Ce texte est, pour l'essentiel, la traduction d'un article de Matthew Wiener, dont on pourra trouver l'original sur le Web en suivant ce lien :
`http://groups.google.com/group/sci.math/msg/43d5fc44bc713171`

Quelles sont les primitives de e^{-x^2} ? De $\frac{\sin x}{x}$? De x^x ?

Comme pour de nombreux problèmes similaires, il n'y a pas de réponse.

Plus précisément, considérons la notion de «fonctions élémentaires». Ce sont les fonctions qui peuvent être exprimées à l'aide d'exponentielles et de logarithmes, à l'aide des opérations algébriques usuelles (y compris la résolution, non nécessairement par radicaux, d'équations algébriques). Comme les fonctions trigonométriques et leurs réciproques peuvent être exprimées de cette manière (en utilisant le corps $\mathbf{C}$ des nombres complexes), ces fonctions sont également élémentaires.

Les fonctions élémentaires sont, pour ainsi dire, les fonctions d'avant le calcul intégral.

Il y a alors un théorème affirmant que certaines fonctions élémentaires n'ont pas de primitives élémentaires. Elles ont bien des primitives, mais «on ne peut pas les exprimer». Les plus courantes se voient donner un nom nouveau, ainsi le «sinus intégral», Si, est une primitive de $\sin(x)/x$, la «fonction d'erreur», erf, est (à un facteur d'échelle près) la primitive de e^{-x^2}, et ainsi de suite.

Cet article utilise la notion de corps différentiel pour démontrer ces résultats (et quelques autres). Un *corps différentiel* est un corps (commutatif) $(\mathbf{K}, +, .)$ muni d'une *dérivation*, c'est-à-dire d'une application $d : \mathbf{K} \to \mathbf{K}$, notée $a \mapsto d(a) = a'$, et telle que $(a+b)' = a' + b'$ et $(a.b)' = a'.b + a.b'$. Étant donné un corps différentiel $\mathbf{K}$, l'ensemble des a tels que $a' = 0$ est (trivialement) un sous-corps, noté $\mathrm{Con}(\mathbf{K})$, et appelé le corps des *constantes* de $\mathbf{K}$. Nous noterons par $\int f$ une primitive de f (c'est-à-dire un g tel que $g' = f$); deux primitives de f diffèrent par une constante, que nous négligerons désormais.

Les exemples usuels de corps différentiels sont des sous-corps de $\mathbf{M}$, le corps des fonctions méromorphes sur $\mathbf{C}$ (ou sur un ouvert de $\mathbf{C}$; à cause du principe du prolongement analytique, il est rarement nécessaire de préciser cet ouvert).

Étant donnés deux corps différentiels $\mathbf{F}$ et $\mathbf{G}$, où $\mathbf{F}$ est un sous-corps de $\mathbf{G}$ (au sens différentiel, c'est-à-dire que la dérivation de $\mathbf{G}$ prolonge celle de $\mathbf{F}$, ce que nous ne préciserons plus désormais), on dit que $\mathbf{G}$ est une *extension algébrique* de $\mathbf{F}$ si sa dimension (en tant que $\mathbf{F}$-espace vectoriel) est finie (et sinon, on dit que $\mathbf{G}$ est une extension transcendante).

On dit que $\mathbf{G}$ est une *extension logarithmique* de $\mathbf{F}$ si $\mathbf{G} = \mathbf{F}(t)$ pour un t transcendant (c'est-à-dire que $\mathbf{G}$ est une extension transcendante de $\mathbf{F}$) tel que $t' = s'/s$ pour un certain s de $\mathbf{F}$. On peut interpréter t comme étant $\ln(s)$, mais ce n'est pas nécessaire : il y a simplement un élément de $\mathbf{G}$ ayant la dérivée qui convient. De même, on dit que $\mathbf{G}$ est une extension exponentielle de $\mathbf{F}$ si $\mathbf{G} = \mathbf{F}(t)$ pour un t transcendant tel que $t' = t.s'$ pour un certain s de $\mathbf{F}$. Ici encore, nous pouvons considérer t comme étant $\exp(s)$, même s'il n'y a pas de véritable fonction exponentielle dans $\mathbf{F}$.

Enfin, nous dirons que $\mathbf{G}$ est une extension différentielle *élémentaire* de $\mathbf{F}$ s'il existe une chaîne finie de sous-corps allant de $\mathbf{F}$ à $\mathbf{G}$, où chaque sous-corps est une extension algébrique, logarithmique ou exponentielle du sous-corps précédent. Nous pouvons alors affirmer le

Théorème principal (Liouville-Rosenlicht). *Soient* $\mathbf{F}$ *et* $\mathbf{G}$ *deux corps différentiels,* $\mathbf{G}$ *étant une extension différentielle élémentaire de* $\mathbf{F}$*, avec* $\mathrm{Con}(\mathbf{F}) = \mathrm{Con}(\mathbf{G})$*; soient* $f \in \mathbf{F}$*,* $g \in \mathbf{G}$ *et* $g' = f$*. Il existe* $c_1, \ldots, c_n$ *appartenant à* $\mathrm{Con}(\mathbf{F})$ *et* $u_1, \ldots, u_n$ *et* v *appartenant à* $\mathbf{F}$*, tels que*

$$f = c_1 \frac{u_1'}{u_1} + \cdots c_n \frac{u_n'}{u_n} + v'.$$

Ce théorème, dans le cas particulier de $\mathbf{M}$, est dû à Liouville ; sa généralisation algébrique à Rosenlicht. Des théorèmes plus puissants du même type ont été prouvés par Risch, Davenport et d'autres, et sont au cœur des systèmes d'intégration symbolique.

Ainsi, les seules fonctions ayant des primitives élémentaires sont celles ayant la forme très particulière qu'on vient de voir, et ces primitives sont somme d'une fonction «de même complexité» que la fonction initiale (v), et de logarithmes de fonctions de même complexité (les u_i).

La démonstration de ce théorème figure dans la deuxième partie de cet article; nous allons commencer par donner des exemples d'applications à des preuves de non-intégrabilité.

Exemples de fonctions non intégrables élémentairement.

Dans les cas usuels, $\mathbf{F}$ et $\mathbf{G}$ sont des sous-corps de $\mathbf{M}$, et donc $\mathrm{Con}(\mathbf{F}) = \mathrm{Con}(\mathbf{G}) = \mathbf{C}$ est toujours vraie. Il faut remarquer que cette égalité est nécessaire, si l'on veut conserver à la notion de «fonction élémentaire» son sens usuel : sur $\mathcal{C}^\infty(\mathbf{R})$, la fonction $x \mapsto 1/(1+x^2)$ possède une primitive élémentaire, mais qui n'est pas de la forme logarithmique précédente...

Appliquons d'abord le théorème au cas de l'intégration de $f.\exp(g)$, où f et g sont des fonctions rationnelles. Si g est constante, il reste seulement une fonction rationnelle, qui peut être intégrée en décomposant en éléments simples. Supposons donc que g soit non constante. Soit $t = \exp(g)$, et donc $t' = g't$. Comme g est non constante, g a un pôle (éventuellement à l'infini) et donc $\exp(g)$ possède une singularité essentielle, et t est transcendante sur le corps des fractions rationnelles $\mathbf{C}(z)$. Soit $\mathbf{F} = \mathbf{C}(z)(t)$, et soit $\mathbf{G}$ une extension différentielle élémentaire contenant une primitive de $f.t$.

Le théorème de Liouville s'applique, et nous pouvons écrire

$$(*) \qquad f.t = c_1 \frac{u_1'}{u_1} + \cdots c_n \frac{u_n'}{u_n} + v',$$

avec les c_i constantes et les u_i et v dans $\mathbf{F}$. Chaque u_i est quotient de deux polynômes de $\mathbf{C}(z)[t]$, soit U/V. Mais $(U/V)'/(U/V) = U'/U - V'/V$ (dérivée logarithmique), nous pouvons donc réécrire la formule $(*)$ en supposant que chaque u_i est dans $\mathbf{C}(z)[t]$. De même, si un u_i se factorise ($u_i = U.V$), on aura $(U.V)'/(U.V) = U'/U + V'/V$; nous pouvons donc supposer en outre que chaque u_i est irréductible sur $\mathbf{C}(z)$.

À quoi ressemble un u'/u typique ? Par exemple, considérons le cas où u est du second degré en t. Si A, B et C sont des fonctions rationnelles sur $\mathbf{C}(z)$, il en est de même de A', B' et C' et

$$\frac{(At^2+Bt+C)'}{At^2+Bt+C} = \frac{(A'+2Ag')t^2+(B'+Bg')t+C'}{At^2+Bt+C}$$

(on remarquera que le degré d'un polynôme en t reste le même après différenciation. Nous prenons en effet les dérivées par rapport à z, et non à t. Si nous écrivons cela explicitement, il vient $(t^n)' = \exp(ng)' = ng' \exp(ng) = ng't^n$).

En général, chaque u'/u est un quotient de polynômes de mêmes degrés. À l'aide d'une division euclidienne, nous pouvons aussi l'écrire sous la forme $D + R/u$, avec $D \in \mathbf{C}(z)$, $R \in \mathbf{C}(z)[t]$, et avec $\deg(R) < \deg(u)$.

Décomposant en éléments simples, nous pouvons écrire v comme somme d'un polynôme de $\mathbf{C}(z)[t]$ et de fractions de la forme P/Q^n avec $\deg(P) < \deg(Q)$, Q irréductible, où chaque P et Q appartient à $\mathbf{C}(z)[t]$. Ainsi, v' sera la somme d'un polynôme et d'éléments simples.

Or tout cela est censé être exactement $f.t$. D'après l'unicité de la décomposition en éléments simples, tous les termes autres que les multiples de t ont donc une somme nulle. Seule la partie polynomiale de v peut contribuer à $f.t$, et ce terme doit donc être un monôme sur $\mathbf{C}(z)$. Ainsi, $f.t = (h.t)'$, pour une certaine fraction rationnelle h (la tentation d'affirmer ici $v = h.t$ est incorrecte, car il pourrait y avoir un terme de $\mathbf{C}(z)$, compensé par des termes de la forme u'/u. Nous avons seulement besoin d'identifier les termes de v qui contribuent à $f.t$, aussi cela n'a pas d'importance).

En résumé, si $f.\exp(g)$ a une primitive élémentaire, où f et g sont des fractions rationnelles et g est non nulle, alors cette primitive est de la forme $h.\exp(g)$, avec h rationnelle.

Nous allons examiner des exemples particulier de cette situation, et d'autres qui s'y ramènent (les exemples entre crochets, qui se ramènent à l'exemple principal par un changement de variables). Dans tous les cas qui suivent, la contradiction obtenue montre que la fonction n'a pas de primitive élémentaire.

1 e^{z^2} [$e^z\sqrt{z}$, $\dfrac{e^z}{\sqrt{z}}$]

Soit $h.e^{z^2}$ une de ses primitives. Alors $h' + 2zh = 1$, et $h = \exp(-z^2)\int \exp(z^2)$ n'a pas de pôles (sauf peut-être à l'infini), ainsi h, si rationnelle, doit être un polynôme. Mais la dérivée de h ne peut annuler le terme dominant de $2zh$, d'où la contradiction souhaitée.

2 $\dfrac{e^z}{z}$ [e^{e^z}, $\dfrac{1}{\ln z}$]

Soit $h.\exp(z)$ une primitive. On a alors $h' + h = 1/z$. Il y a deux façons rapides de montrer que h n'est pas rationnelle : on peut résoudre explicitement l'équation différentielle du premier ordre (obtenant $\exp(-z)\int(\exp(z)/z)$), et remarquer alors que la solution a une singularité logarithmique en 0 : ainsi, par exemple, $h(z)$ tend vers l'infini mais $h(z)\sqrt{z}$ tend vers 0 quand z tend vers 0; aucune fraction rationnelle n'a ce comportement. On peut aussi supposer que h est décomposée en éléments simples. Il est évident qu'aucun terme de h' ne donnera $1/z$, donc $1/z$ doit déjà être présent dans h. Mais $(1/z)' = -1/z^2$, et ce terme fait donc partie de h', il y a donc un $1/z^2$ dans h pour le compenser, puis un terme en $-2/z^3$, etc. Ceci conduit à une descente infinie impossible.

3 $\dfrac{\sin z}{z}$ [$\sin e^z$]et $\sin z^2$ [$\sqrt{z}\sin z$, $\dfrac{\sin(z)}{\sqrt{z}}$]

Comme $\sin z = \dfrac{e^{iz} - e^{-iz}}{2i}$, utilisons la même méthode que pour $f.\exp(g)$. Soit f une fonction rationnelle, soit $t = e^{iz}$ (ainsi $t'/t = i$) et soit $T = \exp(iz^2)$ (ainsi $T'/T = 2iz$); nous voulons une primitive soit de $f.(t - 1/t)/2i$, soit de $T - 1/T$.

Dans le premier cas, en identifiant dans la décomposition en éléments simples $(f.t)/2i$ et $(h.t)' = (h' + ih).t$ on obtient la même contradiction que précédemment. Dans le cas de $\sin z^2$, nous voulons $T/2i = (h.T)' = (h' + 2izh).T$, et comme précédemment, cela ne peut pas se produire.

Bien que cela suffise à conclure, poursuivons l'analyse dans le cas $f.\sin(z)$, car il y a encore des termes supplémentaires non examinés. Cette fois nous concluons qu'il y a, parmi v, un terme additionnel en k/t; nous avons donc $-f/2it = (k/t)' = (k' - ik)/t$. Ainsi la primitive de $f(t - 1/t)/2i$ est $h.t + k/t$. Si f est paire et réelle, h and k (comme $t = \exp(iz)$ et $1/t = \exp(-iz)$) sont images (par parité) l'une de l'autre, et comme on pouvait s'y attendre, la primitive est paire. Soit $C = \cos z$, $S = \sin z$, $h = H + iF$ et $k = K + iG$; la partie réelle de la primitive de f (et donc cette primitive elle-même) est $(HC - FS) + (KC + GS) = (H + K)C + (G - F)S$. Ainsi, sur les réels, nous voyons qu'une primitive (élémentaire, bien sûr) de $f \sin x$, où f est paire et rationnelle, est de la forme $g \cos x + h \sin x$, où g est rationnelle paire et h rationnelle impaire. Un résultat analogue a lieu pour $g \sin(x)$, (avec g impaire) $f \cos x$ et $g \cos x$. Comme une fonction rationnelle est somme de ses parties paires et impaires, $f \sin$ (si f est rationnelle) a pour primitive $g \sin + h \cos$ (avec g et h rationnelles), ou n'a pas de primitives élémentaires.

Revenant en arrière, appliquons cela à $\sin(x)/x$ directement, en restant dans $\mathbf{R}$. Si cette fonction a une primitive élémentaire, elle doit être de la forme $P.S + I.C$ (avec P paire et I impaire). En dérivant, on obtient $(P' - I).S + (P + I').C$. Comme pour la décomposition en éléments simples, nous avons ici une représentation unique dans $\mathbf{R}(x)\,[S, C]$ (c'est un peu délicat, à cause de la relation $S^2 = 1 - C^2$: cette étape peut être montrée directement, ou en résolvant pour les coefficients de t et de $1/t$ dans $\mathbf{C}$). Ainsi, $P' - I = 1/x$ et $P + I' = 0$, soit $I'' + I = -1/x$. Décomposant I en éléments simples, il est clair que seul $(-1/x)$ dans I peut produire le résultat. Il y a donc un terme en $-2/x^3$ dans I'', donc dans I pour l'annuler et ainsi de suite à l'infini. Ainsi, il n'y a pas de telle fonction rationnelle I.

4 $\dfrac{\arcsin z}{z}$ $[\, z \tan z \,]$

Nous nous plaçons dans le cas où $\mathbf{F} = \mathbf{C}(z, Z)(t)$, considéré comme un sous-corps de $\mathbf{M}$ (l'ensemble des fonctions méromorphes sur un certain domaine), où z est la fonction identité, où $Z = \sqrt{1 - z^2}$, et où t est $\arcsin z$. Alors $Z' = -z/Z$, et $t' = 1/Z$. Nous nous demandons si le résultat du théorème principal peut s'appliquer avec $a = t/z$ pour un certain corps $\mathbf{G}$. La fonction t est transcendante sur $\mathbf{C}(z, Z)$, puisqu'elle a une infinité de points de branchement.

Considérons donc la situation plus générale des fonctions de la forme $f(z).\arcsin z$, où $f(z)$ est rationnelle en z et en $z\sqrt{1 - z^2}$. En posant $z = 2w/(1 + w^2)$, on remarque que les éléments de $C(z, Z)$ sont toujours élémentairement intégrables. Comme $x^2 + y^2 - 1$ est irréductible, $\mathbf{C}\,[x, y]\,/(x^2 + y^2 - 1)$ est un anneau intègre, $\mathbf{C}(z, Z)$ est isomorphe à son corps des fractions de manière évidente, et $\mathbf{C}(z, Z)\,[t]$ est un anneau factoriel dont le corps des fractions satisfait le théorème de décomposition en éléments simples (de la variable t). Ce qui va suivre aura lieu parfois dans certaines extensions algébriques (en z) de $\mathbf{C}(z, Z)$ (qui pourront ne pas être factorielles), mais les termes obtenus devront se combiner pour donner des résultats appartenant à $\mathbf{C}(z, Z)(t)$, où la décomposition en éléments simples est unique, et ainsi les termes en t seront ce qu'affirme le théorème principal. Ainsi, une primitive élémentaire de $f(z) \arcsin z$ doit être une somme de u'/u et de v'.

Les termes en u peuvent, par dérivation logarithmique dans l'extension algébrique appropriée (rappelons que les racines d'une équation algébrique sont des fonctions analytique des coefficients, et que t est transcendant sur $\mathbf{C}(z, Z)$), être supposés tous de la forme $t + r$, avec r algébrique sur z. Alors $u'/u = (1/Z + r')/(t + r)$. Quand nous recombinons ces termes dans $\mathbf{C}(z, Z)$, ils ne forment pas un terme en t (ni une puissance supérieure de t, ni une constante).
La décomposition en éléments simples de v nous donne un polynôme en t, avec des coefficients dans $\mathbf{C}(z, Z)$, plus des multiples de puissances de termes affines en t, et comme précédemment ces derniers ne peuvent contribuer à un terme en t.
Si le polynôme est linéaire ou quadratique, disons $v = g.t^2 + h.t + k$, alors $v' = g'.t^2 + (2g/Z + h').t + (h/Z + k')$. Rien ne peut éliminer g', donc g est une constante, c, et alors $2c/Z + h' = f$, donc $\int(f.t) = 2c.t + \int(h'.t)$. $\int(h'.t)$ peut s'intégrer par parties. Ainsi la primitive devient $c \arcsin^2 z + h(z) \arcsin z - \int(h(z)/\sqrt{1 - z^2})$, et comme remarqué plus haut, ce dernier terme est élémentaire.
Si le polynôme est de degré ≥ 3, soit $v = A.t^n + B.t^(n - 1) + \cdots$, alors $v' = A'.t^n + (n.A/Z + B')t^{n-1} + \cdots$. A doit être une constante. Mais alors $nc/Z + B' = 0$, donc $B = -nct$, contradictoire avec $B \in C(z, Z)$.

En particulier, comme $1/z + c/\sqrt{1 - z^2}$ n'a pas de primitive rationnelle en z et $\sqrt{1 - z^2}$, $(\arcsin z)/z$ n'a pas de primitive élémentaire.

5 z^z

Dans ce cas, soit $\mathbf{F} = \mathbf{C}(z, l)(t)$, le corps des fonctions rationnelles en z, l et t, où $l = \ln z$ et $t = \exp(z.l) = z^z$. Remarquons que z, l et t sont algébriquement indépendants. Alors $t' = (l + 1).t$, donc prenant $a = t$ dans le théorème principal, la décomposition en éléments simples montre que la seule possibilité est que $v = w.t + \cdots$ soit la source du terme en t à gauche, avec w appartenant à $\mathbf{C}(z, l)$.

Égalant les coefficients en t, on obtient $1 = w' + (l + 1)w$. Ceci est une équation différentielle d'ordre 1, dont la solution est $w = \int(z^z)/z^z$. Nous devons donc prouver que ce w n'appartient pas à $\mathbf{C}(z, l)$. Supposons donc $w = P/Q$, avec P et Q éléments de $\mathbf{C}[z, l]$ sans facteurs communs. Alors $z^z = (z^z \times P/Q)' = z^z\big((1 + l)PQ + P'Q - PQ'\big)/Q^2$, et donc $Q^2 = (1 + l)PQ + P'Q - PQ'$. Ainsi Q divise Q' ; Q est donc une constante, que nous pouvons donc prendre égale à 1. Nous sommes donc ramenés à $P' + P + lP = 1$.

Soit $P = \sum_{i=0}^{n} P_i l^i$, avec $P_i \in \mathbf{C}[z]$ pour $0 \leq i \leq n$. Alors dans notre équation subsiste un terme en $P_n l^{n+1}$, d'où la contradiction cherchée.

Débordant légèrement du sujet, il faut remarquer que ce théorème de Liouville ne permet pas de montrer que les fonctions de Bessel ne sont pas élémentaires, puisqu'elles sont définies par des équations différentielles d'ordre 2 (et non exprimables à l'aide de quadratures). Ce genre de résultat s'obtient à l'aide d'une théorie plus profonde : la théorie de Galois différentielle. Une variante du théorème de Liouville, utilisant une forme normale différente, permet cependant de montrer, par exemple, que J_0 ne peut être intégrée à l'aide des fonctions élémentaires augmentées des fonctions de Bessel.

Preuve du théorème principal.

Ce qui suit est une esquisse raisonnablement complète de la démonstration, supposant toutefois une certaine familiarité avec la théorie (élémentaire) des extensions algébriques.

Commençons par quelques lemmes faciles (sous cette hypothèse). Dans chacun d'eux, $\mathbf{F}$ est un corps différentiel, et t est transcendant sur $\mathbf{F}$.

Lemme 1. *Si $\mathbf{K}$ est une extension algébrique de $\mathbf{F}$, il existe dans $\mathbf{K}$ une extension unique de la dérivation différentielle de $\mathbf{F}$, qui fait de $\mathbf{K}$ un corps différentiel.*

Lemme 2. *Si $\mathbf{K} = \mathbf{F}(t)$ est un corps différentiel dont la dérivation prolonge celle de $\mathbf{F}$, et si $t' \in \mathbf{F}$, alors pour tout polynôme $f(t)$ dans $\mathbf{F}[t]$, $f(t)'$ est un polynôme de $F[t]$ de même degré (si le coefficient dominant n'appartient pas à $\mathrm{Con}(\mathbf{F})$) ou du degré immédiatement inférieur (si le coefficient dominant appartient à $\mathrm{Con}(\mathbf{F})$).*

Lemme 3. *Si $\mathbf{K} = \mathbf{F}(t)$ est un corps différentiel dont la dérivation prolonge celle de $\mathbf{F}$, et si $(t'/t) \in \mathbf{F}$, alors pour tout $a \in \mathbf{F}$ et pour tout n entier positif, il existe $h \in \mathbf{F}$ tel que $(at^n)' = ht^n$. Plus généralement, si $f(t)$ est un polynôme quelconque de $\mathbf{F}[t]$, alors $f(t)'$ est du même degré que $f(t)$, et est un multiple de $f(t)$ si, et seulement si, $f(t)$ est un monôme.*

Ces trois lemmes sont raisonnablement élémentaires. Par exemple, $(a * t^n)' = (a' + at'/t) * t^n$ dans le lemme 3. L'équivalence finale du lemme 3 est l'endroit où la transcendance de t intervient. D'autre part, le lemme 1, dans le cas usuel des sous-corps de $\mathbf{M}$, est une conséquence facile du théorème des fonctions implicites.

Réaffirmons le

Théorème principal. *Soit $\mathbf{F}$ et $\mathbf{G}$ des corps différentiels, $a \in \mathbf{F}$, $y \in \mathbf{G}$, et supposons que $y' = a$ et que $\mathbf{G}$ soit une extension différentielle élémentaire de $\mathbf{F}$, avec $\mathrm{Con}(\mathbf{F}) = \mathrm{Con}(\mathbf{G})$. Il existe alors $c_1, ..., c_n$ dans $\mathrm{Con}(\mathbf{F})$, $u_1, ..., u_n$, v dans $\mathbf{F}$ tels que*

$$(*) \qquad a = c_1 \frac{u_1'}{u_1} + \cdots c_n \frac{u_n'}{u_n} + v'.$$

Démontration :

Par hypothèse, il y a une chaîne finie de corps entre $\mathbf{F}$ et $\mathbf{G}$ tels que chaque corps est une extension algébrique, logarithmique ou exponentielle du précédent. Nous allons montrer que si a est de la forme $(*)$ avec les u_i et v dans $\mathbf{F}_2$, et si $\mathbf{F}_2$ est de l'un des trois types possibles d'extensions de $\mathbf{F}_1$, alors a peut se mettre sous la forme $(*)$ avec des u_i et v dans F_1. Comme la forme $(*)$ est évidemment obtenue dans $\mathbf{G}$ (en prenant tous les c nuls, les u égaux à 1 et v le y initial tel que $y' = a$), par récurrence descendante, on voit que la forme $(*)$ sera obtenue avec des u_i et v dans $\mathbf{F}$, ce qui démontrera le théorème.

Nous pouvons donc supposer que $\mathbf{G} = \mathbf{F}(t)$.

Cas 1 : t est algébrique sur $\mathbf{F}$. Soit P le polynôme minimal de t (de degré k). Il y a des polynômes U_i et V tels que $U_i(t) = u_i$ et $V(t) = v$. Nous avons donc

$$(**) \qquad a = c_1 \frac{U_1'(t)}{U_1(t)} + \cdots c_n \frac{U_n'(t)}{U_n(t)} + V'(t).$$

D'après l'unicité du prolongement des dérivations dans le cas algébrique, nous pouvons remplacer t par un quelconque de ses conjugués t_1, ..., t_k (les racines de P), et la formule $(**)$ reste vraie. Autrement dit, a appartenant à $\mathbf{F}$, a est invariant par les automorphismes de Galois. Additionnant $(**)$ pour tous les conjugués, et convertissant

les termes de la forme U'/U en produits à l'aide de la dérivée logarithmique, nous obtenons

$$ka = c_1 \frac{(U_1(t_1) \times \cdots \times U_1(t_k))'}{U_1(t_1) \times \cdots \times U_1(t_k)} + \cdots + c_n \frac{(U_n(t_1) \times \cdots \times U_n(t_k))'}{U_n(t_1) \times \cdots \times U_n(t_k)} + V(t_1) + \cdots + V(t_k)$$

Mais les produits $U_i(t_1) \times \cdots \times U_i(t_k)$ sont des polynômes symétriques en t_i à coefficients dans $\mathbf{F}$, et donc dans F. Ainsi, $(*)$ est vrai dans $\mathbf{F}$.

Cas 2 : t est logarithmique sur $\mathbf{F}$. Par dérivation logarithmique, nous pouvons supposer que les u sont distincts et premiers (en t, c'est-à-dire non factorisables dans $\mathbf{F}(t)$) De plus, nous pouvons supposer que v a été décomposée en éléments simples, et ces éléments ne peuvent être que de la forme f/g^j, où $\deg(f) < \deg(g)$ et g est premier.

Soit $t' = s'/s$, pour un $s \in \mathbf{F}$. Si $f(t)$ est dans $\mathbf{F}[t]$, il en est de même de $f(t)'$; si f est premier, f et f' ne peuvent avoir de facteur commun. En particulier, les termes en u'/u sont déjà sous forme réduite. Les termes en f/g^j de v, contribuent au dénominateur de v' par un terme (en g^{j+1}) de la forme $-jfg'/g^{j+1}$. Mais g ne divise pas fg', et les termes ne peuvent donc pas se simplifier. Il en va de même des termes en u'/u, puisque les u sont premiers, et aucun terme en $-jfg'/g^{j+1}$ n'apparaît dans a, car a est élément de $\mathbf{F}$. Ainsi, il n'y a aucun terme de la forme f/g^j dans v. Mais alors tous les u doivent appartenir à $\mathbf{F}$, car il n'y aurait pas de termes pour les compenser autrement. (rappelons que les u sont distincts et premiers). Ainsi les u sont dans $\mathbf{F}$, et v est un polynôme. Mais $v' = a-$ une expression en u, donc v' est aussi élément de $\mathbf{F}$. Ainsi $v = bt + c$ avec $b \in \mathrm{Con}(\mathbf{F})$ et $c \in \mathbf{F}$, d'après le lemme 2. Alors

$$a = c_1 \frac{u_1'}{u_1} + \cdots c_n \frac{u_n'}{u_n} + b\frac{s'}{s} + c'$$

est la forme cherchée, ce qui achève le cas 2.

Cas 3 : t est exponentiel sur $\mathbf{F}$. Soit $t'/t = s'$ pour un certain s in $\mathbf{F}$. Comme dans le cas 2, nous pouvons supposer que tous les u sont distincts et premiers, et décomposer v en éléments simples. En fait, le raisonnement est identique, jusqu'au moment où nous voulons déterminer la forme de v. Le lemme 3 nous dit alors que v est une somme finie de termes $b*t^j$ où chaque coefficient est dans $\mathbf{F}$. Chacun des u est aussi dans $\mathbf{F}$, sauf peut-être un terme égal à t. Ainsi chaque terme u'/u est dans $\mathbf{F}$, et nous concluons encore que $v' \in \mathbf{F}$. D'après le lemme 3, $v \in \mathbf{F}$. Si tous les u sont dans $\mathbf{F}$, a est de la forme cherchée. Sinon, un des u, mettons u_n, est en fait t, et alors

$$a = c_1 \frac{u_1'}{u_1} + \cdots c_n \frac{u_n'}{u_n} + (c_n s + v)'$$

est de la forme voulue, ce qui conclut le cas 3.

Références :

A. D. Fitt & G. T. Q. Hoare *«The closed-form integration of arbitrary functions»* , Mathematical Gazette (1993), pp 227-236.
I. Kaplansky Introduction to differential algebra (Hermann, 1957)
E. R. Kolchin Differential algebra and algebraic groups (Academic Press, 1973)
A. R. Magid Lectures on differential Galois theory (AMS, 1994)
E Marchisotto & G Zakeri *«An invitation to integration in finite terms»*, College Mathematics Journal (1994), pp 295-308.
J. F. Ritt Integration in finite terms (Columbia, 1948).
J. F. Ritt Differential algebra (AMS, 1950).

M. Rosenlicht *«Liouville's theorem on functions with elementary integrals»*, Pacific Journal of Mathematics (1968), pp 153-161.
M. Rosenlicht *«Integration in finite terms»*, American Mathematics Monthly, (1972), pp 963-972.
G. N. Watson A treatise on the theory of Bessel functions (Cambridge, 1962).