Primitives élémentaires de fonctions élémentaires

Ahmed Moussaoui et Ramanujan Santharoubane
Exposé de maîtrise encadré par François Loeser

Septembre 2008

Table des matières

Avant de commencer notre étude, nous remercions sincèrement François Loeser pour son encadrement ainsi que sa disponibilité.

Introduction

En analyse, on travaille généralement avec des fonctions que l'on définit par des «formules explicites» à partir de fonctions usuelles (fraction rationnelle, exponentielle, logarithme) et en utilisant les opérations de somme, produit, quotient et composition. Lorsque l'on dérive de telles fonctions, on a toujours une expression explicite. En revanche, la recherche d'une formule explicite d'une primitive devient plus laborieuse. En effet, toute fonction continue admet des primitives, il est donc naturel de vouloir en calculer une explicitement. On a à notre disposition des techniques de calcul (intégration par partie, décomposition en élément simple, changement de variable, etc ...) , mais malheuresement elles ne permettent pas toujours d'aboutir. On peut donc se demander s'il est toujours possible de calculer une primitive. Si oui, existe-t-il un algorithme de calcul qui permet ce calcul ?

Pour cela, nous introduirons le concept de corps différentiel qui permet d'aborder le problème d'un point de vue totalement algébrique en oubliant même la notion de fonction. On pourra alors définir précisément les fonctions qui ont une expression explicite que nous appellerons fonctions élémentaires. Nous étudierons alors une partie de la théorie algébrique des équations différentielles avec le théorème de Picard-Vessiot. Nous nous intéresserons par la suite au théorème de Liouville-Ostrowski, qui indique la forme des fonctions admettant une primitive élémentaire. Enfin, nous présenterons l'algorithme de Risch qui permet de tester, dans un cadre restreint, si une fonction élémentaire admet ou pas une primitive élémentaire et le cas échéant, la calculer.

1 Corps différentiels

On introduit dans cette partie les notions de corps différentiel et des morphismes associés. Ceci permettra de formaliser dans la suite le problème algébriquement.

Définition 1.1 *Soit A un anneau commutatif unitaire. Une dérivation sur A est un homomorphisme de groupes abéliens $D : A \longrightarrow A$ qui vérifie :*

$$\forall a, b \in A, D(ab) = aD(b) + bD(a)\,.$$

Un anneau différentiel (A, D) est la donnée d'un anneau A et d'une dérivation D de A. Lorsque A un corps, on parle alors de corps différentiel. On notera $D(a) = a'$ et si $n \geqslant 0$, $D^n(a) = a^{(n)}$.

Remarque 1.1 Cette notion ne fait que formaliser le concept classique de dérivation, de ce fait les exemples ne manquent pas :

- $\mathbb{K}(X)$ muni de la dérivation usuelle est un corps différentiel (où $\mathbb{K}$ est un corps)
- l'anneau $C^\infty(\mathbb{R}, \mathbb{R})$ des fonctions muni de la dérivation usuelle est un anneau différentiel.

On peut aussi démontrer très facilement que la dérivation sur un corps (ou un anneau) différentiel renvoie à des formules classiques. En effet, si (A, D) est un anneau différentiel, alors :

(i) $D(1) = 0$

(ii) $\forall a \in A, \forall n \geqslant 1, D(a^n) = na^{n-1}D(a)$

(iii) $\forall a, b \in A, \forall n \geqslant 1, D^n(ab) = \sum_{k=0}^{n} C_n^k D^k(a) D^{n-k}(b)$

(iv) $\forall a \in A, \forall b \in A^\times, D(\frac{a}{b}) = \frac{bD(a)-aD(b)}{b^2}$, en particulier : $D(\frac{1}{b}) = \frac{-D(b)}{b^2}$.

Proposition 1.1 *Soit (K, D) un corps différentiel. L'ensemble $C = \{x \in K, D(x) = 0\}$ est un sous-corps de K. On l'appelle corps des constantes. L'application D devient ainsi un endomorphisme de C-espace vectoriel. (Cette notion peut être aussi considérée sur un anneau différentiel, les constantes forment alors un sous-anneau).*

Exemple 1.1 Cette notion est toute aussi classique. On pense naturellement à $\mathbb{K}(X)$ (muni de la dérivation usuelle) de corps des constantes $\mathbb{K}$, lorsque $\mathbb{K}$ est de caractéristique nulle. En revanche, si $\mathbb{K}$ est de caractéristique p , le sous corps des constantes de $\mathbb{K}(X)$ est $\mathbb{K}(X^p)$.

Définition 1.2 *Soient $(K_1, D_1), (K_2, D_2)$ deux corps différentiels et $f : K_1 \longrightarrow K_2$ un morphisme d'anneaux. On dit que f est un morphisme d'anneaux différentiels si et seulement si :*

$$f \circ D_1 = D_2 \circ f \, ,$$

et on note $f : (K_1, D_1) \longrightarrow (K_2, D_2)$.

Définition 1.3 *Soient (K, D), (L, D') deux corps différentiel tels que K est un sous-corps de L. On dit que L est une extension différentielle de K si et seulement si D et D' coïncident sur K. On pourra noter (L, D) au lieu de $(L, D^{'})$.*

Définition 1.4 *Soit (A, D) un anneau différentiel et I un idéal de A. Lorsque I est stable par dérivation, on dit que I est un idéal différentiel.*

Exemple 1.2 Si f est un morphisme d'anneaux différentiels, alors son noyau est un idéal différentiel.

Réciproquement, si (A, D_A) est un anneau différentiel, I un idéal différentiel de A alors on peut munir le quotient $B = A/I$ d'une structure d'anneau différentiel telle que la projection canonique $\pi : A \twoheadrightarrow B$ soit un morphisme d'anneaux différentiels. En effet, le morphisme de groupes abéliens $\pi \circ D_A : A \to B$ est nul sur I, qui est un sous groupe de A. Il existe donc un unique morphisme de groupes abéliens D_B qui relève D_A à B. On vérifie sans difficultés que D_B est bien une dérivation sur le quotient $B = A/I$.

2 Équations différentielles

2.1 Résultats sur les équations différentielles linéaires homogènes

Définition 2.1 *Soit (K, D) un corps différentiel. Une équation différentielle linéaire homogène sur K est une équation de la forme :*

$$Y^{'} = AY \, ,$$

avec $A \in \mathcal{M}_n(K)$.

Remarque 2.1 Une équation de la forme : $y^n + a_{n-1}y^{(n-1)} + ... + a_0 y = 0 \quad (E)$ (avec pour tout $i \in [\![0, n-1]\!]$, $a_i \in K$) est bien une équation différentielle linéaire homogène car si l'on pose :

$$A = \begin{pmatrix} 0 & 1 & 0 & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-1} \end{pmatrix} \text{ et } Y = \begin{pmatrix} y \\ y' \\ \vdots \\ y^{(n-1)} \end{pmatrix}$$

On a bien : y solution de $(E) \iff Y$ solution de : $Y' = AY$.

Théorème 2.1 *Soit $n \geqslant 1$ un entier. Soit (K, D) un corps différentiel de corps des constantes C et $(E) : Y' = AY$, avec $A \in \mathcal{M}_n(K)$, une équation différentielle. L'ensemble des solutions de (E) est un C-espace vectoriel de dimension au plus n.*

Démonstration 2.1 Soit V l'ensemble des solutions de (E) sur K^n.
On munit, bien entendu, V d' une structure de C-espace vectoriel. Montrons qu'il est de dimension au plus n. Pour ce faire montrons que si $(Y_1, ..., Y_m)$ sont m solutions libres sur C alors elles le sont sur K.
Procédons par récurrence sur m :
Si $m = 1$: c'est trivial.
Supposons $m \geqslant 2$: par hypothèse de récurrence $(Y_1, ..., Y_{m-1})$ sont libres sur K. Supposons par l'absurde que l'on ait une relation de dépendance linéaire non triviale sur K entre les $Y_1, ..., Y_m$:

$$a_1 Y_1 + ... + a_m Y_m = 0\,,$$

où nécessairement $a_m \neq 0$. De sorte qu'en divisant par a_m on peut se ramener à $a_m = 1$. Si l'on dérive cette relation on obtient :

$$(a_1' Y_1 + ... + a_{m-1}' Y_{m-1}) + (a_1 Y_1' + ... + a_{m-1} Y_{m-1}' + Y_m') = 0\,,$$

or

$$\forall i \in [\![1, m]\!], Y_i' = AY_i\,,$$

d'où :

$$a_1 Y_1' + ... + a_{m-1} Y_{m-1}' + Y_m' = A(a_1 Y_1 + ... + Y_m) = 0\,,$$

et donc :

$$a_1' Y_1 + ... + a_{m-1}' Y_{m-1} = 0\,,$$

d'où par hypothèse de récurrence :

$$a_1' = ... = a_{m-1}' = 0\,,$$

(car les $m-1$ premiers vecteurs sont libres sur K).

Or cela implique que pour tout $i \in [\![1, m]\!], a_i \in C$. De ce fait, on a une relation de dépendance linéaire entre $Y_1, ..., Y_m$ sur C, ce qui contredit l'hypothèse initiale. En résumé la dimension de V sur C est au plus la dimension de K^n sur K c'est à dire n. □

2.2 Extensions de Picard-Vessiot

Étant donné un polynôme, nous savons construire son corps de décomposition qui est le plus petit corps qui contient ses racines. Autrement dit, c'est le plus petit corps à isomorphisme près engendré par ses racines. Dans ce qui suit, nous allons construire l'analogue pour une équation différentielle linéaire homogène : pour une telle équation d'ordre n sur un corps différentiel K, nous construisons une extension minimale qui contient n solutions linéairement indépendantes.

Définition 2.2 *Soit (K, D) un corps différentiel de corps des constantes C. On suppose C algébriquement clos et de caractéristique 0. Soit $(E) : Y' = AY$, avec $A \in \mathcal{M}_n(K)$, une équation différentielle linéaire homogène sur K. Soit (L, D) une extension différentielle de K. Par définition, L est une extension de Picard-Vessiot pour (E) si et seulement si :*

- *le corps des constantes de L est C*
- *(E) admet une base de solutions $(Y_1, ..., Y_n)$ dans L^n*
- *L est engendré par les coefficients $Y_{i,j}$ de cette base.*

Théorème 2.2 *Soit (K, D) un corps différentiel. Toute équation différentielle linéaire homogène sur K admet une unique extension de Picard-Vessiot à isomorphisme différentiel près.*

Démonstration 2.2 Soit $A \in \mathcal{M}_n(K)$. Considérons l'équation $(E) : Y' = AY$. Nous allons seulement tenter de comprendre sur quoi se batit une extension de Picard-Vessiot pour cette équation et évincer l'unicité dans cette démonstration.
Introduisons, l'anneau engendré par les coefficients $Y_{i,j}$ c'est à dire $R = K[Y_{1,1}, ..., Y_{n,n}]$, l'anneau des polynômes à n^2 indéterminées. Soit G la matrice des $Y_{i,j}$. Doter R d'une dérivation qui prolonge celle définie sur K, revient à définir les dérivées des $Y_{i,j}$. On construit alors sur R la dérivation $D(G) = AG$. Ainsi si $G = (Y_1, ..., Y_n)$ (notation colonnes) on a pour tout $k \in [\![1, n]\!]$, $D(Y_k) = AY_k$, ce qui nous fournit n solutions.
Cependant les solutions ainsi construites ne sont pas toujours libres, ce qui nous oblige à forcer les choses en nous plaçant sur un espace sur lequel $\det(G) \neq 0$ (il suffit de développer par rapport à une colonne) est inversible, à savoir $S = R[T]/(1 - T\det(G))$: la classe de T est l'inverse de $\det(G)$. Comme précedement, si nous voulons étendre la dérivation sur S on doit savoir dériver T (plus précisement la classe de T que l'on désignera abusivement T). Il faut pour cela que l'idéal $(1 - T\det G)$ soit un idéal différentiel. Vérifions cela en calculant $D(1 - T\det(G))$. Un résultat classique nous dit que $D(\det(G)) = \text{Tr}(\underline{G}D(G))$ (où $\underline{G}$ est la transposée de la comatrice de G), ce qui nous donne :

$$\begin{aligned} D(1 - T\det(G)) &= -\text{Tr}(\underline{G}D(G))T - D(T)\det(G) \\ &= -\text{Tr}(\underline{G}AG)T - D(T)\det(G) \\ &= -\text{Tr}(AG\underline{G})T - D(T)\det(G) \\ &= -\text{Tr}(A\det G)T - D(T)\det(G) \\ &= -\det G(D(T) + \text{Tr}(A)T) \end{aligned}$$

En posant $D(T) = -\text{Tr}(A)T$, on confère à S une structure d'anneau différentiel. On a donc pour le moment :

- un anneau différentiel (S, D) dont la dérivation étend celle de K
- n solutions de (E) linéairements indépendantes dans S^n
- S qui est engendré par les coefficients de ces solutions.

Cependants deux problèmes subsistent : S n'est pas forcément un corps et le corps des constantes de S n'est pas nécessairement C. Considérons I un idéal maximal parmi les idéaux différentiels de S différent de S. Les idéaux différentiels de S/I sont triviaux. D'après le lemme ci-dessous, S/I est intègre et le corps des constantes de son corps des fractions L est égal à C . On a donc construit une extension de Picard-Vessiot pour l'équation différentielle $Y' = AY$, à savoir (L, D). □

Lemme 2.1 *Soit (K, D) un corps différentiel de caractéristique nulle, C son corps des constantes. Soit (A, D) une extension différentielle de (K, D). On suppose que les idéaux différentiels de A sont triviaux. Alors :*

- *l'anneau A est intègre. Notons F son corps des fractions (que l'on munit de sa dérivation canonique)*
- *le corps des constantes de F est contenu dans A*
- *si A est une K-algèbre de type fini et si C est algébriquement clos, le corps des constantes de F est égal à C.*

Démonstration 2.3 Montrons que A ne contient aucun élément nilpotent non nul. Considérons $\mathrm{Nil}(A) = \{x \in A / \exists n \in \mathbb{N}^*, x^n = 0\}$. C'est un idéal différentiel de A. En effet, soit $x \in \mathrm{Nil}(A)$ et $n > 0$ tel que $x^n = 0$. Montrons par récurrence finie que pour tout $k \in [\![0, n]\!]$, on a :

$$x^{n-k}(x')^{2k} = 0\,.$$

Pour $k = 0$, c'est la relation de départ.
Si le résultat est vrai pour au rang $k < n$, on obtient en dérivant :

$$(n-k)x^{n-k-1}(x')^{2k+1} + 2kx''x^{n-k}(x')^{2k-1} = 0\,.$$

En multipliant par x', on obtient $(n-k)x^{n-(k+1)}(x')^{2(k+1)} = 0$. L'anneau étant de caractéristique nulle, le résultat s'en suit. On obtient donc $(x')^{2n} = 0$. Ce qui montre que $\mathrm{Nil}(A)$ est un idéal différentiel, puisque $1 \notin \mathrm{Nil}(A)$, on obtient $\mathrm{Nil}(A) = \{0\}$.

Soit $a \in A$ et $I = \{b \in A,\, ab = 0\}$. Si $b \in I$, en dérivant la relation $ab = 0$, on obtient $ab' + a'b = 0$, d'où après multiplication par a : $a^2b' = 0$. Par suite, $(ab')^2 = 0$. Or, d'après ce qui précède, ceci implique que $ab' = 0$. L' ensemble I est donc un idéal différentiel de A. Puisque $a \neq 0$, $I \neq A$, donc $I = (0)$. Ce qui prouve que A est intègre.

Notons C' le corps des constantes de F, c'est un sous-corps de F qui contient C.
Soit $x \in C'$ et $I = \{a \in A,\, ax \in A\}$. C'est un idéal différentiel de A.
En effet, si $a \in I$, alors $ax = b$, avec $b \in A$. On a donc $ax' + a'x = b'$, et puisque x est constant, $a'x \in A$. Ce qui montre que $a' \in I$, *i.e.* I est un idéal différentiel de A. Comme $x \in F$, $I \neq (0)$. Il s' en suit que $I = A$. En particulier, $1 \in I$ et $x = 1x \in A$.

D'après ce qui précède, $C' \subset A$. Considérons un idéal maximal $\mathfrak{m}$ de A.
L'anneau $A/\mathfrak{m}$ est alors, d'une part un corps, et d'autre part une K-algèbre de type fini. C'est donc une extension algébrique de K. Comme tout homomorphisme de corps, l'homomorphisme $C' \longrightarrow A/m$ est injectif et on peut identifier C' à son image dans $A/\mathfrak{m}$. Par suite, tout élément de C' est algébrique sur K. D' après le lemme ci-desssous, les éléments de C' étant constants, tout élément de C' est algébrique sur le corps C, corps des constantes de K. Puisque C est algébriquement clos, $C' = C$. □

Lemme 2.2 *Soit $(K, D) \subset (L, D)$ une extension de corps différentiels. On note C le corps des constantes de K . Soit $x \in L$. Les deux propriétés suivantes sont équivalentes :*

(i) *x est algébrique sur C*

(ii) *x est constant et algébrique sur K.*

3 Extensions élémentaires

Tous les corps considérés sont dans la suite de caractéristique nulle.

3.1 Généralités

Définition 3.1 *Soient (K, D) un corps différentiel et (L, D) une extension différentielle de K. Soient $y \in L$ et $x \in K - \{0\}$. On dit que :*

- *y est une exponentielle de x si $y' = xy$*
- *y est un logarithme de x si $y' = \dfrac{x'}{x}$.*

Définition 3.2 *Soient (K, D) un corps différentiel et (L, D) une extension différentielle de K. L est dite élémentaire si et seulement si on peut trouver $t_1, ..., t_n \in L$ tels que :*

- *$L = K(t_1, ..., t_n)$*
- *le corps des constantes sur L est le même que celui de K.*
- *$\forall j \in [\![1, n]\!]$, on a l'un des cas suivant : (avec la convention $K(t_0) = K$) :*
  1. *t_j est algébrique sur $K(t_1, ..., t_{j-1})$*
  2. *t_j est un logarithme d'un élément non nul de $K(t_1, ..., t_{j-1})$*
  3. *t_j est une exponentielle d'un élément de $K(t_1, ..., t_{j-1})$.*

3.2 Le théorème de Liouville-Ostrowski

Théorème 3.1 (Liouville-Ostrowski) *Soit (K, D) un corps différentiel de corps des constantes C et soit $f \in K$. Si l'équation $y' = f$ admet une solution dans une extension élémentaire L de K si et seulement si il existe $n \geq 0$, $c_1, ..., c_n \in C$ et $v, u_1, ..., u_n \in K$ tels que :*

$$f = v' + c_1 \frac{u_1'}{u_1} + ... + c_n \frac{u_n'}{u_n}. \quad (1)$$

Démonstration 3.1 Supposons que f possède une primitive dans une extension élémentaire de K de la forme $L = K(t_1, ..., t_p)$ et procédons par récurrence sur p. Plus précisement, on voit que f prend la forme (1) avec les $v, ..., u_n$ dans L : il suffit de prendre v une primitive de f dans L. Nous allons ainsi démontrer préalablement que si f s'écrit sous la forme (1) sur $K(t_1, ..., t_p)$ alors elle possède une écriture sous cette même forme dans $K(t_1, ..., t_{p-1})$ et ainsi par récurrence sur p, on aura une écriture sur K (ce que le théorème prétend). De façon plus concise, cela revient à montrer que si $K \subset K(t)$ est une extension élémentaire (c'est à dire que t est soit un logarithme, soit une exponentielle, soit algébrique sur K) et si $f \in K$ s'écrit sous la forme (1) sur $K(t)$, alors on a une écriture similaire sur K. Distinguons pour cela trois cas selon la nature de l'extension $K \subset K(t)$.

Cas 1 : t algébrique sur K Soit $K \subset K(t) \subset L$ la clôture galoisienne de l'extension. L' extension L/K est séparable, finie, donc par le théorême de l'élément primitif on peut trouver $\xi \in L$ tel que $L = K(\xi)$. Comme vu précedement, construire une dérivation sur L revient à construire la dérivée de ξ. Soit μ le polynôme minimal de ξ sur K. La relation

$\mu(\xi) = 0$ nous impose $D(\xi) = -\dfrac{\mu^D(\xi)}{\mu^{'}(\xi)}$ (on a bien $\mu^{'}(\xi)$ non nul) où

$$P^D = \sum_{k=0}^{n} D(a_k)X^k,$$

quand

$$P = \sum_{k=0}^{n} a_k X^k.$$

On définie alors $D : L \to L$ par $D(y) = D(P(\xi)) = P^D(\xi) + P^{'}(\xi)D(\xi)$ quand $P \in K[X]$ et $y = P(\xi)$. L' application D vérifie bien les axiomes d'une dérivation. Cependant, pour que cette application soit bien définie, il faut que le résultat soit indépendant du choix du représentant P. Soient P et Q dans $K[X]$ tels que $\mu \mid (P - Q)$, il existe donc $\beta \in K[X]$ tel que $P - Q = \beta\mu$. On a par choix de $D(\xi)$:

$$D(\beta(\xi)\mu(\xi)) = D(\beta(\xi))\mu(\xi) + D(\mu(\xi))\beta(\xi) = \mu^D(\xi) + \mu^{'}(\xi)D(\xi) = 0\,,$$

ce qui montre que (L, D) est bien une extension différentielle de (K, D).

Un petit calcul montre que pour tout $\sigma \in \mathrm{Gal}(L/K)$, pour tout $x \in L^*$,

$$\sigma\left(\frac{x'}{x}\right) = \frac{\sigma(x)'}{\sigma(x)}\,,$$

où $\mathrm{Gal}(L/K)$ désigne le groupe de Galois de L/K. Considérons pour $k \in [\![1, n]\!]$:

$$\gamma_k = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(u_k) \text{ et } \nu = \frac{1}{[L : K]} \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(v)\,.$$

Ces quantités sont bien dans K car invariantes par $\mathrm{Gal}(L/K)$ (en effet, on sait que si L/K est normale alors $K = L^{\mathrm{Gal}(L/K)}$) et on a bien :

$$f = \nu^{'} + \sum_{k=1}^{n} \frac{c_k}{[L : K]} \frac{\gamma_k^{'}}{\gamma_k}\,.$$

Cas 2 : t est une exponentielle ou un logarithme sur K Tout d'abord, on suppose t transcendant sur K car sinon on se ramène au cas précédent. Dans cette situation, $K(t)$ s'identifie au corps des fractions rationnelles sur K mais munie d'une autre dérivation que l'on notera par abus $f^{'}$(car on ne parlera pas de la dérivation usuelle). Par conséquent, les notions de décomposition en éléments simples (d'unicité de cette décomposition), de $pgcd$ et autres seront utilisées (identiquement que sur $K(X)$ et $K[X]$). Commençons par simplifier le problème. Pour i fixé, $u_i(t)$ s'écrit : $u_i(t) = \lambda \prod_{k=1}^{r} P_k^{\alpha_k}(t)$, avec les P_k irréductibles unitaires deux à deux distincts, les α_k dans $\mathbb{Z}$ et $\lambda \in K$. D'où :

$$\frac{u_i^{'}}{u_i} = \frac{\lambda^{'}}{\lambda} + \sum_{k=1}^{r} \alpha_k \frac{P_k^{'}}{P_k}\,.$$

On voit donc que, quitte à changer les notations, on peut en développant ainsi l'expression (1) se ramener à des u_i deux à deux distincts qui sont, soit des polynômes irréductibles unitaires en t, soit des éléments de K. On peut aussi décomposer $v(t)$ en éléments simples. La

simplification s'arrête ici et nous devons maintenant regarder de près le cas exponentiel et le cas logarithme.

Supposons d'abord que t soit un logarithme. Il existe donc $a \in K - \{0\}$ tel que $t' = \frac{a'}{a}$. Soit $P \in K[X]$ un polynôme irréductible. Supposons par l'absurde que la décomposition en éléments simples de v contienne un facteur de la forme $\frac{A}{P^r}$ avec $r \geqslant 1$ et $P \nmid A$ (on choisit un tel r maximum). Ainsi v' est une somme de termes dont l'un des termes est $\frac{AP^{'}}{P^{r+1}}$; or comme P est unitaire et que $t^{'} = \frac{a^{'}}{a} \in K$ un petit calcul montre que $\deg(P^{'}) < \deg(P)$ donc le caractère irréductible de P implique que $P \nmid P^{'}$ donc $\frac{AP^{'}}{P^{r+1}}$ est une expression irréductible. D'autre par les termes en $\frac{u_i^{'}}{u_i}$ ne donne que des puissances de P au dénominateur d'au plus 1. Enfin comme r est maximum, le terme $\frac{AP^{'}}{P^{r+1}}$ ne s'annule pas avec un autre terme et se retrouve donc au dénominateur dans l'écriture irréductible de $f \in K$ qui est unique (dans $K(t)$) : il y a donc une contradiction au départ ! On en déduit que v est un polynôme en t donc $f - v^{'}$ aussi cela implique que les u_i sont dans K par unicité de la décomposition en éléments simples. Un petit calcul montre que comme $v^{'} \in K$, v est de la forme $v(t) = ct + d$ avec c constant et $d \in K$. On a en résumé :

$$f = d^{'} + c\frac{a^{'}}{a} + \sum_{k=1}^{n} c_k \frac{u_k^{'}}{u_k}\,,$$

où tout le monde est bien dans K.

Maintenant, regardons le cas où t est une exponentielle. Posons $t' = a't$ avec $a \in K$. Nous allons procéder d'une manière très analogue au cas logarithme. Prennons P un polynôme irréductible unitaire de $K[t]$. Ici P' est un polynôme de même de degré que P, par conséquent l'argument précédent ne fonctionne plus (on n'a plus forcément $P \nmid P'$) Cherchons tout de même les P tel que $P \mid P^{'}$:
Pour un tel P on a $\frac{P'}{P} \in K$ (ils sont de même degré). Posons $P = \sum_{k=1}^{N} a_k t^k$. On a : $P' = \sum_{k=1}^{N} (a'_k + k a_k a')t^k$. Montrons que P est un monôme. Supposons par l'absurde qu'il existe $l \neq k$ tel que $a_l, a_k \neq 0$. Les coefficients de P et P' étant proportionels on a :

$$\frac{a'_k + k a_k a'}{a_k} = \frac{a'_l + k a_l a'}{a_l}\,.$$

Donc :

$$\frac{a'_l}{a_l} + l\frac{t'}{t} = \frac{a'_k}{a_k} + k\frac{t'}{t}\,.$$

On en déduit que $(\frac{a_k t^k}{a_l t^l})' = 0$ (il suffit de développer l'expression). D'où $\frac{a_k t^k}{a_l t^l} \in C \subseteq K$. Ceci contredit le caractère transcendant de t. Par conséquent P est un monôme (la réciproque est évidente : P monôme implique $P \mid P'$).

Maintenant que nous avons la liste des polynômes qui nous posent problème, reprenons le cours de la démonstration. Soit P un polynôme irréductible unitaire différent de t. En raisonnant mot pour mot comme dans le cas logarithme on voit que P n'apparait ni dans le dénominateur de v ni dans la liste des u_i. Les u_i étant deux à deux distincts t ne peut apparaitre qu'au plus une fois dans la liste des u_i, on peut donc sans perte de généralités poser $u_1 = t$. On en déduit deux choses : premièrement les u_i pour $i \geqslant 2$ sont dans K ; enfin v s'écrit $v(t) = \sum_{j=-N}^{N} a_j t^j$ avec les a_j dans K. En raisonnant sur les coefficients (*cf.*

détermination des P tels que $P \mid P'$) on voit que $v(t)' \in K$ implique $v(t) \in K$. Au final, on a :

$$f = c_1 \frac{t'}{t} + \sum_{i=2}^{n} c_i \frac{u_i'}{u_i} + v' = \sum_{i=2}^{n} c_i \frac{u_i'}{u_i} + (c_1 a + v)',$$

où les u_i pour $i \geqslant 2$ sont dans K, v est dans K. C'est gagné ! □

3.3 Application à e^{x^2}

Voyons comment les choses se passent pour une fonction assez connue : $x \mapsto e^{x^2}$. Peut-on exprimer une primitive de cette fonction dans une extension élémentaire de $\mathbb{C}(x, \exp(x^2))$? Raisonnons par l'absurde et supposons que c'est le cas. D'après le théorème de Liouville-Ostrowski, on peut trouver $n \geqslant 0$, $a_1, ..., a_n \in \mathbb{C}$ et $v, u_1, ..., u_n \in \mathbb{C}(x, \exp(x^2))$ tels que :

$$\exp(x^2) = v' + c_1 \frac{u_1'}{u_1} + ... + c_n \frac{u_n'}{u_n}\,.$$

En utilisant le même raisonnement que dans la démonstration du théorème de Liouville-Ostrowski dans le cas exponentiel, on voit que la seule égalité possible est de la forme :

$$\exp(x^2) = v' + c2t\,,$$

avec c constant et $v \in \mathbb{C}(x)[\exp(x^2)]$.

En identifiant les termes en $\exp(x^2)$, il existe $a \in \mathbb{C}(x)$ tel que : $a' + 2xa = 1$. Or ceci implique que a est un polynôme. En effet, si a n'est pas un polynôme alors il admet un pôle (on est sur $\mathbb{C}$), la multiplicité de ce pôle est un cran supérieur pour a'. Or $a' = -2xa + 1$ donc la multiplicité doit être la même : contradiction. Le fait que a soit un polynôme entraine aussi une contradiction sur le degré de a. Cet exemple nous illustre parfaitement que toute fonction n'admet pas, en général, une primitive exprimable élémentairement !

4 Algorithme de Risch

Nous venons de voir dans un cadre théorique un théorème qui donne un critère effectif de calculabilité d'une primitive, mettons maintenant cela en pratique à travers l'algorithme de Risch. Nous allons ainsi voir comment un logiciel de calcul formel utilise réellement le théorème de Liouville-Ostrowski.

Dans tout ce qui suit, K désignera le corps des constantes de toutes les extensions considérées.

Définition 4.1 *Soit n un entier naturel. Une tour de variable de taille n sur K est la donnée d'un $(n+1)$-uplet $(t, \theta_1, ..., \theta_n)$ avec θ_k exponentiel transcendant ou logarithme transcendant sur $K(t, \theta_1, ..., \theta_{k-1})$ (avec la convention $K(t, \theta_0) = K(t)$).*

Remarque 4.1 Pour être cohérent avec la définition donnée précédement d'une extension élémentaire, nous devrions prendre aussi en compte les θ_k algébriques, cependant nous allons nous limiter dans cet exposé à ce cadre simplifié qui nécessite déjà des efforts.

Remarque 4.2 Nous avons accès, grâce à ces tours de variables, à l'ensemble des fonctions que l'on peut fabriquer à partir d'un logiciel de calcul formel simple. Bien entendu, on peut construire des théories plus fines en incluant d'autres fonctions à nos fonctions élémentaires (arctan si $K = \mathbb{R}$,...) et en prenant en compte les éléments algèbriques.

On considère ici une tour de variables de taille $s \geqslant 1$ sur K : $(t, \theta_1, ..., \theta_s)$. Et on se demande si $f \in K(t, \theta_1, ..., \theta_s)$ admet une primitive élémentaire.

On peut alors écrire $f = \dfrac{N_0(\theta_s)}{D_0(\theta_s)}$ avec $N_0, D_0 \in K(t, \theta_1, ..., \theta_{s-1})[X]$ premiers entre eux. L'algorithme de Risch consistera alors en l'intégration via la fraction rationnelle. On va chercher à résoudre l'équation $f = v' + c_1 \dfrac{u_1'}{u_1} + ... + c_N \dfrac{u_N'}{u_N}$, où les inconnues sont $v, u_1, ..., u_N \in K(t, \theta_1, ..., \theta_s)$. L'algorithme de Risch agit récursivement sur ce modèle d'équations : on se ramène à un système d'équations de ce type mais dans $K(t, \theta_1, ..., \theta_{s-1})$.

4.1 Réduction du problème

On essaye de décomposer la fraction $\frac{N_0}{D_0}$ pour permettre le calcul d'une primitive. L'obtention de cette décomposition est basée sur une identité de Bezout entre des polynômes P et P' de $K(t, \theta_1, ..., \theta_{s-1})[X]$. On se heurte à une difficulté lorsqu'on a une extension exponentielle. En effet, si $\theta_s = e^g$, alors $\theta_s' = g'\theta_s$, qui ne sont plus premiers entre eux.

Si θ_s est une exponentielle et si D_0 multiple de X alors on peut écrire $\frac{N_0}{D_0} = \frac{N_1}{D_1} + \frac{P}{X^k}$ avec $D_0 = X^k D_1$ et $X \wedge D_1 = 1$.

On isole alors la partie entière de $\frac{N_0}{D_0}$ (ou de $\frac{N_1}{D_1}$), qui est un polynôme. Ainsi, on peut écrire $\frac{N_0}{D_0} = \frac{N}{D} + \sum_j a_j X^j$.

Finalement, on a une décomposition de la forme :

$$\frac{N_0}{D_0} = \frac{N}{D} + \sum_j a_j X^j \text{ avec } \begin{cases} \deg N < \deg D & \\ X \nmid D & \\ (a_j) \in K(\theta_1, ..., \theta_{n-1})^{(\mathbb{Z})} & \\ \forall j < 0, a_j = 0 & \text{si } X \text{ un logarithme} \\ \forall j < 0, a_j \neq 0 \text{ pour des } k < 0 & \text{si } X \text{ est une exponentielle} \end{cases}$$

On effectue désormais le problème de primitivation en deux partie : primitivation de la fraction propre $\frac{N}{D}$, primitivation du polynôme «généralisé» $\sum_j a_j X^j$.

4.2 Intégration de la fraction propre

4.2.1 Réduction sans facteurs multiples, factorisation sans carré

Considérons la factorisation en produit d'irréductible de $D = \prod D_i^{\alpha_i}$ et regroupons les D_i suivant leur valuation α_i :

$$D = \prod_i P_i^i \,.$$

Cette factorisation est appelé factorisation sans carrée de D et $\prod_i P_i$ la partie sans carré de D. Les P_i sont sans facteurs multiples et premiers entre eux deux à deux.

Remarque 4.3 Ces deux remarques nous seront utiles par la suite :
- Si P est un polynôme unitaire, irréductible, alors il est premier avec P' pour des raisons de degré.

– Si P est un polynôme unitaire, sans carré, alors il est premier avec P'. En effet, si la décomposition en facteur irréductible de P s'écrit

$$P = \prod_k Q_k \text{ alors } P' = \sum_k Q_k' \prod_{j \neq k} Q_j.$$

Ainsi, par réduction modulo Q_k, on obtient

$$P' \equiv Q_k' \prod_{j \neq k} Q_j \not\equiv 0[Q_k],$$

car les Q_j et Q_k' sont premiers avec Q_k. Ainsi, P' n'est divisible par aucun facteur irréductible de P : ils sont donc premiers entre eux.

La décomposition sans carré peut s'obtenir grace à un algorithme que nous décrivons ici.

Soit k un corps de caractéristique nulle, $P \in k[X]$ unitaire et $P = P_1 P_2^2 ... P_n^n$ sa factorisation sans carré. Un calcul simple montre que

$$P' = \sum_{i=1}^{n} i P_i^{i-1} \prod_{k \neq i} P_k^k = P_2 P_3^2 ... P_n^{n-1} (P_1' P_2 ... P_n + ... + n P_1 ... P_n').$$

On remarque que $P_2 P_3^2 ... P_n^{n-1}$ divise $P \wedge P'$. En fait, ces deux polynomes sont égaux. En effet, si tel n'était pas le cas, alors il y a un facteur irréductible Q de $P \wedge P'$ divisant l'un des P_i, disons P_k, de valuation k exactement. Or, par réduction modulo Q^k, on trouve

$$P' \equiv k P_k' \prod_{i \neq k} P_i \not\equiv 0[Q^k].$$

Ce qui est absurde. Les polynomes $P_2 P_3^2 ... P_n^{n-1}$ et $P \wedge P'$ étant unitaires, ils sont égaux. Ceci permet de déduire l'algorithme de factorisation sans carré :

ALGORITHME DE FACTORISATION SANS CARRÉ

- poser $u_0 = D$
- calculer récursivement par l'algorithme d'Euclide $u_{i+1} = u_i \wedge u_i'$ et $v_i = \dfrac{u_{i-1}}{u_i}$ jusqu'à ce que $u_i = 1$
- soit m la dernière valeur de i telle que $u_i \neq 1$
- pour i de 1 à $m-1$, calculer $h_i = \dfrac{v_i}{v_{i+1}}$ et poser $h_m = v_m$

Remarque 4.4 A l'étape i, on a : $u_i = P_{i+1} P_{i+2}^2 ... P_n^{n-i}$, $v_i = P_i ... P_m$ et $h_i = P_i$.

4.2.2 Décomposition en fractions partielles

La factorisation sans carré permet d'obtenir une décomposition en fractions partielles de $\frac{N}{D}$, qui est une sorte de généralisation de la décomposition en éléments simples. La forme particulière de cette décomposition permet une technique d'intégration itératives des fractions obtenus, grâce à des relations de Bezout.

La décomposition en fractions partielles de $\frac{N}{D}$ selon la factorisation sans carré, consiste à écrire $\frac{N}{D}$ sous la forme :

$$\frac{N}{D} = \frac{N_1}{P_1} + ... + \frac{N_n}{P_n^n}, \quad \text{avec } \forall i \in [\![1, n]\!], \deg N_i < \deg P_i^i \,.$$

En réduisant au même dénominateur, on obtient la relation :

$$N = N_1 P_2^2 ... P_n^n + ... + N_i P_1 ... P_{i-1}^{i-1} P_{i+1}^{i+1} ... P_n^n + ... + N_n P_1 ... P_{n-1}^{n-1} \,.$$

Fixons $i \in [\![1, n]\!]$ et réduisons cette relation modulo P_i^i, on obtient donc :

$$N \equiv N_i P_1 ... P_{i-1}^{i-1} P_{i+1}^{i+1} ... P_n^n [P_i^i] \,.$$

Puisque chaque P_k^k est premier avec P_i^i, il est inversible modulo P_i^i. En notant $\widehat{P_k^k}$ un inverse de P_k^k modulo P_i^i (que l'on peut calculer grâce à une identité de Bezout), on obtient :

$$N_i \equiv N \widehat{P_1} ... \widehat{P_{i-1}^{i-1}} \widehat{P_{i+1}^{i+1}} ... \widehat{P_n^n} [P_i^i] \,.$$

La condition de degré permet d'en déduire N_i ainsi que l'existence de cette décomposition.

ALGORITHME DE DÉCOMPOSITION EN FRACTIONS PARTIELLES

- calculer pour $i \in [\![1, n]\!]$ $Q_i = D/P_i^i$
- calculer par l'algorithme d'Euclide étendu, une relation de Bezout $U_i Q_i + V_i P_i^i = 1$
- calculer le reste N_i de la division euclidienne de NU_i par P_i^i

Pour chacun des polynômes P_i, l'identité de Bezout entre P_i et P_i' permet de réduire :

$$N_i = A_i P_i + B_i P_i' \text{ ce qui donne } \frac{N_i}{P_i^i} = \frac{A_i}{P_i^{i-1}} + \frac{B_i P_i'}{P_i^i} \,.$$

Une intégration par partie donne : $\displaystyle\int \frac{N_i}{P_i^i} = \frac{-B_i}{(i-1)P_i^{i-1}} + \frac{1}{i-1} \int \frac{B_i' + (i-1)A_i}{P_i^{i-1}} \,.$

On itère cette étape jusqu'à l'obtention d'une puissance 1 au dénominateur. On obtient donc :

$$\int \frac{N}{D} = \sum_{i>0} \left(\frac{C_{i,i-1}}{P_i^{i-1}} + ... + \frac{C_{i,2}}{P_i^2} + \int \frac{C_{i,1}}{P_i} \right) \,.$$

Il suffit donc d'intégrer $\displaystyle\frac{A}{B} = \sum_{i>0} \frac{C_{i,1}}{P_i} \,.$

4.2.3 Partie logarithmique

Rappel sur le résultant : Soit $\mathbb{K}$ un corps et $P, Q \in K[X]$ de degrés respectifs n et m non nuls. On appel résultant de $P = \sum_k a_k X^k$ et $Q = \sum_k b_k X^k$ et on note $\text{res}(P, Q)$ le déterminant de la matrice $(n+m) \times (n+m)$:

$$\begin{pmatrix} a_0 & & & b_0 & & \\ \vdots & \ddots & & \vdots & \ddots & \\ a_n & & a_0 & b_m & & b_0 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_n & & & b_m \end{pmatrix}$$

Le premier motif se décale m fois et le second motif se décale n fois.

Proposition 4.1 *Soit $P, Q \in K[X]$. On a l'équivalence : $P \wedge Q = 1 \iff res(P,Q) \neq 0$. De plus, si $P \wedge Q \neq 1$, P, Q ont une racine commune dans une clôture algébrique de K.*

Démonstration 4.1 On considère l'application linéaire :

$$\psi : \left\{ \begin{array}{ccc} \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X] & \longrightarrow & \mathbb{K}_{m+n-1}[X] \\ (A,B) & \longmapsto & AP + BQ \end{array} \right.$$

Remarquons que le résultant de P et Q est tout simplement le déterminant de ψ dans la base canonique. Donc, clairement, si le résultant est non nul, ψ est un isomorphisme (les espaces d'arrivé et de départ ont même dimension) et ainsi le polynôme constant égal à 1 est atteint (ce qui équivaut à P et Q premiers entre eux par Bézout). Réciproquement, supposons $P \wedge Q = 1$ et prennons $(A,B) \in \ker(\psi)$. Cela signifie que $PA = -QB$ d'où Q divise PA donc divise A car premier avec P ; ceci n'est possible que si $A = 0$ car $\deg(A) < \deg(Q)$. On raisonne symétriquement pour B. Au final $(A,B) = (0,0)$, donc ψ inversible (toujours par un argument de dimension) et ainsi le résultant est non nul. □

Soit $\frac{A}{B} \in K(t, \theta_1, ..., \theta_{s-1})[X]$, avec B unitaire, sans carré, $A \wedge B = 1$ et $\deg A < \deg B$.

Si l'on dérive une fraction rationnelle en X, la dénominateur de la dérivée se décompose en produit de facteurs de multiplicité supérieure ou égale à deux. Il s'en suit que les fractions résiduelles obtenues à la fin de l'étape précédente ($\frac{A}{B}$), ne proviennent que de la dérivation d'une fonction du type $F = \sum_{k=0}^{p} c_k \ln u_k$:

$$\frac{A}{B} = F' = \sum_{k=0}^{p} c_k \frac{u_k'}{u_k} .$$

Après réduction au même dénominateur, il vient :

$$A \prod_{k=1}^{p} u_k = B \sum_{k=1}^{p} \left(c_k u_k' \prod_{j \neq k} u_j \right) .$$

Par réduction modulo u_k, on voit que u_k divise $B u_k' \prod_{j \neq k} u_j$. Etant premier avec $u_k' \prod_{j \neq k} u_j$, il divise B. Ainsi, puisque les u_k sont premiers entre eux deux à deux, leur produit divise B. Or, il est clair que B divise $\prod_{k=1}^{p} u_k$ car $A \wedge B = 1$. Quitte à ajouter une constante, on peut supposer les u_k unitaires. D'où, dans un premier temps,

$$B = \prod_{k=1}^{p} u_k .$$

Il s'agit pour nous d'exprimer les u_k et c_k à partir de A et B. Remarquons que l'expression de A en fonction des u_k ressemble à la dérivée de B aux constantes près. Par suite, en posant $\Delta(t) = A - tB'$, on trouve :

$$\Delta(t) = \sum_{k=0}^{p} (c_k - t) u_k' \prod_{j \neq k} u_j .$$

Il s'en suit que u_k divise $\Delta(c_k)$ et donc $(A - c_k B') \wedge B = u_k$. Si bien que l'on peut calculer u_k à partir de A, B et c_k. Le problème réside donc en la connaissance des c_k et pour y remédier, on utilise le résultant.

Théorème 4.1 *Une primitive de* $\dfrac{A}{B}$ *est donnée par* $\displaystyle\sum_{k=0}^{p} c_k \ln u_k$ *avec* $c_k \in L$, $u_k \in L[X]$, *avec* L *extension algébrique finie de* $\mathbb{K}$ *si et seulement si* $R(T) = res_X(B, A - TB')$ *est scindé sur* L *avec* c_k *pour racines.*

Démonstration 4.2 En effet, comme nous l'avons vu précédement, si $\displaystyle\int \frac{A}{B} = \sum_{k=0}^{p} c_k \ln u_k$, alors $B = u_1 ... u_n$ et $R(T)$ est scindé avec c_k pour racines car $(A - c_k B') \wedge B = u_k$.
Réciproquement, notons $\overline{K}$ une clôture algébrique de K. Alors $c \in \overline{K}$ est un zéro de R, si et seulement les polynômes B et $A - cB'$ ont une racine commune. Or, B étant sans carré, une racine de B ne peut être racine de B'. Par suite, si $c \in \overline{K}$ on a les équivalences :

$$R(c) = 0 \Longleftrightarrow \exists \xi \in \overline{K} / \left\{ \begin{array}{l} B(\xi) = 0 \\ A(\xi) - cB'(\xi) = 0 \end{array} \right. \Longleftrightarrow \exists \xi \in \overline{K} / \left\{ \begin{array}{l} B(\xi) = 0 \\ c = \frac{A(\xi)}{B'(\xi)} \end{array} \right.$$

Notant $Z(P)$ l'ensemble des racines d'un polynôme P, on a : $Z(B) \overset{\psi}{\longrightarrow\!\!\!\!\!\rightarrow} Z(R)$
avec $\psi : \left\{ \begin{array}{ccc} Z(B) & \longrightarrow & Z(R) \\ \xi & \longmapsto & \frac{A(\xi)}{B'(\xi)} \end{array} \right.$

Notons $c_1, ..., c_p$ les racines distincts de R. Il vient donc :

$$\prod_{\beta \in \psi^{-1}(c_i)} (X - \beta) = B \wedge (A - c_i B') = u_i \,,$$

et par suite

$$B = \prod_{\beta \in Z(B)} (X - \beta) = u_1 ... u_p \,.$$

Pour tout $i \in [\![1, p]\!]$, pour tout $\beta \in \psi^{-1}(c_i)$, on a :

$$\left(\sum_{i=1}^{p} c_i \frac{u_i'}{u_i}(\xi) \right) B(\xi) = c_i u_1(\xi) ... u_i'(\xi) ... u_p(\xi) = c_i B'(\xi) = A(\xi) \,.$$

Les polynômes $\left(\displaystyle\sum_{i=1}^{p} c_i \frac{u_i'}{u_i} \right) B$ et A étant de degré strictement inférieur à $\deg B$, coïncidant sur $\deg B$ racines distinctes de B, sont égaux. D'où l'implication recherchée. □

En pratique, on s'intéresse à des fonctions de la variable réelle ou complexe, il faut donc tester si les racines obtenus sont des constantes. Pour cela, on normalise R, et on vérifie que chacun des nouveaux coefficients sont constants. En effet, si les racines de R sont constantes alors les coefficients aussi car ils s'expriment comme fonctions symétriques élémentaires des racines. En résumé :

ALGORITHME POUR LA PARTIE LOGARITHMIQUE

- calculer le résultant $R(T) = \text{res}_X(B, A - TB')$
- normaliser R et tester si les coefficients sont constants car sinon la fonction n'admet pas de primitive élémentaire
- si les coefficients sont constants, calculer les racines de R :
  - sur $\mathbb{C}$, on obtient l'ensemble des c_k
  - sur $\mathbb{R}$, vérifier que toutes les racines de R sont réelles car sinon la fonction n'admet pas de primitive élémentaire
- quand R est scindé, calculer u_k avec la formule $u_k = B \wedge (A - c_k B')$

4.3 Partie polynome généralisé

Il nous reste à présent à primitiver la partie polynomiale de la décomposition. Il s'agit donc de résoudre :

$$\left(\sum_j A_j X^j\right)' = \sum_j a_j X^j \,,$$

avec une somme portant sur $\mathbb{Z}$ si X est une exponentielle, sur $\mathbb{N}$ sinon.

4.3.1 Extension logarithmique

Supposons dans cette partie que $X = \ln(Y)$ est un logarithme. On doit donc résoudre :

$$\sum_{j\geqslant 0}\left(A_j^{'} + (j+1)A_{j+1}\frac{Y'}{Y}\right)X^j = \sum_{j\geqslant 0} a_j X^j \,.$$

Notons d le degré de $\sum_{j\geqslant 0} a_j X^j$. Pour $j > d$, on a :

$$A_j^{'} + (j+1)A_{j+1}\frac{Y'}{Y} = 0\,.$$

La forme recherchée d'une primitive impose que pour j assez grand $A_j = 0$. Par suite, si $A_{j_0+1} = 0$, alors A_{j_0} est constant. Si $A_{j_0} \neq 0$, alors on a :

$$A_{j_0-1}^{'} = -j_0 A_{j_0}\frac{Y'}{Y}.$$

Il vient donc à une constante additive près, $A_{j_0-1} = -j_0 A_{j_0} X$ ce qui n'est pas car A_{j_0-1} est indépendant de X. Il s'en suit que pour $j > d+1$, $A_j = 0$ et A_{d+1} constant.

On résoud ce système par valeur décroissant. La valeur de la constante A_{d+1} sera alors déterminée par une condition.

4.3.2 Extension exponentielle

Supposons dans cette partie que $X = \exp(Y)$ est une exponentielle. De même, on doit résoudre une équation sur les coefficients :

$$A_j^{'} + jY'A_j = a_j\,.$$

Les choses ici se compliquent car on est amené à résoudre une équation du type :

$$y^{'} + fy = g\,,$$

avec f, g dans une tour de variables plus petite. Nous voyons que si $f = 0$ alors on peut appeler récursivement l'algorithme de Risch. Cependant si $f \neq 0$ nous devons nous intéresser plus précisement à la nature de Y. Nous allons dans la suite donner les grandes étapes de la résolution de ce problème.

4.3.3 Grandes lignes de la résolution de $y^{'} + fy = g$

Détermination du dénominateur : Nous allons ici déterminer le dénominateur D de y en déterminant ses facteurs irréductibles.
Soit P un facteur irréductible de D. Soit $\alpha < 0$ la valuation P-adique de D, β celle de f et γ celle de g.
On note f_d le dénominateur de f et g_d celui de g. Examinons les différentes situations :

- **Si Y n'est pas une exponentielle** : Si $\beta \neq -1$, on peut montrer par une étude cas par cas (simple mais longue) que α est l'opposé de la valuation P-adique de D_0, avec

  $$D_0 = \frac{pgcd(g_d, \partial_Y(g_d))}{pgcd(U, \partial_Y(U))}\,,$$

  où $U = pgcd(f_d, g_d)$.
  On a donc trouvé une partie du dénominateur. On va maintenant s'intéresser aux P tels que $\beta = -1$ que l'on va regrouper en f_1. On calcule ensuite par l' algorithme de Bezout le terme $\frac{N}{f_1}$ de f_d et on voit par un raisonnement proche de celui utilisé pour calculer « la partie logarithmique » que les α correspondants sont les racines entières (de la variable t) du résultant en Y de $N - tf_1^{'}$ et de f_1.
- **Si $Y = \exp(Z)$ et $P = \exp(Z)$** : la valuation de $y^{'}$ est α, celle de fy est $\alpha - \beta$. Donc si $\beta > 0$, on a $\alpha = \gamma$, si $\beta < 0$, on a $\alpha = \beta + \gamma$.
  Le cas $\beta = 0$ se complique : s'il n'y a pas de simplifications, alors on est ramené au cas précédent ; s'il y a des simplifications, on note f_0 le terme constant de f et y_α le terme de plus bas degré de y (dans la partie polynôme généralisée de la décomposition canonique).
  Ainsi, on a l'équation en y_α :

  $$y_\alpha^{'} + (\alpha Z^{'} + f_0)y_\alpha = 0\,.$$

  Donc $y_\alpha = \exp(-\alpha Z - \int f_0)$, soit $\ln(y_\alpha) + \alpha Z = -\int f_0$.
  On admet qu'alors $-\int f_0$ s'écrit $AZ + B$ avec $A \in \mathbb{Q}$ et B indépendant de Z dans la tour de départ. De ce fait, on a nécessairement $\alpha = A$, car sinon on aurait $\exp(Z)$ algébrique (il suffit de tirer $\exp(Z)$ dans l'expression de $\int f_0$).

En ayant le dénominateur on peut en simplifiant, se ramener à une équation sur le numérateur N.

Algorithme SPDE de Rothstein : On est donc amener à résoudre une équation du type : $RN^{'} + SN = T$.

Quand R ne divise pas S . Posons

$$R_1 = \frac{R}{pgcd(R,S)},\ S_1 = \frac{S}{pgcd(R,S)},,\ T_1 = \frac{T}{pgcd(R,S)}\,,$$

avec $\deg(R_1) \geqslant 1$. On se ramène ainsi à : $R_1 N^{'} + S_1 N = T_1$, avec de plus R_1 et S_1 premiers entre eux.
D'après l'identité de Bézout, il existe donc U, V tels que :

$$R_1 U + S_1 V = T_1\,,$$

avec $\deg(V) < \deg(R_1)$.
En soustrayant cette égalité à l'égalité de départ on obtient : $R_1(N^{'} - U) = -S_1(N - V)$. Ainsi R_1 divise $(N - V)$: on est donc en droit de poser $H = (N - V)/R_1$. On trouve une équation du même type en H :

$$R_1 H^{'} + (S_1 + R_1^{'})H = U - V^{'},$$

dont on sait que le degré de la solution est strictement inférieur au degré de la solution de l'équation initiale (car $0 < \deg(R_1)$ et $\deg(V) < \deg(R_1)$).
Si $R_1 \nmid S_1 + R_1^{'}$, on peut réappliquer mot pour mot la même manipulation. Par conséquent, une certaine itération du procédé nous amène à résoudre une équation du type

$$RN^{'} + SN = T,$$

avec $R \mid S$ (car les dégrés des solutions sont des nombres entiers naturels et ne peuvent donc former une suite strictement décroissante).

Quand R divise S : On doit donc résoudre une équation qui se réduit (après division par R) sous la forme : $N^{'} + SN = T$. Regardons ce qui se passe cas par cas :

- **Si** $S = 0$: On se ramène au problème de Risch initial sur une tour plus petite.
- **Si** $\deg(S) > 0$: On a $\deg(NS) > \deg(N^{'})$. Donc on a $\deg(N) = \deg(T) - \deg(S)$ et l'on peut résoudre l'équation coefficient par coefficient (en commençant par le plus haut et puis par récurrence descendante).
- **Si** $\deg(S) = 0$ **et** $Y = t$: De même $\deg(NS) > \deg(N^{'})$ et se ramène au cas précédent.
- **Si** $\deg(S) = 0$ $(S = c)$ **et** $Y = \ln(Z)$: On se ramène à un système sur les coefficients :

  $$N_{k+1}^{'} + (k+1)\frac{Z^{'}}{Z}N_{k+1} + cN_k = T_k.$$

  On a donc une équation connue pour le terme de plus haut degré ($y^{'} + fy = g$) sur une tour de variable plus petite, que l'on résoud pour ensuite s'attaquer identiquement aux termes de degrés inférieurs.
- **Si** $\deg(S) = 0$ $(S = c)$ **et** $Y = \exp(Z)$: Le système sur les coefficients est ici :

  $$N_k^{'} + (kZ^{'} + c)N_k = T_k.$$

  On résoud donc coefficient par coefficient car on a une équation connue sur une tour de variable plus petite.

  Le problème masqué sur les 2 derniers sous cas est que l'on ne connait pas le degré de N. Nous admettons que l'on peut trouver ce degré sans en donner la preuve.

Références

[1] A. Chambert-Loir, *A field guide to algebra*. Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2005

[2] R. H. Risch, *The problem of integration in finite terms*. Amer. Math. Soc. 193, (1969), 167-189

[3] R. H. Risch, *The solution of the problem of integration in finite terms*. Bull. Amer. Math. Soc. 76 (1970), 605-608

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

[5] B. Parisse, *L'intégration (l'algorithme de Risch)*. www-fourier.ujf-grenoble.fr/~parisse/cas/risch.ps

[6] F. Chyzak, *Intégration symbolique des fractions rationnelles*.