \dots, u_m$ les zéros de P, et y_i les solutions de $L(y) = 0$ dont ils sont des dérivées logarithmiques. On a alors

$$b_{m-1} = -(u_1 + \dots + u_m) = -(\frac{y_1'}{y_1} + \dots + \frac{y_m'}{y_m}) = -\frac{(\prod y_i)'}{\prod y_i}.$$

Le coefficient $-b_{m-1}$ est donc la dérivée logarithmique d'un produit de m solutions de $L(y) = 0$.

Lemme 4 (**[20, 15]**). *Soit y_1, y_2 une base de solutions de $L(y) = 0$. On peut construire une équation différentielle, notée $L^{ⓢm}$, dont l'espace des solutions est l'ensemble des polynômes homogènes de degré m à coefficients dans C en y_1, y_2.*

Cette équation s'appelle la *m-ième puissance symétrique* de L.

Démonstration. Soit y une solution arbitraire de $L(y) = 0$. On pose $z = y^m$. On calcule z', z'', $\dots$, z^{m+1} en remplaçant à chaque fois y'' par son expression donnée par $L(y) = 0$. Les $z^{(i)}$ sont donc des combinaisons linéaires de monômes de degré m en y, y'. Ces monômes forment un k-espace vectoriel de dimension $m + 1$; si on a $m + 2$ éléments d'un tel espace, ils sont linéairement dépendants, donc z, z', z'', $\dots$, z^{m+1} satisfont une relation de dépendance linéaire sur k qu'on note $L^{ⓢm}(z) = 0$: on sait pour l'instant qu'elle est d'ordre au plus $m + 1$.

Soit A l'anneau différentiel $K[X_1, X_2]$ où l'on étend la dérivation en imposant que $X_1' = X_2' = 0$. Par construction, on a $L^{ⓢm}((X_1y_1 + X_2y_2)^m) = 0$. On en déduit facilement que tout monôme de degré m en y_1, y_2 est solution de $L^{ⓢm}(z) = 0$. Or, si ces monômes étaient linéairement dépendants, alors y_1, y_2 seraient linéairement dépendants (car tout polynôme homogène en deux variables se factorise en produit de facteurs linéaires sur C) : ils forment donc un espace vectoriel de dimension $m+1$. Donc $L^{ⓢm}(z)$ est d'ordre $m+1$ et l'espace de ses solutions est exactement cet espace vectoriel. □

On peut calculer la dépendance linéaire entre z, z', z'', $\dots$, $z^{(m+1)}$ avec les méthodes standard d'algèbre linéaire. Mais on peut aussi faire un peu plus fin, comme le montre l'exercice suivant.

Exercice 6 (**[6]**). On considère l'équation différentielle du second ordre $L(y) = y'' + ay' + by = 0$. On définit la suite récurrente d'opérateurs L_i par :

$$\begin{cases} L_0(y) & = & y, \\ L_1(y) & = & y', \\ L_{i+1}(y) & = & L_i(y)' + iaL_i(y) + i(m-i+1)bL_{i-1}(y). \end{cases}$$

1. Soit y une solution de $L(y) = 0$. Montrer par récurrence que

$$L_i(y^m) = m(m-1)\cdots(m-i+1)y^{m-i}(y')^i.$$

2. En déduire que $L_{m+1} = L^{ⓢm}$.

3.5. Solutions algébriques de l'équation de Riccati

Théorème 5 (**[14, 29, 25]**). *L'équation de Riccati admet une solution algébrique de degré au plus m si et seulement si la puissance symétrique $L^{ⓢm}(z) = 0$ admet une solution exponentielle.*

Démonstration. Si l'équation de Riccati admet une solution algébrique de degré m, nous avons vu que le coefficient b_{m-1} de son polynôme minimal est la dérivée logarithmique d'une solution exponentielle de $L^{ⓢm}(z) = 0$.

Réciproquement, soit z une solution exponentielle de $L^{ⓢm}(z) = 0$. Le lemme 4 montre qu'il existe un polynôme $Q(y_1, y_2)$ homogène de degré m tel que $z = Q(y_1, y_2)$. Soit v la dérivée logarithmique de z. Le polynôme $Q(y_1, y_2)$ se factorise comme produit de facteurs linéaires sur C. Soit $u_1, \ldots, u_m$ les dérivées logarithmiques de ces facteurs. Une combinaison linéaire de solutions est une solution, donc les u_i sont des solutions de l'équation de Riccati. Pour tout $g \in G$, comme $g(v) = v$, $g(u_i)$ doit être un des u_j : d'après la proposition 1 et les remarques qui suivent, on en déduit que les u_i sont algébriques de degré au plus m. □

Si les u_i ne sont pas de degré m, alors peut vérifier que le produit P de leurs polynômes minimaux sera de degré m et son coefficient b_{m-1} sera donné par $b_{m-1} = -z'/z$.

Dans **[29]**, il est montré comment, dans de nombreux cas, on peut même se ramener à chercher des solutions rationnelles de $L^{ⓢm}(y)$, ce qui simplifie l'algorithme car la recherche de solutions rationnelles est plus simple que la recherche des solutions exponentielles.

L'équation de Riccati est $u' = -a - a_1u - u^2$. En dérivant la relation $P(u) = 0$ et en remplaçant u' par son expression, on obtient une relation polynomiale de degré $m+1$ pour u. Le reste de la division euclidienne de ce polynôme de degré $m+1$ par P devant être nul, on en déduit les relations suivantes (**[29, 14]**) pour obtenir

« gratuitement » tous les autres coefficients quand on connaît b_{m-1} :

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

On obtient finalement l'algorithme suivant pour calculer des solutions algébriques de l'équation de Riccati :

Pour $m \in \{1, 2, 4, 6, 12\}$:

- Calculer $L^{ⓢm}(y)$
- Chercher si elle admet une solution exponentielle f
- Si oui : poser $b_{m-1} = -f$, calculer les autres coefficients b_i de P en utilisant les relations $(\sharp)_m$, et retourner P
  sinon, continuer avec le m suivant.

Si aucune solution n'est trouvée de cette manière, il n'y a pas de solutions liouvilliennes.

Exercice 7 **([29, 8])**. On considère l'équation différentielle $L(y) = y'' - ry = 0$.

1. Écrire l'équation de Riccati associée.
2. Montrer que $L^{ⓢ2}(y) = y''' - 4ry' - 2r'y''$.
3. On suppose que L admet une solution algébrique de degré 2.
   (a) Montrer que son polynôme minimal est de la forme
   $$P = u^2 - \frac{f'}{f}u + \frac{f''}{2f} - r$$
   où $L^{ⓢ2}(f) = 0$.
   (b) On note $disc(P)$ le discriminant de P. Montrer que $f\, disc(P) = c$ où c est une constante.
   (c) On suppose que $L^{ⓢ2}(f) = 0$ admet une solution $f \in \mathbb{C}(x)$ et que $disc(P) \neq 0$. Montrer que l'équation de Riccati admet une ou deux solutions rationnelles que l'on calculera. En déduire que L admet les solutions liouvilliennes $y = \sqrt{f}e^{\pm \int \sqrt{c}/2f}$.
   (d) Réciproquement, montrer que si l'équation $L(y) = 0$ admet deux solutions exponentielles linéairement indépendantes, alors les matrices du groupe de Galois sont diagonales et $L^{ⓢ2}(y) = 0$ admet une solution rationnelle.
   (e) Application : résoudre l'équation $y'' - \dfrac{c}{16x^2}y = 0$ où $c \in \mathbb{C}$.

Références

[1] Abramov S.A & Kvashenko K.Yu (1991) *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.

[2] Abramov S.A, Bronstein M & Petkovšek M (1995) *On polynomial solutions of linear operators* Proceedings of International Symposium on Symbolic and Algebraic Computation'95, ACM Press, 1995.

[3] Beukers F (1992) *Differential Galois theory* In : From Number Theory to Physics (Ed : Waldschmidt, Moussa, Luck, Itzykson), Springer 1992.

[4] Bronstein M (1992) *Solutions of linear differential equations in their coefficient field* J.Symb.Comp **13**, 1992

[5] Bronstein M (1996) *Symbolic integration*, Springer Verlag.

[6] Bronstein M, Mulders T & Weil J.A (1997) *On Symmetric Powers of Differential Operators* Proceedings of International Symposium on Symbolic and Algebraic Computation'97, ACM Press, 1997.

[7] Cox D., Little J. & O'Shea D. (1992) *Ideals, varieties, and Algorithms* Undergraduate Texts in Math, Springer 1992

[8] Fakler W (1996) *On second order homogeneous linear differential equations with liouvillian solutions* A paraître dans Theoretical Computer Science.

[9] Geddes O, Czapor S.R, Labahn G (1992) *Algorithms for computer algebra* Kluwer Academic Publishers, Dortrecht, Hollande

[10] Hendriks, P. A., Van der Put, M. (1995). *Galois Action on Solutions of a Differential Equation.* J. Symb. Comp. **19**, 559-576.

[11] Hoeij, M. & Weil, J.A (1996) *An algorithm for computing invariants of differential Galois groups* Actes de MEGA'96, À paraître dans Journal of Pure and Applied Algebra.

[12] Kaplanski I (1957) *An introduction to differential Algebra* Hermann

[13] Kolchin, E. R. (1948). *Algebraic matrix groups and the Picard-Vessiot theory of homogeneous ordinary differential equations.* Annals of Math. **49**.

[14] Kovacic, J. (1986). *An algorithm for solving second order linear homogeneous differential equations.* J. Symb. Comp. **2**, 3-43.

[15] Marotte (1898) *Les équations différentielles linéaires et la théorie des groupes* Thèse, Annales École normale supérieure, Gauthier-Villard (1898), Paris

[16] Poole E.G.C (1936) *Introduction to the theory of linear differential equations* Clarendon Press, Oxford, 1936 (réédition : Dover, 1960)

[17] Put, M. van der (1997). *Symbolic analysis of differential equations* in : Some tapas of computer algebra (A. Cohen éditeur), à paraître (Springer).

[18] Ritt J.F (1950) *Differential Algebra* AMS coll. Publications (ou Dover, 1966) 1950

[19] Rosenlicht M (1972) *Integration in finite terms* Amer.Math .Monthly, **79** (1972) pp 963-972.

[20] Singer, M.F. (1981). *Liouvillian solutions of n^{th} order linear differential equations.* Amer. J. Math. **103**, 661-682.

[21] Singer, M.F. (1990). *An outline of differential Galois theory.* In : Computer Algebra and Differential Equations, Ed. E. Tournier, New York : Academic Press.

[22] Singer, M.F. (1997). *Direct and inverse problems in differential Galois theory.* In : Kolchin collected works, à paraître.

[23] Singer, M.F., Ulmer, F. (1993). *Galois Groups of Second and Third Order Linear Differential Equations.* J. Symb. Comp. **16**, 9-36.

[24] Singer, M.F., Ulmer, F. (1993). *Liouvillian and Algebraic Solutions of Second and Third Order Linear Differential Equations.* J. Symb. Comp. **16**, 37-73.

[25] M.F. Singer & F. Ulmer (1996) : *Linear differential equations and products of linear forms.* Actes de MEGA'96, à paraître dans le Journal of Pure and Applied Algebra.

[26] Springer, T.A. (1977). *Invariant theory.* Lecture Notes in Mathematics **585**. Berlin : Springer-Verlag.

[27] Sturmfels, B. (1993). *Algorithms in Invariant Theory.* Texts and Monographs in Symbolic Computation ; Wien ; New York : Springer-Verlag.

[28] Tournier E (éditeur) (1990) *C.A.D.E.(Computer Algebra and Differential Equations)* Academic Press 1989

[29] F. Ulmer & J.A. Weil (1996) : *Note on Kovacic's algorithm,* Journal of Symbolic Computation **22**, 179–200.

[30] Vessiot E (1892) *Sur l'intégration des équations différentielles linéaires* Thèse, Annales de l'école normale supérieure, 1892.

[31] Vessiot E (1915) *Méthodes d'intégration explicites* Encyclopédie du savoir mathématique (Éditions Jacques Gabay, 1992)

[32] Weil J.A, Germa-Péladan A, Ollivier F, & Shih J.A (1995) *Quelques approches algébriques effectives des phénomènes différentiels* Images des Mathématiques 95 (Ed : F. Murat & J.L Colliot-Thelene), Éditions du CNRS, 1995.

Jacques-Arthur Weil, Département de mathématiques, Faculté des sciences, 123 Avenue Albert Thomas, F-87060 Limoges • *E-mail :* `weil@unilim.fr`
Url : `http://medicis.polytechnique.fr/gage/weil.html`