Pablo Le Hénaff

Solutions élémentaires des problèmes d'intégration

Le théorème de Liouville

Mémoire d'initiation à la recherche

Sous la direction de Monsieur **Jimmy Lamboley**

Cycle **p**luridisciplinaire d'**é**tudes **s**upérieures
Troisième année (L3)

Table des matières

Introduction

Certaines fonctions mathématiques sont définies de manière implicite par des équations fonctionnelles, c'est-à-dire des équations dont l'inconnue est une fonction. Toutes les fonctions que nous considérerons seront d'une seule variable réelle ou complexe, et à valeurs réelles ou complexes. Les équations différentielles forment une vaste catégorie d'équations fonctionnelles : ce sont des équations qui mélangent l'inconnue et ses dérivées. L'exemple le plus simple que l'on puisse donner est le calcul de la primitive d'une fonction f continue donnée : il s'agit alors de résoudre l'équation différentielle

$$u' = f \,, \tag{1}$$

où l'inconnue est une fonction u de classe $\mathcal{C}^1$ sur un ouvert connexe non vide. D'autres exemples d'équations différentielles sont les équations différentielles linéaires, c'est-à-dire de la forme

$$g_n u^{(n)} + \cdots + g_1 u' + g_0 u = f \tag{2}$$

où les $g_0, \ldots, g_n$ sont des fonctions suffisamment régulières. Plusieurs approches peuvent être utilisée pour résoudre de telles équations : on peut par exemple rechercher les solutions *analytiques*, c'est-à-dire développables en série entière au voisinage de chaque point. L'équation se traduit alors comme une relation sur les coefficients de la série entière. À moins de reconnaître une série connue, la solution n'est pas obtenue sous une *forme fermée*, c'est-à-dire avec une expression ne faisant pas intervenir de somme infinie, mais uniquement des expressions algébriques et des fonctions de référence. L'analyse et le calcul intégral nous enseigne que les primitives d'une fonction f de la variable réelle, autrement dit les solutions de l'équation (1) sur un domaine de $\mathbb{R}$, sont les fonctions

$$u(t) = \int_{t_0}^{t} f(s)\,\mathrm{d}s \,, \tag{3}$$

et l'analyse complexe développe une théorie apparentée pour les fonctions de la variable complexe. Là encore, la solution n'est pas donnée sous forme close. Enfin, le théorème de Cauchy-Lipschitz affirme l'existence et l'unicité des solutions d'équations différentielles.

Nous avons donc à notre disposition des outils pour traiter ces problèmes de résolution des équations différentielles. En revanche, nous obtenons rarement des solutions sous des formes agréables à manipuler, c'est-à-dire des combinaisons de fonctions élémentaires et d'opérations algébriques. Nous voulons savoir dans quels cas, aussi bien pour la recherche de primitive que pour les équations différentielles linéaires (respectivement les équations (1) et (2)) il existe des solutions sous forme simple, comme nous l'avons décrit, et dans quels cas il est vain de chercher. Par exemple, dans le cas des primitives, on peut à partir de la formule (3) et par intégrations par parties et changements de variables successifs, espérer aboutir à une forme fermée.

Donnons quelques exemples. La *fonction d'erreur*

$$\mathrm{erf}(x) = \int_0^x \mathrm{e}^{-t^2}\,\mathrm{d}t = \sum_{n\geq 0} \frac{(-1)^n}{n!} x^{2n+1}$$

est utilisée intensivement pour le calcul de la fonction de répartition de la loi normale centrée réduite en probabilités, et pourtant nous montrerons qu'elle n'admet pas d'expression simple. Il en est de même pour la fonction *sinus intégral*, définie par

$$\mathrm{si}(x) = \int_0^x \frac{\sin t}{t}\,\mathrm{d}t = \sum_{n\geq 0} (-1)^n \frac{t^{2n}}{2n+1}\,.$$

Remarquons la similarité de la problématique avec la question de la résolubilité des équations polynômiales par radicaux : étant donné une équation polynômiale

$$P(x) = 0\,, \tag{4}$$

peut-on en exprimer les solutions à l'aide des opérations élémentaires $+, -, \times, \div$ et d'exposants rationnels (c'est-à-dire avec des racines n-ièmes, $n \in \mathbb{N}^*$) ? La *théorie de Galois* permet de répondre à cette question. En particulier, une équation polynômiale de degré ≥ 5 n'est pas toujours résoluble par radicaux. Pour aborder le cas des équations différentielles linéaires, il faut faire appel à la *théorie de Galois différentielle.*

Dans ce mémoire, nous allons expliquer comment la théorie développée par Joseph Liouville et ses successeurs répond aux questions que nous nous sommes posées. Cette approche fait appel, dans sa version moderne, à un formalisme algébrique particulier que nous tenterons de justifier, et dont nous exposerons les bases en première partie. Nous supposons le lecteur familier avec la notion de corps, qui sera centrale tout au long de l'étude.

1 Extensions de corps

1.1 Extensions algébriques, extensions transcendantes

Définition 1.1. *Une extension de corps $L : K$ est un corps L qui contient K (éventuellement au sens où il existe un morphisme injectif $K \hookrightarrow L$). Le degré de l'extension $L : K$ est la dimension de L comme K-espace vectoriel.*

Par exemple, $\mathbb{R}$ est une extension de $\mathbb{Q}$, de degré infini. De même, le corps $\mathbb{C}(X)$ des fractions rationnelles à coefficients dans $\mathbb{C}$ est une extension de $\mathbb{C}$. Préciser le corps de base K dans la notation $L : K$ est important. En pratique, comment construit-on des extensions de corps ? Étant donné une extension $L : K$ et un élément $a \in L$, on peut construire la plus petite extension de K, contenue dans L, qui contient a. On la notera $K(a)$: on a « ajouté » au corps K l'élément a. Une telle extension où un unique élément est ajouté est dite monogène. Par exemple, si p est un nombre premier, alors $\mathbb{Q}(\sqrt{p}) = \{a + b\sqrt{p},\ a, b \in \mathbb{Q}\}$. En effet, on montre facilement que le membre de droite est un sous-corps de $\mathbb{R}$, et il contient trivialement $\mathbb{Q}$ et $\sqrt{p}$. On peut également ajouter plusieurs éléments successivement à K, c'est-à-dire construire une extension $K(a_1)(a_2)\ldots(a_n) \subseteq L$ où $a_i \in L$ pour $i \in \{1, \ldots, n\}$. On notera alors $K(a_1)(a_2)\ldots(a_n) = K(a_1, \ldots, a_n)$.

Remarque 1. *Les corps sont naturellement nos objets d'étude, car ils comprennent les 4 opérations qui nous semblent « élémentaires », à savoir l'addition, la soustraction, la* *multiplication et la division. Pourquoi la notion d'extension de corps tient-elle une place importante, à la fois en théorie de Galois et en algèbre différentielle ? Dans la question de la résolubilité par radicaux d'une équation polynômiale, c'est la « simplicité » de l'extension de corps qui contient les racines qui correspond à la « simplicité » de celles-ci (quels éléments doit-où rajouter au corps des rationnels pour obtenir le plus petit corps contenant les solutions de l'équation ?).*

Définition 1.2. *Si $L : K$ est une extension de corps, on dit qu'un élément $a \in L$ est algébrique sur K s'il est racine d'un polynôme non nul à coefficients dans K. Dans le cas contraire, on dira que a est transcendant sur K. Si a est algébrique sur K, on notera* $\mathrm{Pol}_K(a)$ *le polynôme unitaire générateur de l'idéal des polynômes de $K[X]$ annulateurs de a. Une extension $K(a_1, \ldots, a_n) : K$ est dite algébrique si $a_1, \ldots, a_n$ sont algébriques sur K.*

Par exemple, l'extension $\mathbb{Q}(\sqrt{p}) : \mathbb{Q}$ est algébrique, de base $(1, \sqrt{p})$ sur $\mathbb{Q}$, et $\mathrm{Pol}_{\mathbb{Q}}(\sqrt{p}) = X^2 - p \in \mathbb{Q}[X]$. Le nombre $(\sqrt{2}+1)^{2/5}$ appartient à l'extension $\mathbb{Q}(a_1, a_2)$ où $a_1 = \sqrt{2}$ et $a_2 = (a_1+1)^{2/5}$ sont algébriques respectivement sur $\mathbb{Q}$ et $\mathbb{Q}(a_1)$ avec $\mathrm{Pol}_{\mathbb{Q}}(a_1) = X^2 - 2$ et $\mathrm{Pol}_{\mathbb{Q}(a_1)}(a_2) = X^5 - (a_1+1)^2 \in (\mathbb{Q}(a_1))[X]$. En réalité, le théorème de l'élément primitif assure que cette extension est monogène.

Proposition 1. *Si a est algébrique sur K, alors tout élément de $K(a)$ s'écrit de manière unique sous la forme*

$$\sum_{i=0}^{d-1} k_i a^i \quad \text{où } d = \deg \mathrm{Pol}_K(a) \text{ et } (k_i)_i \in K^d \,. \tag{5}$$

En particulier, le degré de $K(a) : K$ est fini et vaut le degré de $\mathrm{Pol}_K(a)$*, et* $(1, a, \ldots, a^{d-1})$ *est une base pour $K(a)$ sur le corps K.*

Si a est transcendant sur K, alors $K(a)$ est isomorphe au corps des fractions rationnelles à coefficients dans K, via

$$\varphi_a : \left\{ \begin{array}{rcl} K(X) & \longrightarrow & K(a) \\ T & \longmapsto & T(a) \end{array} \right. .$$

Une extension transcendante est donc de degré infini.

Ainsi, dans le cas où $a \in L$ est transcendant sur K, on pourra considérer l'unique décomposition en éléments simples d'un élément $\alpha = \varphi_a(T)$ de $K(a)$. En outre, dans une extension algébrique, l'égalité de deux polynômes en l'élément ajouté permettra l'identification de leurs coefficients (par unicité de l'écriture sous forme de polynôme) !

1.2 Corps et extensions différentiels

Définition 1.3. *Un corps K est un corps différentiel s'il est muni d'une dérivation, c'est-à-dire une application $\partial : K \longrightarrow K$ telle que*

$$\forall k_1, k_2 \in K,\ \partial(k_1 + k_2) = \partial(k_1) + \partial(k_2) \quad \text{et} \quad \partial(k_1 k_2) = \partial(k_1) k_2 + k_1\, \partial(k_2) \,. \tag{6}$$

Le sous-corps $\mathrm{Con}(K) = \{k \in K,\ \partial(k) = 0\}$ *de* K *est un sous corps, appelé le* sous-corps des constantes. *Une extension* $L : K$ *est une extension différentielle si* L *est un corps différentiel dont la dérivation prolonge celle de* K *(c'est-à-dire que les deux dérivations coïncident sur* K*), et si* $\mathrm{Con}(L) = \mathrm{Con}(K)$.

Remarque 2. *La seconde égalité de la condition* (6) *s'appelle la* règle de Leibniz.

Par exemple, le corps[1] $\mathcal{M}(\Omega)$ des fonctions méromorphes sur un ouvert Ω de $\mathbb{C}$, muni de la dérivation au sens complexe, est un corps différentiel, dont le corps des constantes est (isomorphe à) $\mathbb{C}$. $\mathcal{M}(\Omega)$ est une extension différentielle de $\mathbb{C}(X)$, si nous identifions chaque fractions rationnelle à sa fonction méromorphe associée, restreinte à Ω.

Proposition 2. *Une dérivation sur* K *vérifie nécessairement les propriétés suivantes :*

$$\partial(0) = \partial(1) = 0 \quad \text{et} \quad \forall k_1 \in K,\, k_2 \in K^*,\ \partial\left(\frac{k_1}{k_2}\right) = \frac{\partial(k_1)k_2 - k_1\,\partial(k_2)}{k_2^2}\,.$$

De plus, la dérivation logarithmique ℓ *induite par* ∂*, définie par*

$$\forall k \in K^*, \quad \ell(k) = \frac{\partial(k)}{k}$$

vérifie

$$\forall k_1, k_2 \in K^*, \quad \ell(k_1k_2) = \ell(k_1) + \ell(k_2) \quad \text{et} \quad \ell\left(\frac{k_1}{k_2}\right) = \ell(k_1) - \ell(k_2)\,. \tag{7}$$

Dans la suite, il nous arrivera de noter plus classiquement $x' = \partial(x)$.

1.3 Fonctions et extensions élémentaires

Nous désirons formaliser le concept de « fonction élémentaire » à partir du cadre que nous avons donné précédemment. Nous voulons certainement considérer comme élémentaires les fonctions rationnelles, ainsi que les fonctions obtenues à partir de ces fonctions rationnelles par compositions successives avec les fonctions exponentielle et logarithme. La bonne définition d'une extension élémentaire est la suivante :

Définition 1.4. *Soit* $L : K$ *une extension de corps différentiels et* $f \in L^*$*. L'extension différentielle* $K(f) : K$ *est une extension élémentaire si* f *vérifie l'une des trois hypothèses suivantes :*

(a) f *est algébrique sur* K*, ou bien*

(b) $f'/f \in K$*, ou bien*

(c) $f' = k'/k$ *pour un* $k \in K$.

1. Les fonctions méromorphes forment bien un corps (voir un cours d'analyse complexe). En particulier, on peut définir l'inverse d'une fonction méromorphe avec une fonction méromorphe, car les zéros d'une fonction méromorphe sont isolés. Ce corps peut être vu comme le corps des fractions de l'anneau des fonctions holomorphes.

Dans le cas (b)*, f est une exponentielle d'un élément de K, et dans le cas* (c)*, f est un logarithme d'un élément de K.*

Si $n \geq 2$ et $f_1, \ldots, f_n \in L$, par récurrence, l'extension différentielle $K(f_1, \ldots, f_n) : K$ est dite élémentaire si $K(f_1, \ldots, f_n) : K(f_1, \ldots, f_{n-1})$ et $K(f_1, \ldots, f_{n-1}) : K$ sont élémentaires.

Les appellations « exponentielle » et « logarithme » sont données en référence aux formules $(\exp f)' = f' \exp f$ et $(\ln f)' = f'/f$, et ces notions coïncident avec les notions classiques d'exponentielle et de logarithme dans le cas $L = \mathcal{M}(\Omega)$, qui nous intéressera par la suite. Notons que dans les cas (b) et (c), on peut supposer que f est transcendant sur K, puisque sinon le cas (a) s'applique. Par exemple, la fonction $x \mapsto \exp(\frac{1}{2} \ln x) = \sqrt{x}$ est certes une exponentielle d'un élément d'une extension logarithmique de $\mathbb{R}(X)$, mais cette fonction est surtout algébrique sur $\mathbb{R}(X)$.

En pratique, qu'est-ce que le corps K ? Il s'agit en fait d'un corps différentiel de fonctions élémentaires qui contient la fonction dont nous voulons montrer qu'elle n'admet pas de primitive. Par exemple, dans le cas de la fonction d'erreur, nous considérerons le corps $K = \mathbb{C}(X)(\exp -X^2) \simeq \mathbb{C}(X, \exp(-X^2))$, la fonction $\exp(-X^2)$ étant transcendante sur les fractions rationnelles.

Définition 1.5. *Une fonction élémentaire est un élément d'une extension différentielle élémentaire du corps $\mathbb{C}(X)$.*

Exemple 1. *Soit $\mathbb{K} = \mathbb{R}(X)$, et f la fonction élémentaire de la variable réelle définie par*

$$f(x) = \frac{x \sin x}{\sqrt{1 + x^2}} .$$

Posons

$$a_1(x) = i, \quad a_2(x) = \exp(a_1 x), \quad a_3(x) = \exp(-a_1 x), \quad a_4(x) = \sqrt{1 + x^2} .$$

Alors f est un élément de l'extension $\mathbb{K}(a_1, a_2, a_3, a_4)$, où $a_1 = i$ est algébrique sur $\mathbb{R}$, donc sur $\mathbb{R}(X)$, a_2 est l'exponentielle de $x \mapsto a_1 x \in \mathbb{K}(a_1)$ et a_3 celle de $x \mapsto -a_1 x$, et a_4 est algébrique sur $\mathbb{K}$, donc sur $\mathbb{K}(a_1, a_2, a_3)$. Finalement, l'extension $\mathbb{K}(a_1, a_2, a_3, a_4) : \mathbb{K}$ est élémentaire, et

$$f(x) = x \frac{a_2(x) - a_3(x)}{2 a_1(x) a_4(x)} \in \mathbb{K}(a_1, a_2, a_3, a_4) .$$

Donc f est bien élémentaire au sens que nous avons donné plus haut.

2 Le théorème de Liouville

2.1 Énoncé

Nous énonçons enfin le théorème principal, dont la première version est dûe à Joseph Liouville (1809 - 1882).

Théorème 1 (Théorème de Liouville)**.** *Soit K un corps différentiel, $L : K$ une extension différentielle. On se donne $f \in K$. f admet une primitive dans une extension différentielle élémentaire de K (contenue dans L) si et seulement si f est de la forme suivante :*

$$f = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}\,, \quad n \geq 0,\ v, u_1, \ldots, u_n \in K^*,\ c_1, \ldots, c_n \in \mathrm{Con}(K)\,. \tag{8}$$

Remarque 3. *Ce théorème donne une condition nécessaire et suffisante pour qu'une fonction donnée admette une primitive élémentaire, au sens que nous avons donné plus haut. Ce n'est pas une méthode pour trouver une primitive à une fonction donnée : on l'utilisera pour montrer qu'une fonction* ne peut pas avoir *de primitive élémentaire, mais nous ne pouvons pas nous en servir pour déterminer une primitive élémentaire à une fonction qui pourrait en admettre une. L'*algorithme de Risch *permet de trouver de telles primitives ; il est implémenté dans la plupart des logiciels de calcul formel.*

Nous voulons donc montrer que les seules fonctions qui admettent une primitive élémentaire sur K sont celles qui ont la forme très particulière de l'identité (8).

2.2 Démonstration

La condition suffisante est immédiate en remarquant que

$$f = \partial\left(v + \sum_{i=1}^{n} c_i \log u_i\right).$$

La condition nécessaire est une simple généralisation par récurrence de la proposition suivante :

Proposition 3. *Soit K un corps différentiel, $f \in K$ et $K(t) : K$ une extension élémentaire de K (ie t est algébrique, transcendant exponentiel ou transcendant logarithmique sur K). On suppose qu'il existe $u \in K(t)$, $c_1, \ldots, c_n \in \mathrm{Con}\,K(t) = \mathrm{Con}\,K$ et $u_1, \ldots, u_n \in K(t)^*$ tels que*

$$f = u' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}\,. \tag{9}$$

Alors il existe $v \in K$, $d_1, \ldots, d_m \in \mathrm{Con}\,K$ et $v_1, \ldots, v_m \in K^*$ tels que

$$f = v' + \sum_{i=1}^{m} d_i \frac{v_i'}{v_i}\,.$$

Dans la suite, nous démontrons donc cette proposition en utilisant les mêmes notations que l'énoncé.

2.2.1 Cas transcendant exponentiel ou logarithmique

Dans cette section, nous supposons que l'extension différentielle $K(t) : K$ est transcendante sur K. Les éléments de $K(t)$ sont des fractions rationnelles en t à coefficients dans K, par la proposition 1. Si nous considérons la dérivée logarithmique d'un tel élément, grâce aux propriétés données dans la proposition 2, nous pouvons nous ramener à l'étude de la dérivée logarithmique des seuls polynômes en t (que nous notons $K[t]$) ; nous pouvons mêmes supposer ceux-ci *irréductibles* et *unitaires*. Dans la suite de la preuve, nous aurons besoin de savoir dans quel cas la dérivée logarithmique d'un polynôme en t, irréductible et unitaire, est elle-même un polynôme en t ; nous aurons donc besoin de répondre à la question : *dans quel cas un polynôme en t, irréductible et unitaire, divise-t-il sa dérivée ?*

Soit donc $g \in K[t]$ non constant, mettons $g = P(t)$ où $P = \sum_{i=0}^{n} \alpha_i X^i$, $n \geq 1$ et $\alpha_n \neq 0$. Alors on a

$$\begin{aligned} g' &= \alpha_0' + \sum_{i=1}^{n} (\alpha_i' t^i + \alpha_i i t' t^{i-1}) \\ &= \sum_{i=0}^{n} \alpha_i' t^i + t' \sum_{i=1}^{n} \alpha_i i t^{i-1} = \alpha_n' t^n + \sum_{i=0}^{n-1} (\alpha_i' + (i+1) t' \alpha_{i+1}) t^i \\ &= \partial P(t) + t' P'(t) \,, \end{aligned} \tag{10}$$

où on a noté $\partial P = \sum_{i=0}^{n} \alpha_i' X^i$ le polynôme dont les coefficients sont les dérivées des coefficients de P, et P' est le polynôme dérivé usuel. On en déduit que

$$P(t)' \text{ est un polynôme en } t, \text{ de degré} \leq \text{au degré de } P(t). \tag{11}$$

Examinons les deux cas particuliers où t est un logarithme ou une exponentielle d'un élément $a \in K^*$.

(a) Supposons que t est le logarithme de a : $t' = a'/a \in K$. Si $\alpha_n \notin \operatorname{Con} K$, le degré de $P(t)'$ en t est égal au degré de $P(t)$. Dans le cas contraire (c'est le cas lorsque $P(t)$ est unitaire), supposons par l'absurde que $\alpha_{n-1}' + n t' \alpha_n = 0$: puisque $\alpha_n \in \operatorname{Con} K$, cela donne $(\alpha_{n-1} + n\alpha_n t)' = 0$, d'où $\alpha_{n-1} + n\alpha_n t \in \operatorname{Con} K \subseteq K$. Finalement, $t \in K$, ce qui est absurde puisque t est transcendant sur K. Ainsi, $\alpha_{n-1}' + n t' \alpha_n \neq 0$ et

$$\text{le degré de } P(t)' \text{ est immédiatement inférieur à celui de } P(t). \tag{12}$$

Si $P(t)$ est *unitaire*, nous avons donc le résultat suivant :

$$P(t) \text{ divise } P(t)' \quad \Longleftrightarrow \quad P(t) = 1,\ P(t)' = 0\,. \tag{13}$$

De plus, par l'affirmation (12), nous avons

$$P(t)' \in K \quad \Longleftrightarrow \quad P(t) = ct + b,\ c \in \operatorname{Con} K,\ b \in K\,. \tag{14}$$

(b) Supposons maintenant que t est l'exponentielle de a : $t' = at$. Nous allons montrer que

$$P(t) \text{ divise } P(t)',\ P \text{ irréductible et unitaire} \quad \Longleftrightarrow \quad P(t) = t\,. \tag{15}$$

En utilisant (11), on voit que $P(t)$ divise $P(t)'$ si et seulement s'il existe $\lambda \in K$ tel que $P(t)' = \lambda P(t)$. Supposons que ce soit le cas, et que P soit unitaire et irréductible ; cela fournit par identification du coefficient dominant (en utilisant (10)) $\lambda = na$. Supposons qu'il existe $0 \leq j \leq n-1$ tel que $\alpha_j \neq 0$. On aurait alors, par identification également,

$$0 = (n-j)\frac{t'}{t}\alpha_j - \alpha_j' \quad \text{donc} \quad \frac{(n-j)t' t^{n-j-1}\alpha_j - t^{n-j}\alpha_j'}{\alpha_j^2} = \left(\frac{t^{n-j}}{\alpha_j}\right)' = 0\,,$$

donc t^{n-j}/α_j serait constant, donc dans K, ce qui contredit la transcendance de t. Ainsi, $P(t) = t^n$ mais P étant irréductible, on a nécessairement $P(t) = t$.

Maintenant que nous avons établi ces quelques résultats, nous pouvons passer à la démonstration proprement dite, dans les cas transcendant logarithmique et exponentiel. L'égalité (9) se réécrit

$$K \ni f = u' + \sum_{i=1}^{n} c_i\,\ell(u_i) = u' + \sum_{j=1}^{m} k_j\,\ell(a_j) + \sum_{j=1}^{p} \tilde{k}_j\,\ell(w_j) \tag{16}$$

où les $\tilde{k}_j$, k_j sont des constantes ($\operatorname{Con} K$ est un corps), les a_j des élements de K,les w_j sont des polynômes en t distincts, non constants, irréductibles et unitaires, et où l'on a fait une utilisation cruciale de la propriété (7). On peut également décomposer la fraction rationnelle u en éléments simples :

$$u = r + \sum_{i,j} \frac{p_{i,j}}{q_i^j}\,, \quad p_{i,j},\ q_i \text{ des polynômes irréductibles en } t \text{ tels que } \deg p_{i,j} < \deg q_i\,.$$

On en déduit que u' est de la forme

$$u' = r' + \sum_{i,j}\left(\frac{p_{i,j}'}{q_i^j} - j\,\frac{p_{i,j}}{q_i^{j+1}}\right)\,,$$

et comme on peut supposer que $p_{i,j}$ et q_i sont premiers entre eux, on voit qu'un terme $p_{i,j}/q_i^{j+1}$ ne peut pas être compensé par un élément de la somme des dérivées logarithmique des w_j dans (16) (nous utilisons le fait que la décomposition en éléments simples d'une fraction rationnelle est unique), et finalement u', donc u, ne peut être qu'un polynôme ($u = r$). Il nous reste finalement

$$\sum_{j=1}^{p} \tilde{k}_j\,\ell(w_j) = f - \sum_{j=1}^{m} k_j\,\ell(a_j) - r' \in K[t]\,,$$

ainsi w_j divise w_j' pour tout j, ceci par unicité de la décomposition en éléments simples d'une fraction rationnelle. Reprenant les résultats précédents, si l'on s'intéresse à chaque cas logarithmique ou exponentiel séparément :

(a) Si t est le logarithme de a, d'après (13), il n'y a aucun polynôme non constant unitaire irréductible w_j, et on obtient $f = r' + \sum k_j\, \ell(a_j)$, d'où $r' \in K$, puis par (14), $r = ct + b$ et finalement

$$f = b' + c\,\ell(a) + \sum k_j\, \ell(a_j)\,,$$

ce qui est bien la forme voulue.

(b) Si t est l'exponentielle de a, nous obtenons

$$f = r' + \sum_{j=1}^{m} k_j\, \ell(a_j) + k\frac{t'}{t} = r' + \sum_{j=1}^{m} k_j\, \ell(a_j) + ka'.$$

Donc r est un polynôme en t de degré au plus 1, donc la forme $f = (r + ka)' + \sum_{j=1}^{m} k_j\, \ell(a_j)$ est celle que nous recherchons. Cela achève la preuve des cas transcendants logarithmiques et exponentiels.

2.2.2 Cas algébrique

Nous voulons montrer que la proposition 3 est vérifiée dans le cas où t est algébrique sur K. Il existe plusieurs variantes de cette démonstration, toutes étant basées sur les notions de norme et de trace, qui peuvent être définies de manière équivalente avec la théorie de Galois, ou bien avec des concepts plus simples d'algèbre linéaire. Dans le deuxième cas toutefois, la démonstration est moins aisée et plus longue ; c'est cette manière de procéder que nous exposons ici.

On se donne donc une extension $K(t) : K$ différentielle algébrique, de degré n. On choisit une base $(e_1, \ldots, e_n)$ de $K(t)$ comme K-espace vectoriel. À chaque $x \in K(t)$, on peut associer l'application K-linéaire $m_x : K(t) \longrightarrow K(t)$, $y \longmapsto xy$ de multiplication par x (les corps que nous considérons sont tous commutatifs).

Cette association est injective : clairement, si $m_{x_1} = m_{x_2}$, alors $x_1 = x_2$. De plus, $m_{x_1+x_2} = m_{x_1} + m_{x_2}$ et $m_{\lambda x} = \lambda m_x$ pour $\lambda \in K$. Nous avons donc défini un plongement linéaire $m : K(t) \hookrightarrow \mathcal{L}_K(K(t)) \simeq \mathcal{M}_n(K)$, ce qui permet d'identifier $K(t)$ à un sous-espace vectoriel de $\mathcal{M}_n(K)$.

Définition 2.1. *On appelle respectivement* ***norme*** *et* ***trace*** *de $x \in K(t)$ les quantités*

$$\mathrm{N}(x) = \det(m_x) \quad \textit{et} \quad \mathrm{tr}(x) = \mathrm{tr}(m_x)\,.$$

Proposition 4. *(a)* $\mathrm{N}(x),\ \mathrm{tr}(x) \in K$,

(b) Si $x \in K$, $\mathrm{N}(x) = x^n$ et $\mathrm{tr}(x) = nx$,

(c) Si $x, y \in K(t)$, $\mathrm{N}(xy) = \mathrm{N}(x)\,\mathrm{N}(y)$,

(d) $\mathrm{tr} : K(t) \longrightarrow K(t)$ est K-linéaire.

Proposition 5. *Pour $x \in K(t)$,*

$$\mathrm{tr}\left(\frac{\partial(x)}{x}\right) = \frac{\partial(\mathrm{N}(x))}{\mathrm{N}(x)}\,,$$

autrement dit

$$\boxed{\operatorname{tr}(\ell(x)) = \ell(\mathrm{N}(x))}.$$

Lemme 1. *Soit (K, ∂) un corps différentiel. On note encore ∂ la dérivation sur les matrices de $\mathcal{M}_n(K)$ induite par la dérivation de K : $\partial(M)_{ij} = \partial(M_{ij})$ pour $M \in \mathcal{M}_n(K)$ et $1 \leq i, j \leq n$ (il s'agit bien d'une dérivation sur l'anneau des matrices à coefficients dans K). Alors pour toute matrice $A \in \mathcal{M}_n(K)$, on a*

$$\partial(\det A) = \operatorname{tr}((\operatorname{com} A)^t\, \partial(A))\,,$$

où $\operatorname{com}(A)$ *désigne la comatrice de A.*

Démonstration. Nous allons montrer une version plus analytique, car la version générale est extrêmement longue et calculatoire. Supposons que K soit un corps de fonctions dérivables par rapport à t. Une matrice $A \in \mathcal{M}_n(K)$ est donc une fonction matricielle de t dérivable. Il s'agit d'un exercice classique de montrer que $\nabla \det(A) = \operatorname{com}(A)$ pour une matrice $A \in \mathcal{M}_n(K)$ (autrement dit $\mathrm{d} \det_A(H) = \langle \operatorname{com}(A), H \rangle = \operatorname{tr}((\operatorname{com} A)^t H)$ avec $\langle \cdot, \cdot \rangle$ le produit scalaire canonique sur les matrices). Ainsi, par composition, on a

$$\frac{\mathrm{d}(\det A)}{\mathrm{d}t} = \langle \nabla \det(A), \frac{\mathrm{d}A}{\mathrm{d}t} \rangle = \operatorname{tr}\left((\operatorname{com} A)^t \frac{\mathrm{d}A}{\mathrm{d}t} \right) . \qquad \square$$

Une fois la proposition 5 démontrée, la preuve du cas algébrique de la proposition 3 est courte. En effet, partant de l'égalité (9), il suffit d'appliquer la trace pour obtenir :

$$nf = \partial(\operatorname{tr} u) + \sum_{i=1}^{n} c_i \operatorname{tr}\left(\frac{\partial(u_i)}{u_i} \right) = \partial(\operatorname{tr} u) + \sum_{i=1}^{n} c_i \frac{\mathrm{N}(u_i)}{u_i} .$$

On a désigné par n le degré de l'extension $K(t) : K$ dans cette égalité. Il suffit de diviser par $n \in \operatorname{Con} K$ pour obtenir la forme voulue, ce qui achève la démonstration du cas algébrique.

3 Applications

3.1 La fonction d'erreur n'est pas élémentaire

Nous commençons par un lemme sur l'exponentielle d'une fraction rationnelle :

Lemme 2. *Soit $f \in \mathbb{C}(X)$ une fraction rationnelle. Alors $\exp f$ est transcendante si et seulement si f n'est pas constante.*

Un corollaire important du théorème de Liouville permet de traiter le cas de la fonction d'erreur.

Corollaire 1.1. *Soient f, g deux fractions rationnelles avec g non constante. Alors la fonction $f \exp g$ admet une primitive élémentaire si et seulement s'il existe une fraction rationnelle a telle que $f = a' + ag'$.*

Démonstration. Condition suffisante : écrire $f \exp g = a' \exp g + ag' \exp g = (a \exp g)'$.

Condition nécessaire. Notons $t = \exp g$ qui est transcendant sur les fractions rationnelles par l'hypothèse et le lemme. Supposons que ft admet une primitive élémentaire : on peut écrire par application du théorème de Liouville :

$$ft = u' + \sum_{i=1}^{n} c_i \, \ell(u_i) \, ,$$

où les c_i sont des constantes (donc des nombres complexes) et u, u_i sont des fractions rationnelles en X et en t. En appliquant comme précédemment les propriétés de ℓ (ie supposer que les u_i sont des polynômes irréductibles distincts et u un polynôme en t), et en utilisant l'unicité de la décomposition en éléments simples et le résultat (15), nous voyons que finalement $ft = u' + cg'$ pour un c nombre complexe, puis u est de degré 1 en t avec un coefficient dominant non constant : $u = at+b$. Finalement, $ft = a't + ag't + b' + cg'$ et en identifiant les termes en t, il vient $f = a' + ag'$. $\square$

On en déduit immédiatement que $\exp(-X^2)$ n'admet pas de primitive élémentaire, car l'égalité $1 = a' - 2aX$ est impossible (a est nécessairement un polynôme, puis raisonner sur les degrés). Donc la fonction d'erreur n'est pas élémentaire !

3.2 Le sinus intégral

On montre d'une manière analogue que la fonction sinus intégral $\int \sin(x)/x \, \mathrm{d}x$ n'est pas élémentaire.