SIAM J. COMPUT.
Vol. 14, No. 4, November 1985

015

AN EXTENSION OF LIOUVILLE'S THEOREM ON INTEGRATION IN FINITE TERMS*

M. F. SINGER†, B. D. SAUNDERS‡ AND B. F. CAVINESS§

Abstract. In Part I of this paper, we give an extension of Liouville's Theorem and give a number of examples which show that integration with special functions involves some phenomena that do not occur in integration with the elementary functions alone. Our main result generalizes Liouville's Theorem by allowing, in addition to the elementary functions, special functions such as the error function, Fresnel integrals and the logarithmic integral (but not the dilogorithm or exponential integral) to appear in the integral of an elementary function. The basic conclusion is that these functions, if they appear, appear linearly. We give an algorithm which decides if an elementary function, built up using only exponential functions and rational operations has an integral which can be expressed in terms of elementary functions and error functions.

Key words. Liouville's theorem, integration in finite terms, special functions, error function

Introduction. In 1969 Moses [MOSE69] first raised the possibility of extending the Risch decision procedure for indefinite integration to include a certain class of special functions. Some of his ideas have been incorporated as heuristic methods in MACSYMA and REDUCE. However, little progress has been made on the theory necessary to extend the Risch algorithm. One step in this direction was the paper by Moses and Zippel [MOZI79] in which a weak Liouville Theorem was given for special functions (this result also appears in [SING77]).

In Part I of this paper, we give an extension of Liouville's Theorem [RISC69, p. 169] and give a number of examples which show that integration with special functions involves some phenomena that do not occur in integration with the elementary functions alone. Our main result generalizes Liouville's Theorem by allowing, in addition to the elementary functions, special functions such as the error function, Fresnel integrals and the logarithmic integral (but not the dilogorithm or exponential integral) to appear in the integral of an elementary function. The basic conclusion is that these functions, if they appear, appear linearly.

In Part II of this paper, we use the results of Part I to examine the question of when the integral of an elementary function can be expressed in terms of elementary functions and error functions. We give an algorithm which decides if an elementary function, built up using only exponential functions and rational operations has an integral which can be expressed in terms of elementary functions and error functions.

Some of the results of this paper have been announced in [SSC81]. We wish to thank Barry Trager for drawing our attention to Example 2.1 in § 2.

Finally, all fields in this paper are assumed to be of characteristic 0. **C**, **Q** and **Z** stand for the complex numbers, rational numbers, and integers respectively.

I. An extension of Liouville's Theorem.

1. Statement and discussion of results. We begin by defining a generalization of the elementary functions. Let F be a differential field of characteristic 0 with derivation

* Received by the editors March 19, 1982, and in final revised form July 5, 1984.

† Department of Mathematics, North Carolina State University, Raleigh, North Carolina 27650.

‡ Department of Mathematical Sciences, Rensselaer Polytechnic Institute, Troy, New York, 12181. The work of this author was supported in part by the National Science Foundation under grant MCS79-09158.

§ Department of Computer and Information Sciences, University of Delaware, Newark, Delaware 19711. The work of this author was supported in part by the National Science Foundation under grant MCS79-09158.

and constants C. Let A and B be finite indexing sets and let

$$\mathscr{E} = \{G_\alpha(\exp R_\alpha(Y))\}_{\alpha \in A},$$
$$\mathscr{L} = \{H_\beta(\log S_\beta(Y))\}_{\beta \in B},$$

be sets of expressions where:

(1) G_α, R_α, H_β, S_β are in $C(Y)$ for all $\alpha \in A$, $\beta \in B$, i.e. they are all rational functions with constant coefficients;

(2) for all $\beta \in B$, if $H_\beta(Y) = P_\beta(Y)/Q_\beta(Y)$ with P_β, Q_β in $C[Y]$, then $\deg P_\beta \leqq \deg Q_\beta + 1$.

We say that a differential extension E of F is an *$\mathscr{E}\mathscr{L}$-elementary extension* of F if there exists a tower of fields $F = F_0 \subset F_1 \subset \cdots \subset F_n = E$ such that $F_i = F_{i-1}(\theta_i)$ where for each i, $1 \leqq i \leqq n$, one of the following holds:

(i) θ_i is algebraic over F_{i-1};
(ii) $\theta_i' = u'\theta_i$ for some $u \in F_{i-1}$;
(iii) $\theta_i' = u'/u$ for some nonzero $u \in F_{i-1}$;
(1.1) (iv) for some $\alpha \in A$, there are u, $v \in F_{i-1}$ such that $\theta_i' = u' G_\alpha(v)$ where $v' = (R_\alpha(u))'v$;
(v) for some $\beta \in B$, there are u, v in F_{i-1} such that $\theta_i' = u' H_\beta(v)$ where $v' = (S_\beta(u))'/S_\beta(u)$ and $S_\beta(u) \neq 0$.

Informally, we could write (1.1) cases (ii)-(v) as
(ii′) $\theta_i = \exp u$;
(iii′) $\theta_i = \log u$;
(iv′) $\theta_i = \int u' G_\alpha(\exp R_\alpha(u))\, dx$;
(v′) $\theta_i = \int u' H_\beta(\log S_\beta(u))\, dx$.

Cases (ii)-(iv) and (ii′)-(iv′) are not equivalent since, for example, (ii) determines θ_i up to a multiplicative constant while (ii′) refers to a specific function, exp. Although this distinction is not usually emphasized in the standard Liouville Theorem, it is not a pedantry here. The distinction between (iv)-(v) and (iv′)-(v′) is crucial to prevent transcendental constants from being introduced by integration. This will be discussed in detail in § 2.

The definition of $\mathscr{E}\mathscr{L}$-elementary functions is broad enough to include such functions as the error function, the Fresnel integrals and the logarithmic integral. Let $F = \mathbf{C}(x)$, $\mathbf{C}$ the complex numbers. The error function is defined by

$$\operatorname{erf}(u) = \int u' \, e^{-u^2} \, dx$$

where $G_\alpha(\exp R_\alpha(Y)) = \exp(-Y^2)$ with $G_\alpha(W) = W$ and $R_\alpha(Y) = -Y^2$.

The Fresnel integrals are defined by

$$S(u) = \int u' \sin\left[\frac{\pi}{2} u^2\right] dx,$$

$$C(u) = \int u' \cos\left[\frac{\pi}{2} u^2\right] dx.$$

For $S(u)$ we have that

$$G_\alpha(\exp R_\alpha(Y)) = \frac{[e^{i\pi/2\,Y^2}]^2 - 1}{2i\, e^{i\pi/2\,Y^2}}$$

where $G_\alpha(W)=(W^2-1)/2iW$ and $R_\alpha(Y)=i\pi Y^2/2$. For $C(u)$ we have a similar expression.

The logarithmic integral is defined by

$$\mathrm{li}\,(u)=\int \frac{u'}{\log u}\,dx$$

with $H_\beta(W)=1/W$ and $S_\beta(Y)=Y$.

$\mathscr{E}\mathscr{L}$-elementary functions do not include the dilogarithm (or Spence function) defined by

$$\mathrm{Li}_2\,(u)=-\int \frac{u'\log u}{u-1}\,dx$$

nor the exponential integral

$$\mathrm{Ei}\,(u)=\int \frac{u'e^u}{u}\,dx$$

since they both violate condition (1) of the definition. Of course, $\mathrm{Ei}\,(u)=\mathrm{li}\,(e^u)$, so the exponential integral is implicitly covered by our analysis. One would like a theory that explicitly includes these functions but this remains an open problem.

We can now state the generalization of Liouville's Theorem.

THEOREM 1.1. *Let F be a differential field of characteristic zero with an algebraically closed subfield of constants C. Let γ be in F and assume there exist an $\mathscr{E}\mathscr{L}$-elementary extension E of F and an element y in E such that $y'=\gamma$. Then there exist constants a_i, $b_{i\alpha}$, $c_{i\beta}$ in C, w_i in F, and $u_{i\alpha}$, $u_{i\beta}$, $v_{i\alpha}$, $v_{i\beta}$, algebraic over F, such that*

$$\gamma=w_0'+\sum_{i=1}^{n} a_i\frac{w_i'}{w_i}+\sum_{\alpha\in A}\sum_{i\in I_\alpha} b_{i\alpha}u_{i\alpha}'G_\alpha(v_{i\alpha})+\sum_{\beta\in B}\sum_{i\in J_\beta} c_{i\beta}u_{i\beta}'H_\beta(v_{i\beta}) \tag{1.2}$$

where I_α and J_β are finite sets of integers for all α and β and

$$v_{i\alpha}'=(R_\alpha(u_{i\alpha}))'v_{i\alpha},\qquad v_{i\beta}'=\frac{(S_\beta(u_{i\beta}))'}{S_\beta(u_{i\beta})},\qquad S_\beta(u_{i\beta})\neq 0$$

for all α, β and i.

The proof of Theorem 1.1 will be given in § 3. Now some comments about the hypotheses and conclusion of the theorem.

Condition (2) in the first paragraph of this section seems artificial, but the theorem is false without it. Consider the following example.

Example 1.1. Let $F=\mathbf{C}(x,\log x)$, where $\mathbf{C}$ is the field of complex numbers, $\mathscr{E}=\varnothing$ and $\mathscr{L}=\{(\log Y(Y+1))^2\}$. In this case the index set B is a singleton and $H=Y^2$. This is excluded by condition (2) since deg (numerator of H) $=2>$ deg (denominator of H) $+1$.

Claim. (a) $\int \log x/(x+1)$ lies in an $\mathscr{E}\mathscr{L}$-elementary extension of F but (b) $\log x/(x+1)\neq w_0'+\sum c_i w_i'/w_i+\sum d_i u_i' v_i^2$ for any w_i, u_i, v_i algebraic over F with $v_i'=(u_i(u_i+1))'/u_i(u_i+1)$ and constants c_i, d_i in $\mathbf{C}$.

To verify (a), compute $\int(\log x(x+1))^2\,dx$ by parts. First we have that

$$\int(\log x)^2\,dx=x(\log x)^2-2x\log x+2x,$$

$$\int(\log(x+1))^2\,dx=(x+1)(\log(x+1))^2-2(x+1)\log(x+1)+2(x+1),$$

and

$$\int (\log x)(\log (x+1))\,dx = x(\log x)\log(x+1) - (x+1)\log(x+1) - \log x + 2x + \int \frac{\log x}{x+1}\,dx.$$

Hence

$$\begin{aligned}\int (\log x(x+1))^2\,dx &= \int (\log x + \log(x+1))^2\,dx \\ &= \int (\log x)^2 + 2\int (\log x)(\log(x+1))\,dx + \int (\log(x+1))^2\,dx \\ &= \text{elementary function} + 2\int \frac{\log x}{x+1}\,dx.\end{aligned}$$

To verify (b) assume that $\log x/(x+1) = w_0' + \sum_{i=1}^n c_i w_i'/w_i + \sum_{i=1}^m d_i u_i' v_i^2$ with w_i, u_i, v_i algebraic over F and $v_i' = (u_i(u_i+1))'/u_i(u_i+1)$. From the structure theorem ([ROCA79, p. 359]), we have for each i, $1 \leqq i \leqq m$, that $u_i(u_u+1) = c_i x^{r_i}$ for some rational number r_i and $c_i \in \mathbf{C}$. We can assume that neither c_i nor r_i is zero. We also have $v_i = r_i \log x + k_i$ for some $k_i \in \mathbf{C}$. Furthermore, each u_i is algebraic over $K = \mathbf{C}(x, \log x, x^{r_1}, \cdots, x^{r_m})$ and satisfies the irreducible equation $u(u+1) - c_i x^{r_i} = 0$. Letting Tr be the trace function from $K(u_1, \cdots, u_m)$ to K, we see from this equation that $\operatorname{Tr}(u_i)$ is an integer. Therefore, $\operatorname{Tr}(u_i') = (\operatorname{Tr} u_i)' = 0$. Apply the trace to both sides of

$$\frac{\log x}{x+1} = w_0' + \sum c_i \frac{w_i'}{w_i} + \sum d_i u'(r_i \log x + k_i)^2$$

to obtain

$$\mu \frac{\log x}{x+1} = (\operatorname{Tr} w_0)' + \sum c_i \frac{(Nw_i)'}{Nw_i}$$

where μ is a positive integer and Nw_i is the norm of w_i. This contradicts the fact that $\int \log x/(x+1)$ is not elementary and hence (b) is verified.

Unlike the standard Liouville Theorem, the above theorem only guarantees that there exist w_i, $u_{i\alpha}$, $u_{i\beta}$, $v_{i\alpha}$, $v_{i\beta}$, *algebraic* over F such that (1.2) holds. One would have hoped that these elements could be chosen to lie in F but this is not the case in general.

Example 1.2. Let $F = \mathbf{C}(x, \exp x, \exp(-\exp x + x/2))$, $\mathscr{E} = \{\exp(-Y^2)\}$, $\mathscr{L} = \emptyset$. Note that F is a purely transcendental extension of $\mathbf{C}$.

Claim. (a) $\int \exp(-\exp x + x/2)\,dx$ lies in an $\mathscr{E}\mathscr{L}$-elementary extension of F. (b) $\exp(-\exp x + x/2) \neq w_0' + \sum c_i w_i'/w_i + \sum d_i u_i' v_i$, where $v_i' = (-2u_i u_i')v_i$, for any w_i, u_i, v_i *in* F.

To verify (a), we see that

$$\int \exp\left(-\exp x + \frac{x}{2}\right) dx = \int \exp(-\exp x)\exp\left(\frac{x}{2}\right) dx = \sqrt{\pi}\,\operatorname{erf}\left(\exp\frac{x}{2}\right).$$

Note that $\exp(x/2) \notin F$.

To verify (b), assume such an expression existed. By the structure theorem in [ROCA79], we have $u_i^2 = r_i(\exp x + x/2) + s_i x + a_i$ where r_i and s_i are rational numbers and $a_i \in \mathbf{C}$. Since F is a purely transcendental extension of $\mathbf{C}$, this is only possible if

$r_i = s_i = 0$ and $u_i \in \mathbf{C}$. Therefore we would have $\exp(-\exp x + x/2) = w_0' + \sum c_i w_i'/w_i$, contradicting the fact that the error function is not elementary.

2. The question of constants. In this section we will discuss the question of transcendental constants appearing in our integral when we express this integral in terms of $\mathscr{E}\mathscr{L}$-elementary functions. We will rely heavily on the notion of a constrained extension of a differential field and other concepts from differential algebra. We refer the reader to [KOL73] as a general reference for differential algebra and explicitly to page 142 for an exposition of the concept of constrained extension.

We quote two facts from [KOL73]: 1) Let F be a differential field of characteristic 0, P a differential ideal in the ring of differential polynomials $F\{y_1, \cdots, y_n\}$ and B a differential polynomial in $F\{y_1, \cdots, y_n\}$ such that $B \notin P$. There exist elements $\eta_1, \cdots, \eta_n$ in some extension of F such that $(\eta_1, \cdots, \eta_n)$ is a zero of P, $B(\eta_1, \cdots, \eta_n) \neq 0$ and $(\eta_1, \cdots, \eta_n)$ is constrained over F; 2) Let F be as before. If $(\eta_1, \cdots, \eta_n)$ is constrained over F, then the constants of $F\langle \eta_1, \cdots, \eta_n \rangle$ are algebraic over the constants of F.

PROPOSITION 2.1. *Let F be a differential field of characteristic* 0, *I a differential ideal in $F\{y_1, \cdots, y_m\}$ and $D \in F\{y_1, \cdots, y_n\}$ such that $D \notin I$. If there exist an $\mathscr{E}\mathscr{L}$-elementary extension E of F and elements $\zeta_1, \cdots, \zeta_m$ in E such that $(\zeta_1, \cdots, \zeta_m)$ is a zero of I with $D(\zeta_1, \cdots, \zeta_m) \neq 0$, then there exists an $\mathscr{E}\mathscr{L}$-elementary extension $\bar{E}$ of F, whose constants are algebraic over the constants of F, and $\bar{\zeta}_1, \cdots, \bar{\zeta}_m) \neq 0$.*

Proof. Let $E = F(\theta_1, \cdots, \theta_n)$ where each θ_i satisfies (i), (ii), (iii), (iv) or (v) of (1.1). Each of these conditions defines θ_i in terms of differential equations involving elements of $F(\theta_1, \cdots, \theta_{i-1})$. These elements can be written as quotients of elements in $F[\theta_1, \cdots, \theta_{i-1}]$. Let C_i be the product of the denominators of all elements of $F(\theta_1, \cdots, \theta_{i-1})$ appearing in the definition of θ_i. Similarly each ζ_i can be written as $\zeta_i = A_i(\theta_1, \cdots, \theta_n)/B_i(\theta_1, \cdots, \theta_n)$. Let $G(y_1, \cdots, y_n) = D(\prod_{i=1}^m B_i)(\prod_{i=1}^n C_i)$. We can write $F\{\theta_1, \cdots, \theta_n\}$ as $F\{y_1, \cdots, y_n\}/P$ for some prime differential ideal P. Note that $G \notin P$ and $I \subset P$. Using 1) above, we can find $\eta_1, \cdots, \eta_n$, constrained over F such that $(\eta_1, \cdots, \eta_n)$ is a zero of P and $G(\eta_1, \cdots, \eta_n) \neq 0$. One can easily check that $F\langle \eta_1, \cdots, \eta_n \rangle$ is an $\mathscr{E}\mathscr{L}$-elementary extension of F which, by fact 2) above, has constants which are at worst algebraic over the constants of F. Furthermore, letting $\bar{\zeta}_i = A_i(\eta_1, \cdots, \eta_n)/B_i(\eta_1, \cdots, \eta_n)$, we have that $(\bar{\zeta}_1, \cdots, \bar{\zeta}_m)$ is a zero of I and $D(\bar{\zeta}_1, \cdots, \bar{\zeta}_m) \neq 0$. □

COROLLARY 2.2. *Let F be a differential field of characteristic* 0 *and $\gamma \in F$. If $y' = \gamma$ has a solution in some $\mathscr{E}\mathscr{L}$-elementary extension of F, then $y' = \gamma$ has a solution in some $\mathscr{E}\mathscr{L}$-elementary extension of F whose constants are algebraic over the constants of F.*

Proof. Let ζ be a solution of $y' = \gamma$ lying in an $\mathscr{E}\mathscr{L}$-elementary extension of F and let $F\{\zeta\} = F\{y\}/I$ for some prime differential ideal I. Let $D = 1$ and apply Proposition 2.1. □

As mentioned in § 1, we took care to define $\mathscr{E}\mathscr{L}$-elementary functions in terms of differential equations without explicitly mentioning the functions exp and log. This is to prevent the appearance of constants that are generated transcendentally, e.g., as values of exp or log. If we insist upon using the functions exp and log, i.e. those functions satisfying $y' = y$, $y(0) = 1$ and $y' = 1/x$, $y(1) = 0$ respectively, we are forced to deal with this kind of constant as the following example shows.

Example 2.1. Let $\mathbf{Q}$ be the rational numbers and let $F = \mathbf{Q}(x, \exp(-x^2+1))$, $\mathscr{E} = \{\exp(-Y^2)\}$, $\mathscr{L} = \varnothing$, and $\gamma = \exp(-x^2+1)$.

Claim. (1) There exist u, v in F such that $\gamma = u'v$ where $v' = (-u^2)'v$ and so, a fortiori, there is an $\mathscr{E}\mathscr{L}$-elementary extension E of F, with the same constants as F, and a y in E such that $t' = \gamma$.

(2) γ cannot be written as $\gamma = w_0' + \sum c_i(w_i'/w_i) + \sum d_i u_i' \exp(-u_i^2)$ for any elements w_i, u_i, $\exp(-u_i^2)$ algebraic over F and constants c_i, d_i algebraic over Q.

To prove claim (1), let $u = x$, $v = \exp(-x^2+1)$. Then $u' = 1$ and $v' = (-x^2+1)'v = (-x^2)'v = (-u^2)'v$. Let θ be defined by $\theta' = u'v$. One can show that θ is transcendental over F and that $F(\theta)$ has the same field of constants as F. $E = F(\theta)$ is then an $\mathscr{E}\mathscr{L}$-elementary extension of F and $y = \theta$ satisfies $y' = \gamma$.

To prove claim (2), assume that we could write

$$\exp(-x^2+1) = w_0' + \sum_{i=1}^{n} c_i \frac{w_i'}{w_i} + \sum_{i=1}^{m} d_i u_i' \exp(-u_i^2), \tag{2.1}$$

with w_i, u_i, $\exp(-u_i^2)$ algebraic over F and constants c_i, d_i algebraic over $\mathbf{Q}$, and m as small as possible. Since u_i^2 and $\exp(-u_i^2)$ are algebraic over $\mathbf{Q}(x, \exp(-x^2+1))$ we have, by [ROS76, Thm. 2], each u_i is algebraic over $\mathbf{Q}(x)$. We now apply an old result of Liouville (see [RITT48, p. 49] or [ROS75, p. 295] for a modern proof): If $f_1, \cdots, f_k, g_1, \cdots, g_k$ are algebraic functions, such that no two of the g_i differ by a constant, then $f_1 \exp(g_1) + \cdots + f_k \exp(g_k)$ is the derivative of an elementary function if and only if each $f_i \exp(g_i)$ is. To apply this result rewrite (2.1) as

$$\exp(-x^2+1) + \sum d_i u_i' \exp(-u_i^2) = w_0' + \sum c_i \frac{w_i'}{w_i}.$$

Since $\int \exp(-x^2+1)$ is not elementary, we have either: (i) $-u_i^2$ and $-u_i^2$ differ by a constant for some $i \neq j$, or (ii) $-x^2+1$ and $-u_i^2$ differ by a constant for some i. In case (i), we see that the constant (which is algebraic over $\mathbf{Q}$) must be 0, otherwise $\exp(-u_i^2)(\exp(-u_j^2))^{-1}$ would be a transcendental constant lying in an algebraic extension of F, a contradiction. We must therefore have $-u_i^2 = -u_j^2$ so $u_i = \pm u_j$. This implies that we could combine terms in (2.1) to yield an expression with smaller m. In case (ii), the constant again must be zero., Therefore $-x^2+1 = -u_i^2$ for some i. Letting $I = \{i \mid -u_i^2 = -x^2+1\}$ and $J = \{i \mid -u_i^2 \neq x^2+1\}$ we have

$$\left(1 + \sum_{i \in I} d_i u_i'\right) \exp(-x^2+1) + \sum_{i \in J} d_i u_i' \exp(-u_i^2) = w_0' + \sum c_i w_i'/w_i.$$

Applying the result of Liouville and the previous argument, we must get $J = \varnothing$ and so

$$\left(1 + \sum_{i \in I} d_i u_i'\right) \exp(-x^2+1) = w_0' + \sum c_i \frac{w_i'}{w_i}.$$

Since $\int \exp(-x^2+1)\,dx$ is not elementary we must have $1 + \sum d_i u_i' = 0$. Since $-u_i^2 = x^2+1$, we have $\mathrm{Tr}(u_i) = 0$, where Tr is the trace with respect to the extension $\mathbf{Q}(x, u_1, \cdots, u_m)$ of $\mathbf{Q}(x)$. Therefore, $0 = \mathrm{Tr}(1 + \sum d_i u_i') = 1 + \sum d_i(\mathrm{Tr}(u_i))' = 1$, a contradition. □

3. Proof of Theorem 1.1. We will need the following three easy lemmas.

LEMMA 3.1. *Let k be a field containing the algebraic closure of the rationals and let X and Y be indeterminants. Let $A(Y)$ and $B(Y)$ be relatively prime elements of $k[Y]$. Furthermore, assume A/B is not an nth power in $k(Y)$ for any positive integer n. Then the polynomial $B(Y)X^m - A(Y)$ is irreducible in $k(X)[Y]$ for any positive integer m.*

Proof. By Gauss's Lemma $B(Y)X^m - A(Y)$ factors in $k(X)[Y]$ if and only if it factors in $k[X, Y]$ if and only if $X^m - A(Y)/B(Y)$ factors in $k(Y)[X]$. Now apply [LANG65, Thm. 16, p. 221]. □

LEMMA 3.2. *Let k be a field, X and Y indeterminants, and $A(Y)$ and $B(Y)$ relatively prime elements of $k[Y]$. If a and b are elements of k with $a \neq 0$, then $A(Y)-(aX+b)B(Y)$ is irreducible in $k(X)[Y]$.*

Proof. This again follows from two applications of Gauss's Lemma and the fact that $aX+b-A(Y)/B(Y)$ is irreducible in $k(Y)[X]$. □

LEMMA 3.3. *Let k be a differential field with algebraically closed field of constants C. For any $S(Y)$ in $C(Y)$, any u, v in k such that $v'=(S(u))'/S(u)$ and for any a, $b \in C$, there exist $w_0, \cdots, w_n$ in k, $c_1, \cdots, c_n$ in C such that $u'(av+b)=w_0'+\sum c_i w_i' w_i$.*

Proof. It is enough to show that $u'(av+b)$ has an antiderivative in some elementary extension of k and then apply Liouville's Theorem. If we write $S(Y)=\beta \prod (Y-\alpha_i)^{n_i}$ where the α_i are in C and n_i are integers, then we can write $v'=\sum n_i(u-\alpha_i)'/(u-\alpha_i)$. Thus $v=\sum n_i v_i$ for v_i in some elementary extension of K such that $v_i'=(u-\alpha_i)'/(u-\alpha_i)$. One can then check that $u'(av_i+b)=(a(u-\alpha_i)(v_i-1)+bu)'$. □

Proof of Theorem 1.1. First of all, we may assume that for all β in B, $S_\beta(Y)$ is not an mth power for any positive integer m. If some $S_\beta(Y)=(\bar{S}_\beta(Y))^m$ then in the definition of $\mathscr{L}$ and in condition (v) of (1.1) we could replace $S_\beta(Y)$ by $\bar{S}_\beta(Y)$ and $H_\beta(Y)$ by $\bar{H}_\beta(Y)=H_\beta(mY)$, so that $\bar{H}_\beta(\log \bar{S}_\beta(Y))=H_\beta(\log S_\beta(Y))$. In this way we get a new set $\bar{\mathscr{L}}$, prove our theorem for $\mathscr{E}\bar{\mathscr{L}}$-elementary extensions and then switch back.

Furthermore, assuming the hypothesis of the theorem, Corollary 2.2 states that we can assume that $y'=\gamma$ has a solution in an $\mathscr{E}\mathscr{L}$-elementary extension of F, with no new constants.

We first assume F is algebraically closed. In this case, we proceed by induction on the transcendence degree of E over F. When the transcendence degree is zero, the result is trivial. When it is positive we apply induction and the problem is reduced to showing:

Let E be an algebraic extension of $F(\theta)$ where θ is transcendental over F and satisfies conditions (ii), (iii), (iv) or (v) of (1.1). Let $\gamma \in F$ and assume that E has no new constants and that there exist w_i, $u_{i\alpha}$, $u_{i\beta}$, $v_{i\alpha}$, $v_{i\beta}$ in E and constants a_i, $b_{i\alpha}$, $c_{i\beta}$ such that

$$\gamma = w_0' + \sum a_i \frac{w_i'}{w_i} + \sum\sum b_{i\alpha} u_{i\alpha}' G_\alpha(v_{i\alpha}) + \sum\sum c_{i\beta} u_{i\beta}' H_\beta(v_{i\beta}), \tag{3.1}$$

where

$$v_{i\alpha}' = (R_\alpha(u_{i\alpha}))' v_{i\alpha} \quad \text{and} \quad v_{i\beta}' = \frac{(S_\beta(u_{i\beta}))'}{S_\beta(u_{i\beta})}.$$

Then there exist $\bar{w}_i$, $\bar{u}_{i\alpha}$, $\bar{u}_{i\beta}$, $\bar{v}_{i\alpha}$, $\bar{v}_{i\beta}$ in F and constants $\bar{a}_i$, $\bar{b}_{i\alpha}$, $\bar{c}_{i\alpha}$ in F such that

$$\gamma = \bar{w}_0' + \sum \bar{a}_i \frac{\bar{w}_i'}{\bar{w}_i} + \sum\sum \bar{b}_{i\alpha} \bar{u}_{i\alpha}' G_\alpha(\bar{v}_\alpha) + \sum\sum \bar{c}_{i\beta} \bar{u}_{i\beta}' H_\beta(\bar{v}_{i\beta}),$$

where

$$\bar{v}_{i\alpha}' = (R_\alpha(\bar{u}_{i\alpha}))' \bar{v}_{i\alpha} \quad \text{and} \quad \bar{v}_{i\beta}' = \frac{(S_\beta(\bar{u}_{i\beta}))'}{S_\beta(\bar{u}_{i\beta})}.$$

We shall deal with each of the cases (ii)-(v) separately. The main idea is to take the trace of both sides of (3.1) to force everything to belong to $F(\theta)$. We then will equate terms in the partial fraction decomposition with respect to θ and show that the term not depending on θ on the right-hand side can be put in the prescribed form.

Case (ii). $\theta' = u'\theta$ for some u in F.

For each α, β, i we have $v'_{i\alpha} = (R_\alpha(u_{i\alpha}))'v_{i\alpha}$, and $(S_\beta(u_{i\beta}))' = v'_{i\beta}S_\beta(u_{i\beta})$, then by [ROS76, Theorem 2] we have that

$$\begin{aligned} v_{i\alpha} &= f_{i\alpha}\theta^{r_{i\alpha}}, \\ S_\beta(u_{i\beta}) &= f_{i\beta}\theta^{r_{i\beta}}, \end{aligned} \tag{3.2}$$

for some rational numbers $r_{i\alpha}$, $r_{i\beta}$ and elements $f_{i\alpha}$, $f_{i\beta}$ of F. Furthermore we have

$$\begin{aligned} R_\alpha(u_{i\alpha}) &= r_{i\alpha}u + g_{i\alpha}, \\ v_{i\beta} &= r_{i\beta}u + g_{i\beta}, \end{aligned} \tag{3.3}$$

with $g_{i\alpha}$ and $g_{i\beta}$ in F. Note that we can arrange that $r_{i\alpha}$ and $r_{i\beta}$ are actually integers. To see this, let $r_{i\alpha} = s_{i\alpha}/n$ and $r_{i\beta} = s_{i\beta}/n$, where $s_{i\alpha}$, $s_{i\beta}$ and n are integers. Let $\bar{\theta} = \theta^{1/n}$. We then have $\bar{\theta}' = 1/n\, u'\bar{\theta}$ and $F \subset E \subset E(\bar{\theta})$. If we replace E by $E(\bar{\theta})$ and θ by $\bar{\theta}$, we still have fields of the appropriate form and furthermore, $v_{i\alpha} = f_{i\alpha}\bar{\theta}^{s_{i\alpha}}$, and $S_\beta(u_{i\beta}) = f_{i\beta}\bar{\theta}^{s_{i\beta}}$, where $s_{i\alpha}$ and $s_{i\beta}$ are integers. We shall use the old notation but from now on assume that $r_{i\alpha}$ and $r_{i\beta}$ are integers.

We want to take the trace of both sides of (3.1) over $F(\theta)$. Note that from (3.2) and (3.3), the $v_{i\alpha}$ and $S_\beta(u_{i\beta})$ are in $F(\theta)$ and the $R_\alpha(u_{i\alpha})$ and $v_{i\beta}$ are in F (which implies that $u_{i\alpha}$ is in F). The only elements which may give us trouble when we take the trace are the $u_{i\beta}$ which, a priori, are only algebraic over $F(\theta)$.

To calculate the trace of the $u_{i\beta}$, write

$$S_\beta(Y) = \frac{A_\beta(Y)}{B_\beta(Y)}$$

where A_β and B_β are relatively prime polynomials. Then $u_{i\beta}$ satisfies

$$A_\beta(Y) - f_{i\beta}\theta^{r_{i\beta}}B_\beta(Y) = 0$$

which, by Lemma 3.1, is irreducible over $F(\theta)$. Therefore the trace of $u_{i\beta}$ can be calculated from the coefficients of this polynomial. The coefficients are all of the form $\delta(f_{i\beta}\theta^{r_{i\beta}}) + \varepsilon$ where δ and ε are constants. Dividing by the leading coefficient, we get

$$\operatorname{Tr} u_{i\beta} = m\left(\frac{\delta(f_{i\beta}\theta^{r_{i\beta}}) + \varepsilon}{\mu(f_{i\beta}\theta^{r_{i\beta}}) + \nu}\right)$$

where m is an integer and δ, ε, μ, ν are constants. We then have

$$(\operatorname{Tr} u_{i\beta})' = m\frac{(\delta\nu - \varepsilon\mu)(f'_{i\beta} + f_{i\beta}r_{i\beta}u')\theta^{r_{i\beta}}}{(\mu(f_{i\beta}\theta^{r_{i\beta}}) + \nu)^2}.$$

Note that the coefficient of θ^0 in the partial fraction decomposition of this expression is 0, *assuming that* $r_{i\beta} \neq 0$.

We are now ready to take traces in equation (3.1). Doing this we get

$$M\gamma = (\operatorname{Tr} w_0)' + \sum a_i \frac{(Nw_i)'}{Nw_i} + \sum\sum b_{i\alpha}u'_{i\alpha}G_\alpha(v_{i\alpha}) + \sum\sum c_{i\beta}(\operatorname{Tr} u_{i\beta})'H_\beta(v_{i\beta}) \tag{3.4}$$

where M is some integer and, abusing notation, the a_i, $b_{i\alpha}$, $c_{i\beta}$ are possibly different constants. Let us collect the coefficient of θ^0 on the right-hand side of this equation. If we write $\operatorname{Tr} w_0 = \sum\sum(a_{ij}/(\theta - \mu_i)^j) + P(\theta)$, the standard calculations (as in [RISC69, p. 169]) show that the coefficient of θ^0 in $(\operatorname{Tr} w_0)'$ is

$$\tilde{w}'_0 \tag{3.5}$$

where $\tilde{w}_0$ is the coefficient of θ^0 in $P(\theta)$. Considering the next expression in (3.4), we write

$$\sum_i a_i \frac{(Nw_i)'}{Nw_i} = \sum_i \sum_j a_i \left(\frac{l_i'}{l_i} + n_{ij} \frac{(\theta + \mu_j)'}{(\theta - \mu_j)} \right)$$

where $Nw_i = l_i \Pi(\theta - \mu_j)^{n_{ij}}$ for some l_i, μ_j in F and integers n_{ij}. The coefficient of θ^0 here is

$$\sum a_i \frac{l_i'}{l_i} + \sum_i \sum_j a_i n_{ij} u'. \tag{3.6}$$

Next we consider the expression

$$\begin{aligned} \sum\sum b_{i\alpha} u_{i\alpha}' G_\alpha(v_{i\alpha}) &= \sum\sum b_{i\alpha} u_{i\alpha}' G_\alpha(f_{i\alpha}\theta^{r_{i\alpha}}) \\ &= \sum_{r_{i\alpha} \neq 0}\sum b_{i\alpha} u_{i\alpha}' G_\alpha(f_{i\alpha}\theta^{r_{i\alpha}}) + \sum_{r_{i\alpha}=0}\sum b_{i\alpha} u_{i\alpha}' G_\alpha(f_{i\alpha}). \end{aligned}$$

The coefficient of θ^0 in the expression corresponding to the sum over those i, α with $r_{i\alpha} \neq 0$ is $\sum\sum b_{i\alpha} d_{\alpha 0}\, u_{i\alpha}'$ where $d_{\alpha 0}$ is the coefficient of Y^0 in $G_\alpha(Y)$, which is a constant. The expression corresponding to the sum over i, α with $r_{i\alpha} = 0$ has no occurrence of θ, so the coefficient of θ^0 in $\sum\sum b_{i\alpha} u_{i\alpha}' G_\alpha(v_{i\alpha})$ is of the form

$$v' + \sum\sum b_{i\alpha} u_{i\alpha}' G_\alpha(v_{i\alpha}) \tag{3.7}$$

where v, $u_{i\alpha}$, $v_{i\alpha}$ are in F and $v_{i\alpha}' = (R_\alpha(u_{i\alpha}))' v_{i\alpha}$. Finally, we consider the expression

$$\begin{aligned} &\sum\sum c_{i\beta}(\operatorname{Tr} u_{i\beta})' H_\beta(v_{i\beta}) \\ &= \sum_{r_i\beta \neq 0}\sum c_{i\beta}(\operatorname{Tr} u_{i\beta})' H_\beta(v_{i\beta}) + \sum_{r_{i\beta}=0}\sum c_{i\beta}(\operatorname{Tr} u_{i\beta})' H_\beta(v_{i\beta}) \end{aligned} \tag{3.8}$$

where $r_{i\beta}$ is defined in (3.2). Note that by (3.3) $H_\beta(v_{i\beta})$ is in F and that if $r_{i\beta} = 0$ then $u_{i\beta}$ is in F so that $\operatorname{Tr} u_{i\beta}$ is in F. Therefore the sum corresponding to $r_{i\beta} = 0$ has no occurrence of θ. If $r_{i\beta} \neq 0$, we showed that the coefficient of θ^0 in $(\operatorname{Tr} u_{i\beta})'$ is zero, so the coefficient of θ^0 in the term corresponding to $r_{i\beta} \neq 0$ is 0. Therefore the coefficient of θ^0 in $\sum\sum c_{i\beta}(\operatorname{Tr} u_{i\beta})' H_\beta(v_{i\beta})$ is

$$\sum_{r_{i\beta}=0}\sum c_{i\beta}(\operatorname{Tr} u_{i\beta})' H_\beta(v_{i\beta})$$

where $v_{i\beta}' = (S_\beta(u_{i\beta}))'/S_\beta(u_{i\beta})$ and $u_{i\beta}$, $v_{i\beta} \in F$. Combining (3.5), (3.6), (3.7) and (3.8), we see that the coefficient of θ^0 on the right-hand side of (3.4) is of the prescribed form and, since, for $i \neq 0$, θ^i does not occur on the left hand side, we have that $M\gamma$ equals this prescribed form.

Case (iii). $\theta' = u'/u$ for some $u \in F$. Again [ROS76, Thm. 2] implies that

$$R_\alpha(u_{i\alpha}) = d_{i\alpha}\theta + g_{i\alpha}, \qquad v_{i\beta} = d_{i\beta}\theta + g_{i\beta}, \tag{3.9}$$

for some constants $d_{i\alpha}$, $d_{i\beta}$ and elements $g_{i\alpha}$, $g_{i\beta}$ in F and that the $v_{i\alpha}$ and the $S_\beta(u_{i\beta})$ are in F. So in particular, we have that the $v_{i\alpha}$, $v_{i\beta}$, and the $u_{i\beta}$ are in $F(\theta)$. We only know that the $u_{i\alpha}$ are algebraic over $F(\theta)$ and so must calculate their trace.

Let

$$R_\alpha(Y) = \frac{A_\alpha(Y)}{B_\alpha(Y)}$$

where A and B are relatively prime polynomials with constant coefficients. Each $u_{i\alpha}$ satisfies $A_\alpha(u_{i\alpha}) - (d_{i\alpha}\theta + g_{i\alpha})B_\alpha(u_{i\alpha}) = 0$. By Lemma 3.2, the polynomial $A_\alpha(Y) - (d_{i\alpha}\theta + g_{i\alpha})B_\alpha(Y)$ is irreducible over $F(\theta)$ so the trace can be read off from its coefficients. As before, we see that

$$\operatorname{Tr} u_{i\alpha} = m\left(\frac{\delta(d_{i\alpha}\theta + g_{i\alpha}) + \varepsilon}{\mu(d_{i\alpha}\theta + g_{i\alpha}) + \nu}\right)$$

where δ, ε, μ, ν are constants. Therefore

$$(\operatorname{Tr} u_{i\alpha})' = \frac{\text{element of } F}{(\mu(d_{i\alpha}\theta + g_{i\alpha}) + \nu)^2}.$$

Note that if $\mu d_{i\alpha} \neq 0$, then the coefficient of θ^0 in this expression is 0. If $\mu = 0$ and $d_{i\alpha} \neq 0$, then

$$(\operatorname{Tr} u_{i\alpha})' = \frac{m}{\nu}\left(\delta\left(d_{i\alpha}\frac{u'}{u} + g'_{i\alpha}\right)\right) = \frac{\delta}{\nu} mR_\alpha(u_{i\alpha})'$$

Now let us take the trace of both sides of (3.1):

$$M\gamma = (\operatorname{Tr} w_0)' + \sum a_i \frac{(Nw_i)'}{Nw_i} + \sum\sum b_{i\alpha}(\operatorname{Tr} u_{i\alpha})' G_\alpha(v_{i\alpha}) + \sum\sum c_{i\beta} u'_{i\beta} H_\beta(v_{i\beta})$$

and let us consider each of the terms on the right separately.

Recalling from (3.9), that each $v_{i\beta} = d_{i\beta}\theta + g_{i\beta}$ we can write the last sum as

$$\sum\sum c_{i\beta}u'_{i\beta}H_\beta(v_{i\beta}) = \sum_{d_{i\beta}=0}\sum c_{i\beta}u'_{i\beta}H_\beta(v_{i\beta}) + \sum_{d_{i\beta}\neq 0}\sum c_{i\beta}u'_{i\beta}H_\beta(v_{i\beta}) \tag{3.10}$$

The sum corresponding to $d_{i\beta} = 0$ has $u_{i\beta}$ and $v_{i\beta}$ in F and is of the desired form. To deal with the sum corresponding to $d_{i\beta} \neq 0$, recall that we have assumed that deg (numerator H_β) $\leqq$ deg (denominator H_β) + 1 so the partial fraction decomposition of H_β is

$$\sum\sum \frac{a_{ij}}{(Y - \alpha_i)^j} + P_\beta(Y)$$

where P_β is a polynomial of degree $\leqq 1$. We can therefore write

$$\sum_{d_{i\beta}\neq 0}\sum c_{i\beta}u'_{i\beta}H_\beta(v_{i\beta}) = \sum\sum c_{i\beta}u'_{i\beta}(H_\beta(v_{i\beta}) - P_\beta(v_{i\beta})) + \sum\sum c_{i\beta}u'_{i\beta}P_\beta(v_{i\beta}).$$

The first term is a proper rational function of θ (i.e. the degree of the numerator is less than the degree of the denominator). By Lemma 3.3, the second term is of the form $v' + \sum d_i v'_i/v_i$. Therefore we can write (3.10) as

$$\begin{aligned} &\sum\sum c_{i\beta}u'_{i\beta}H_\beta(v_{i\beta}) \\ &\quad = \text{an expression whose } \theta^0 \text{ term is } \sum_{d_{i\beta}=0}\sum c_{i\beta}u'_{i\beta}H_\beta(v_{i\beta}), \\ &\qquad \text{with no terms containing } \theta^i \text{ for } i > 0 \\ &\quad + \text{an expression of the form } v'_0 + \sum d_i \frac{v'_i}{v_i} \end{aligned} \tag{3.11}$$

where $u_{i\beta}$ and $v_{i\beta}$ are in F, v_i are in $F(\theta)$ and the d_i and $c_{i\beta}$ are constants. We shall deal with the θ^0 term of $v' + \sum d_i v'_i/v_i$ later.

We now look at the next term which we write as

$$\sum\sum b_{i\alpha}(\operatorname{Tr} u_{i\alpha})' G_\alpha(v_{i\alpha}) = m_d \sum_{d_{i\alpha}=0}\sum b_{i\alpha}u'_{i\alpha}G_\alpha(v_{i\alpha}) + \sum_{d_{i\alpha}\neq 0}\sum b_{i\alpha}(\operatorname{Tr} u_{i\alpha})' G_\alpha(v_{i\alpha}).$$

Note that if $d_{i\alpha} = 0$, then $u_{i\alpha}$ and $v_{i\alpha}$ are in F so $\operatorname{Tr} u_{i\alpha}$ is an integer multiple of $u_{i\alpha}$.

This integer is designated by m. If $d_{i\alpha} \neq 0$ we have shown that the θ^0 term of $(\operatorname{Tr} u_{i\alpha})'$ is zero or a constant times $R(u_{i\alpha})'$. Therefore the θ^0 term of the sum corresponding to $d_{i\alpha} \neq 0$ is of the form

$$\sum_{d_{i\alpha}\neq 0}\sum e_{i\alpha}R(u_{i\alpha})'G_\alpha(v_{i\alpha}) = \sum_{d_{i\alpha}\neq 0}\sum e_{i\alpha}\frac{v'_{i\alpha}}{v_{i\alpha}}G_\alpha(v_{i\alpha}) = v'_0 + \sum d_i\frac{v'_i}{v_i}$$

where $e_{i\alpha}$ and d_i are constants and the v_i are in $F(\theta)$. This last equality follows from the fact that $G_\alpha(v_{i\alpha})/v_{i\alpha}$ is a rational function of $v_{i\alpha}$ with constant coefficients. Therefore, we have

$$\begin{aligned}
&\sum\sum b_{i\alpha}(\operatorname{Tr} u_{i\alpha})'G_\alpha(v_{i\alpha})\\
&\qquad = \text{an expression whose } \theta^0 \text{ term is } \sum_{d_{i\alpha}=0}\sum b_{i\alpha}u'_{i\alpha}G_\alpha(v_{i\alpha}),\\
&\qquad\qquad \text{with no terms containing } \theta^i \text{ for } i>0\\
&\qquad + \text{an expression of the form } v'_0+\sum d_i\frac{v'_i}{v_i}
\end{aligned} \tag{3.12}$$

where $u_{i\alpha}$ and $v_{i\alpha}$ are in F, v_i are in $F(\theta)$ and the $b_{i\alpha}$ and d_i are constants.

From (3.11) and (3.12) we can conclude that

$$\begin{aligned}
\gamma = v'_0+\sum d_i\frac{v'_i}{v_i} &+ \text{an expression whose } \theta^0 \text{ term is a constant multiple of}\\
&\sum_{d_{i\alpha}=0}\sum b_{i\alpha}u'_{i\alpha}G_\alpha(v_{i\alpha}) + \sum_{d_{i\beta}=0}\sum c_{i\beta}u'_{i\beta}H_\beta(v_{i\beta}) \text{ and with no terms}\\
&\text{containing } \theta^i \text{ for } i>0
\end{aligned} \tag{3.13}$$

where $u_{i\alpha}$, $u_{i\beta}$, $v_{i\alpha}$, $v_{i\beta}$ are in F, v_i are in $F(\theta)$ and $b_{i\alpha}$, $c_{i\alpha}$, d_i are constants. We now want to calculate the θ^0 term of $v'_0+\sum d_i v'_i/v_i$. If we write $v_i = \xi_i \prod_j (\theta-\mu_j)^{n_{ij}}$, $i\neq 0$, where ξ_i, u_j are in F, then the θ^0 term of v'_i/v_i is ξ'_i/ξ_i. Letting $v_0 = \sum_{j=0}^{l} k_i\theta^i$ + terms of degree <0 in θ, we have that the θ^0 term of v'_0 is k'_0+k_1u'/u. If $l>1$ or k_1 is not a constant, we would have that the right-hand side of (3.13) would contain an expression of the form θ^i with $i \geqq 1$. Therefore we have that $l=1$, k_1 is a constant and the θ^0 term of $v'_0+\sum d_iv'_i/v_i$ is of the form $u_0+\sum a_i u'_i/u_i$ with the $u_i \in F$ and a_i constants. This and (3.13) shows that γ has the correct form.

Case (iv) *and* (v). $\theta' = u'G_\alpha(v)$ or $\theta' = u'H_\beta(v)$ where $v' = (R_\alpha(u))'v$ or $v' = (S_\beta(v))'/S_\beta(v)$ with $u, v \in F$.

In this case we can assume that θ is not elementary over F, otherwise the problem could be reduced to the above considerations. Since $\theta' \in F$, we have that the $S(u_{i\beta})$ and $v_{i\alpha}$ are in F and that $R(u_{i\alpha}) = d_{i\alpha}\theta + g_{i\alpha}$ and $v_{i\beta} = d_{i\beta}\theta + g_{i\beta}$ with the $d_{i\alpha}$, $d_{i\beta}$ constants and $g_{i\alpha}$, $g_{i\beta}$ in F. We must have $d_{i\alpha} = d_{i\beta} = 0$, otherwise θ would be elementary over F. Therefore, we can write (3.1) as

$$\gamma - \sum\sum b_{i\alpha}u'_{i\alpha}G_\alpha(v_{i\alpha}) - \sum\sum c_{i\beta}u'_{i\beta}H_\beta(v_{i\beta}) = u'_0 + \sum a_i\frac{u'_i}{u_i} \tag{3.14}$$

with all terms on the left in F. Liouville's Theorem now applies and tells us that the expression on the right must equal $\tilde{u}'_0+\sum \tilde{a}_i\tilde{u}'_i/\tilde{u}_i$ for some $\tilde{u}_i \in F$ and constants $\tilde{a}_i$. This completes the proof of Theorem 1.1 in the case that F is algebraically closed.

Now we remove the assumption that F is algebraically closed. The above argument shows that (1.2) holds with a_i, $b_{i\alpha}$, $c_{i\beta}$ in C and w_i, $u_{i\alpha}$, $u_{i\beta}$, $v_{i\alpha}$, $v_{i\beta}$ algebraic over F. Let K be a finite normal extension of F containing w_i, $u_{i\alpha}$, $u_{i\beta}$, $v_{i\alpha}$, $v_{i\beta}$ and let σ be an element of the Galois group of K over F. Then

$$\sigma(\gamma)=\gamma=(\sigma w_0)'+\sum a_i\frac{(\sigma w_i)'}{\sigma w_i}+\sum\sum b_{i\alpha}\sigma(u_{i\alpha})'G_\alpha(\sigma v_{i\alpha})+\sum\sum c_{i\beta}\sigma(u_{i\beta})'H_\beta(\sigma v_{i\beta})$$

where $(\sigma v_{i\alpha})'=(R_\alpha(\sigma u_{i\alpha}))'\sigma v_{i\alpha}$ and $(\sigma v_{i\beta})'=(S_\beta(\sigma u_{i\beta}))'/S_\beta(\sigma u_{i\beta})$, $S_\beta(\sigma u_{i\beta})\neq 0$.

Summing over all σ in the Galois group of K over F yields, for some M in $\mathbf{Z}$,

$$M\gamma=(\mathrm{Tr}\, w_0)'+\sum a_i\frac{(Nw_i)'}{Nw_i}+\sum_\sigma\sum\sum b_{i\alpha}\sigma(u_{i\alpha})'G_\alpha(\sigma v_{i\alpha})$$
$$+\sum_\sigma\sum\sum c_{i\beta}\sigma(u_{i\beta})'H_\beta(\sigma v_{i\beta}).$$

Since $\mathrm{Tr}\, w_0$ and the norms Nw_i, are in F, this yields the final conclusion of the theorem. □

II. The error function.

4. Statement and discussion of results. In this section we shall specialize the results of the previous sections to the case when $\mathscr{E}=\{\exp(-Y^2)\}$ and $\mathscr{L}=\varnothing$, that is, to integration in terms of error functions and elementary functions. To be more explicit, we say that a differential field E is an *erf-elementary extension of* F if there exists a tower of fields $F=F_0\subset\cdots\subset F_n=E$ such that $F_i=F_{i-1}(\theta_i)$ where for each i, $1\leqq i\leqq n$, one of the following holds:

(i) θ_i is algebraic over F_{i-1};

(ii) $\theta_i'=u_i'\theta_i$ for some u_i in F_{i-1};

(iii) $\theta_i'=u_i'/u_i$ for some $u_i\neq 0$ in F_{i-1};

(iv) $\theta_i'=u_i'v_i$ for some u_i, v_i in F_{i-1} with $v_i'=(-u_i^2)'v_i=-2u_iu_i'v_i$.

Recall that a differential field F is a Liouvillian extension of a differential field k if there exists a tower $k=k_0\subset\cdots\subset k_m=F$ such that $k_i=k_{i-1}(\xi_i)$ where for each i, $1\leqq i\leqq n$, we have either:

(i) ξ_i is algebraic over k_{i-1}, or

(ii) $\xi_i'\in k_{i-1}$, or

(iii) $\xi_i'/\xi_i\in k_{i-1}$.

We then have the following result.

THEOREM 4.1. *Let F be a Liouvillian extension of its field of constants C. Assume C is of characteristic zero and algebraically closed and let γ be an element of F. If γ has an antiderivative in some erf-elementary extension of F, then there exist constants a_i and b_i in C, elements w_i in F, and elements u_i and v_i algebraic over F such that*

$$\gamma=w_0'+\sum a_i\frac{w_i'}{w_i}+\sum b_iu_i'v_i \tag{4.1}$$

where $v_i'=(-u_i^2)'v_i$ and u_i^2, v_i^2 and $u_i'v_i$ are in F.

Proof. By Theorem 1.1, we know that there exist constants a_i and b_i in C and elements w_i in F, u_i and v_i algebraic over F satisfying (4.1). We want to show that these can be chosen such that u_i^2, v_i^2 and $u_i'v_i$ are in F. The lemma of [ROSI77, p. 338] implies that each u_i^2 is in F and some power of v_i is in F. Let E be a normal extension of F containing all the w_i, u_i and v_i and let σ be an automorphism of E over F. We then have $\sigma u_i=\pm u_i$ and $\sigma v_i=\zeta_{\sigma i}v_i$ where $\zeta_{\sigma i}$ is a root of unity. Therefore,

$$\gamma=\sigma\gamma=(\sigma w_0)'+\sum_i a_i\frac{(\sigma w_i)'}{\sigma w_i}+\sum_i b_i(\pm\xi_{\sigma i})u_i'v_i.$$

If we sum over all automorphisms of E over F we get:

$$m\gamma = mw_0' + m\sum_i a_i\frac{w_i'}{w_i} + \sum_i b_i\left(\sum_\sigma \pm\zeta_{\sigma i}\right)u_i'v_i$$

for some integer m. In the expression $\sum_i b_i(\sum_\sigma \pm\zeta_{\sigma i})u_i'v_i$ we shall implicitly assume that we are only summing over those i for which $\sum_\sigma \pm\zeta_{\sigma i} \neq 0$. For such an i, we have

$$u_i'v_i = \left(\sum_\sigma \pm\zeta_{\sigma i}\right)^{-1}\sum_\sigma \sigma(u_i'vi)$$

so $u_i'v_i$ is left fixed by all automorphisms of E over F and so must lie in F. Furthermore, $(u_i')^2 = \frac{1}{4}((u_i^2)')^2/u_i^2$, so $(u_i')^2 \in F$. Since $v_i^2 = (u_i'v_i)^2/(u_i')^2$ we have $v_i^2 \in F$. □

The example at the end of § 1 shows that the u_i and v_i cannot be guaranteed to lie in F. Despite this fact we are able to obtain a decision procedure (presented in § 7) when γ is built up using only exponential functions and rational operations.

Let F and k be differential fields of characteristic zero. We say that F is a *purely exponential extension of* k if $F = k(\theta_1, \cdots, \theta_n)$ where θ_i is transcendental over $k(\theta_1, \cdots, \theta_{i-1})$ and $\theta_i' = u_i'\theta_i$ for some u_i in $k(\theta_1, \cdots, \theta_{i-1})$. The main result of § 7 is the following. Here, we use the term computable field to mean a field in which one can effectively carry out the field theoretic operations and over which one can effectively factor polynomials. Any finitely generated extension of $\mathbf{Q}$ is computable as is the algebraic closure of $\mathbf{Q}$.

THEOREM 4.2. *Let C be a computable field, $C(x)$ a differential field with derivation $'$ defined by $x' = 1$ and $c' = 0$ for all c in C, and let F be a purely exponential extension of $C(x)$. Given γ in F, one can decide in a finite number of steps if γ has an antiderivative in an erf-elementary extension of F and if so find a_i, b_i, u_i, v_i, and w_i satisfying* (4.1).

The rest of this paper is devoted to proving this result.

5. Purely exponential extensions. In practice, when we are asked to integrate a function γ, we are not given a differential field F containing γ. In this section we shall show how to make a good choice for a field of definition containing γ. This field will be chosen so that the exponentials appearing in this field satisfy as few relations as possible and so that the u_i and v_i which could possibly appear in (4.1) are already in F. To do this we need some facts about purely exponential extensions.

Let F be a purely exponential extention of k. When we refer to such a field, we shall always consider it as being given by a *fixed* set of generators $\theta_1, \cdots, \theta_n$ over k, so $F = k(\theta_1, \cdots, \theta_n)$. Renumbering the θ_i, we may write $k = F_0 \subset \cdots \subset F_r = F$ where $F_i = F_{i-1}(\theta_{i1}, \cdots, \theta_{im_i})$ for $i = 1, \cdots, r$ and where the θ_{ij}'s are algebraically independent over k and satisfy $\theta_{ij}' = u_{ij}'\theta_{ij}$ for some u_{ij} in F_{i-1} with u_{ij} not in F_{i-2}. Note that, one can always *uniquely* arrange the θ_i's in groups to satisfy the above. We define the *rank of* $F = k(\theta_1, \cdots, \theta_n)$ *over* k to be the r-tuple $(m_r, \cdots, m_1)$ and we designate this by $\operatorname{rank}_k F$.

Let us consider two examples.

Example 5.1. Let $k = \mathbf{C}(x)$, $F = k(\exp x^2, \exp(\exp x^2), \exp(\exp(x^2)+x))$. $k = \mathbf{C}(x) = F_0 \subset F_1 = F_0(\exp(x^2)) \subset F_2 = F_1(\exp(\exp x^2), \exp(\exp(x^2)+x))$. We have $\operatorname{rank}_k F = (2, 1)$.

Example 5.2. Let k be as above and $\bar{F} = k(\exp x^2, \exp x, \exp(\exp x^2))$. We can write $k = \bar{F}_0 \subset \bar{F}_1 = \bar{F}_0(\exp x^2, \exp x) \subset \bar{F}_2 = \bar{F}_1(\exp(\exp x^2)) = \bar{F}$. We have $\operatorname{rank}_k \bar{F} = (1, 2)$.

Note that $F \cong \bar{F}$; only the generating sets are different. This underlines the important fact that the rank depends on the particular $\theta_1, \cdots, \theta_n$ we chose to generate

F over k. Note that if $\operatorname{rank}_k F = (m_r, \cdots, m_1)$ then $m_1 + \cdots + m_r$ is the transcendence degree of F over k.

We can also define the tank of an exponential in F. Let F be a purely exponential extension of k and let $F_0, \cdots, F_r$ be as above. Let u, v be elements of F such that $v' = u'v$. We define the *rank of* v ($\operatorname{rank}_k v$) to be the smallest i such that $v \in F_i$. Note that if $\operatorname{rank}_k v = i$, then $u \in F_{i-1}$. Also note that in Example 5.1, $\operatorname{rank}_k \exp(x) = 2$ while in Example 5.2 $\operatorname{rank}_k \exp(x) = 1$.

Given two sequences $(m_r, \cdots, m_1)$ and $(\bar{m}_s, \cdots, \bar{m}_1)$ we say $(m_r, \cdots, m_1) < (\bar{m}_s, \cdots, \bar{m}_1)$ if $r < s$ or if $r = s$ and $(m_r, \cdots, m_1)$ is less than $(\bar{m}_s, \cdots, \bar{m}_1)$ in the usual lexicographical ordering. We say that a purely exponential extension F of k is of *minimal rank over* k if for any algebraic extension $\bar{F}$ of F, where $\bar{F}$ is also a purely exponential extension of k, we have $\operatorname{rank}_k F \leqq \operatorname{rank}_k \bar{F}$. For example $C(x, \exp(x^2), \exp(\exp x^2), \exp(\exp x^2 + x))$ is not of minimal rank over $C(x)$, since it is contained in (in fact equal to) $C(x, \exp(x^2), \exp(x), \exp(\exp x^2))$ which is of smaller rank. We will show later that $C(x, \exp(x^2), \exp(x), \exp(\exp x^2))$ is of minimal rank over $C(x)$.

We will need the following technical lemma in Proposition 5.2.

LEMMA 5.1. *Let $E = F(\theta_1, \cdots, \theta_m)$ where $\theta_i' = u_i'\theta_i$ with u_i in $F(\theta_1, \cdots, \theta_{i-1})$. Assume that E and F have the same field of constants and that $\theta_1, \cdots, \theta_m$ are algebraically independent over F. If ζ is an element of E such that ζ' is in F, then ζ is in F.*

Proof. Proceeding by induction on m, we an assume that $m = 1$. In this case write $E = F(\theta)$ where $\theta'/\theta \in F$. Since θ and ζ are algebraically dependent over F, we have, by [ROS76, Thm. 2], that ζ is algebraic over F. Since $F(\theta)$ is a transcendental extension of F, we must have $\zeta \in F$. □

PROPOSITION 5.2. *Let F be a purely exponential extension of $k = C(x)$, where $x' = 1$ and $c' = 0$ for all c in C, and let $k = F_0 \subset \cdots \subset F_r = F$ where $F_i = F_{i-1}(\theta_{i1}, \cdots, \theta_{im_i})$ with $\theta_{ij}' = u_{ij}'\theta_{ij}$ for some $u_{ij} \in F_{i-1}$, $u_{ij} \notin F_{i-2}$. Then F is of minimal rank over k if and only if, for each $i = 2, \cdots, r$ the following holds*:

$$(5.1) \qquad \sum_{j=1}^{m_i} n_j u_{ij} \in F_{i-2} \text{ for some integers } n_j \text{ implies } n_j = 0 \text{ for all } n_j.$$

Proof. Assume that F is of minimal rank over k and that for some i, there exist $n_1, \cdots, n_{m_i}$, not all zero, such that $\sum_{j=1}^{m_i} n_j u_{ij} \in F_{i-2}$. Without loss of generality, we can assume $n_1 \neq 0$. Let

$$\theta = \prod_{j=1}^{m_i} \theta_{ij}^{n_j/n_1} \quad \text{and} \quad v = \sum_{j=1}^{m_i} \frac{n_j}{n_1} u_{ij}.$$

We then have $\theta' = v'\theta$. Let

$$\begin{aligned}
\bar{F}_0 &= F_0,\\
\bar{F}_1 &= F_1,\\
&\vdots\\
\bar{F}_{i-2} &= F_{i-2},\\
\bar{F}_{i-1} &= F_{i-1}(\theta),\\
\bar{F}_i &= \bar{F}_{i-1}(\theta_{i2}^{1/n_1}, \cdots, \theta_{im_i}^{1/n_1}),\\
\bar{F}_{i+1} &= \bar{F}_i \cdot F_{i+1},\\
&\vdots\\
\bar{F}_r &= \bar{F}_{r-1} \cdot F_r,
\end{aligned}$$

where $\bar{F}_k \cdot F_{k+1}$ is the compositum of these two fields. Note that $\bar{F}_r$ is an algebraic extension of F_r. The rank of $\bar{F}_r$ is $(m_r, \cdots, m_{i+1}, m_i - 1, m_{i-1}+1, \cdots, m_1)$ which is smaller than $\operatorname{rank}_k F_r = (m_r, \cdots, m_i, m_{i-1}, \cdots, m_1)$. This contradicts the fact that $F_r = F$ is of minimal rank over k and so (5.1) must hold.

Now assume that (5.1) holds. We wish to show that F is of minimal rank over k. Let $\bar{F}$ be a purely exponential extension, algebraic over F, such that $\operatorname{rank}_k \bar{F} = (\bar{m}_s, \cdots, \bar{m}_1) \leqq (m_r, \cdots, m_1) = \operatorname{rank}_k F$. Let $k = \bar{F}_0 \subset \bar{F}_1 \subset \cdots \subset \bar{F}_s = \bar{F}$ where $\bar{F}_i = \bar{F}_{i-1}(\bar{\theta}_{i1}, \cdots, \bar{\theta}_{i\bar{m}_i})$ where $\bar{\theta}'_{ij} = \bar{u}_{ij}\bar{\theta}_{ij}$ for some $\bar{u}_{ij} \in \bar{F}_{i-1}$ and $\bar{u}_{ij} \notin \bar{F}_{i-2}$. We will show that for each i, $\bar{F}_i$ is algebraic over F_i and therefore that $\bar{m}_i \leqq m_i$ for each i and $s \leqq r$. Since $\operatorname{tr.deg}_k F = \operatorname{tr.deg}_k \bar{F}$, we have $\sum_{i=1}^r m_i = \sum_{i=1}^s \bar{m}_i$ and so $m_i = \bar{m}_i$ for each i. Therefore $\operatorname{rank}_k F = \operatorname{rank}_k \bar{F}$.

To prove that $\bar{F}_i$ is algebraic over F_i, we proceed by induction on i. If $i = 0$, $F_i = k = \bar{F}_i$, so we are done. Now assume that $\bar{F}_j$ is algebraic over F_j for $j < i$. Since $\bar{F}$ is algebraic over F, we have that $\bar{\theta}_{i1}, \cdots, \bar{\theta}_{i\bar{m}_i}$ are algebraic over F. By the lemma of [ROSI77, p. 338], we have that $\bar{\theta}_{ij}^N \in F$ for some nonzero integer N. Furthermore,

$$\frac{(\bar{\theta}_{ij}^N)'}{\bar{\theta}_{ij}^N} = N\bar{u}'_{ij} \in \bar{F}_{i-1} \cap F = F_{i-1}$$

since by induction $\bar{F}_{i-1}$ is algebraic over F_{i-1} and F_{i-1} is relatively algebraically closed in F. If we write $F = C(x)(\theta_{11}, \cdots, \theta_{1m_1}, \cdots, \theta_{r1}, \cdots, \theta_{rm})$ where $\theta'_{ij} = u'_{ij}\theta_{ij}$ then by [ROCA79, Thm. 3.1] we have that

$$\bar{u}_{ij} = \sum_{\substack{1 \leqq b \leqq m_a \\ 1 \leqq a \leqq r}} r_{ab}^{ij} u_{ab} + c$$

for some rational numbers r_{ab}^{ij} and constant c. Since $\bar{u}'_{ij} \in F_{i-1}$, we have by Lemma 5.1 that $\bar{u}_{ij} = \sum r_{ab}^{ij} u_{ab} + c \in F_{i-1}$. If some $r_{ab}^{ij} \neq 0$ *with* $a > i$, we would contradict (5.1). Therefore $r_{ab}^{ij} = 0$ if $a > i$ and

$$\bar{\theta}_{ij} = d \prod_{a=1}^{i} \prod_{b=1}^{m_a} \theta_{ab}^{r_{ab}^{ij}}.$$

This implies that $\bar{\theta}_{ij}$ is algebraic over F_i and so $\bar{F}_i$ is algebraic over F_i. □

Using Proposition 5.2, we now can show that $\mathbf{C}(x, \exp x^2, \exp x, \exp(\exp x^2))$ is of minimal rank over $\mathbf{C}(x)$. Here $F_0 = \mathbf{C}(x) \subset F_1 = F_0(\exp x, \exp x^2) \subset F_2 = F_1(\exp(\exp x^2))$. We must check if $n_0 \exp x^2 \in F_0$ has a nonzero solution n_0 in the integers (which it clearly does not). Similarly we can reaffirm that $\mathbf{C}(x, \exp(x^2), \exp(\exp x^2), \exp(\exp x^2 + x))$ is not of minimal rank. Here $F_0 = \mathbf{C}(x) \subset F_1 = F_0(\exp x^2) \subset F_2 = F_1(\exp(\exp x^2), \exp(x + \exp x^2))$. Here $\theta_{11} = \exp x^2$, $u_{11} = x^2$, $\theta_{21} = \exp(\exp x^2)$, $u_{21} = \exp x^2$, $\theta_{22} = \exp(x + \exp x^2)$, $u_{22} = x + \exp x^2$. Note that $u_{21} - u_{22} = -x \in F_0$.

PROPOSITION 5.3. *Let C be a computable field and F a purely exponential extension of $C(x)$. We can construct an algebraic extension $\bar{F}$ of F such that $\bar{F}$ is a purely exponential extension of $C(x)$ and such that $\bar{F}$ is of minimal rank over $C(x)$.*

Proof. We will use the criterion (5.1) of proposition 5.2. Let $C(x) = F_0 \subset \cdots \subset F_r = F$ with $F_i = F_{i-1}(\theta_{i1}, \cdots, \theta_{im_i})$ as before. For each i, we check if there exist n_{ij}, not all zero such that $\sum_{j=1}^{m_i} n_{ij}u_{ij} \in F_{i-2}$. If, for some i, such a set of n_{ij} exists, say with $n_{il} \neq 0$, let

$$\theta = \prod_{j=1}^{m_i} \theta_{ij}^{n_{ij}/n_{i1}}.$$

Let

$$\bar{F}_j = F_j \text{ for } j < i-1,$$
$$\bar{F}_{i-1} = F_{i-1}(\theta),$$
$$\bar{F}_i = \bar{F}_{i-1}(\theta_{i2}^{1/n_{i1}}, \cdots, \theta_{im_i}^{1/n_{i1}}),$$
$$\bar{F}_j = F_j \cdot \bar{F}_i \quad \text{for } j > i.$$

We then have that $\bar{F}_r$ is a purely exponential extension of k, algebraic over F and of smaller rank than F over k. We claim that if we continue this process, it will end after at most N^2 steps where $N = \text{tr. deg}_k F$. This is because each time we repeat this process we decrease one of the integers in $(m_r, \cdots, m_1)$ by one and increase its neighbor to the right by one. This can be done at most $rm_r + (r-1)m_{r-1} + \cdots + m_1 \leqq rN \leqq N^2$. □

PROPOSITION 5.4. *Let C be an algebraically closed field and F a purely exponential extension of $C(x)$, where $x' = 1$ and $c' = 0$ for all c in C. One can construct a purely exponential extension F^* of $C(x)$, containing F, which has the following property*:

(5.2) *If u and v satisfy $v' = u'v$ and u and v are algebraic over F with v^2 in F, then u and v are in F^*.*

Proof. Let $F = C(x, \theta_1, \cdots, \theta_n)$ where $\theta_i' = u_i'\theta_i$ with u_i in $C(x, \theta_1, \cdots, \theta_{i-1})$ and let $F^* = C(x, \theta_1^{1/2}, \cdots, \theta_n^{1/2})$. One can easily show that F^* is a purely exponential extension of $C(x)$ containing F. Since u and v are algebraic over F, we have by [ROCA79, Thm. 3.1], that $v = d \prod_{i=1}^n \theta_i^{r_i}$ where d is in C and the r_i are in $\mathbf{Q}$. Since $v^2 = d^2 \prod_{i=1}^n \theta_i^{2r_i}$ is in F and F is a purely transcendental extension of C, we have that $2r_i$ is an integer, for each i. Therefore v is in F^* and so u is in F^*. □

6. Squares in purely transcendental extensions. In our decision procedure, we will be called upon to decide when certain elements of a field are squares. We discuss this algebraic question in this section. Let K be a field and $K(x_1, \cdots, x_n)$ a purely transcendental extension of K. Let P be an element of $K(x_1, \cdots, x_n)$ with P not in K and let $\tilde{K}$ be the algebraic closure of K. We wish to show that the set of α in $\tilde{K}$ such that $P + \alpha = Q^2$ for some Q in $\tilde{K}(x_1, \cdots, x_n)$ is finite (or empty) and computable if K is a computable field. We first prove the following ancillary lemma.

LEMMA 6.1. *Let f and g be elements of $K[x_1, \cdots, x_n]$ with no common factors and assume that either f or g is not in K. Then the set of α in $\tilde{K}$ such that $f^2 + \alpha g^2 = h^2$ for some h in $\tilde{K}[x_1, \cdots, x_n]$ is a finite set and can be constructed if K is a computable field.*

Proof. Let f and g be of degree $\leqq k$, let N be the dimension of the vector space of all such polynomials and let $\mathbf{P}^N$ be the projective space of dimension N over $\tilde{K}$. Let S be the subset of $\tilde{K} \times \mathbf{P}^N$ consisting of all $(\alpha, (c_1, \cdots, c_N, d))$ such that $d^2(f^2 + \alpha g^2) = h^2$ where h is a polynomial with coefficients $c_1, \cdots, c_N$. S is a Zariski-closed subset of $\tilde{K} \times \mathbf{P}^N$ and if we let $p: \tilde{K} \times \mathbf{P}^N \to \tilde{K}$ be the projection map, then $p(S)$ is the set mentioned in the lemma. By classical elimination theory ([MUM76, p. 33] or [VDW50, p. 6]), we know that $p(S)$ is a Zariski closed subset of $\tilde{K}$ and so is either finite or all of $\tilde{K}$. Furthermore, we know that if K is constructible, we can find the defining equations of $p(S)$. We need only check that $p(S) \neq \tilde{K}$.

Assume that $p(S) = \tilde{K}$ and that $\partial f/\partial x_1 \neq 0$ (since either f or g is not in K we may assume one of them, say f, depends on some x_i, say x_1). Let u be any element in K^n such that $g(u) \neq 0$ and let α_u be a nonzero element in K such that $f(u)^2 + \alpha_u g(u)^2 = 0$. Since we are assuming that $p(S) = \tilde{K}$, there is some polynomial h_u such that $f^2 + \alpha_u g^2 =$

h_u^2. Note that $h_u(u)=0$. Differentiating h_u^2, we get

$$\frac{\partial h_u^2}{\partial x_1^2}=2h_u\frac{\partial h_u}{\partial x_1}=2f\frac{\partial f}{\partial x_1}+2\alpha_u g\frac{\partial g}{\partial x_1}.$$

We therefore have the following identities

$$f(u)\cdot f(u)+\alpha_u g(u)\cdot g(u)=0,$$

$$f(u)\cdot\frac{\partial f}{\partial x_1}(u)+\alpha_u g(u)\cdot\frac{\partial g}{\partial x_1}(u)=0.$$

From this we can conclude that

$$f(u)\frac{\partial g}{\partial x_1}(u)-g(u)\frac{\partial f}{\partial x_1}(u)=0.$$

Since this holds for all u in the open set where $g(u)\neq 0$, we have that

$$f\frac{\partial g}{\partial x_1}-g\frac{\partial f}{\partial x_1}=0.$$

Since f and g have no common factors, we have that f divides $\partial f/\partial x_1$, a contradiction. Therefore $p(S)\neq\tilde{K}$ and so must be finite. □

PROPOSITION 6.2. *Let $P\in K(x_1,\cdots,x_n)$ with $P\notin K$. Then there exist only a finite number of values α in $\tilde{K}$ such that $P+\alpha=Q^2$ for some $Q\in K(x_1,\cdots,x_n)$. Furthermore, if K is computable, we can find these α.*

Proof. As before, we can show that the set of such α is a Zariski closed subset of $\tilde{K}$, whose defining equations can be calculated if K is computable. To show that this set is finite, it is enough to show that it is not all of $\tilde{K}$. Assuming that it is, we would have 0 being an element of this set and so P would be a square. Write $P=f^2/g^2$ where f and g have no common factors. For each α, we could find relatively prime f_α, g_α such that

$$\frac{f^2}{g^2}+\alpha=\frac{f_\alpha^2}{g_\alpha^2}\quad\text{or}\quad f^2+\alpha g^2=\frac{f_\alpha^2 g^2}{g_\alpha^2}.$$

From this we see that g_α is a constant multiple of g so $f^2+\alpha g^2=cf_\alpha^2$ for some constant c. Now apply the preceding lemma to get a contradiction. □

7. The decision procedure. In this section we shall prove Theorem 4.2. Let C be a computable field, F a purely exponential extension of $C(x)$ and $\gamma\in F$. Extend F to F^* as in Proposition 5.4 and use Proposition 5.3 to extend to a field E which is of minimal rank over $C(x)$. We may assume that C is algebraically closed since the algebraic closure of a computable field is still computable. Using Theorem 4.1 and Proposition 5.4, we see that we want to decide if there exist c_i and d_i in C and w_i, u_i, v_i in E such that

$$\gamma=w_0'+\sum c_i\frac{w_i'}{w_i}+\sum_{i\in I} d_i u_i' v_i\quad\text{where } v_i'=(-u_i^2)'v_i. \tag{7.1}$$

We can assume that if $\sum_{i\in J} d_i u_i' v_i$ has an elementary antiderivative for some subset $J\subset I$ and constants d_i, then $d_i=0$ for all i in J. This just means that all of the elementary part of the antiderivative of γ is contained in $w_0'+\sum c_i(w_i'/w_i)$. The idea behind the procedure is to first determine the possible expressions of the form $u_i'v_i$, with u_i, $v_i\in E$ and $v_i'=(-u_i^2)'v_i$, which could appear in (7.1). This is done as follows.

Let $C(x)=E_0\subset\cdots\subset E_r=E$ where $E_i=E_{i-1}(\theta_{i1},\cdots,\theta_{im_i})$ and $u'_{ij}=u'_{ij}\theta_{ij}$ with $u_{ij}\in E_{i-1}$ and $u_{ij}\notin E_{i-2}$. Let v and u be elements of E such that $v'=(-u^2)'v$ and let v have rank s (i.e. $v\in E_s$ but $v\notin E_{s-1}$). The Structure Theorem of [ROCA79] permits us to write

$$v=d\prod_{\substack{1\leqq j\leqq m_i\\1\leqq i\leqq s}}\theta_{ij}^{-n_{ij}}\tag{7.2}$$

with $n_{ij}\in\mathbf{Z}$, $d\in C$. For notational convenience, our n_{ij} are the negatives of those in [ROCA79]. Note that i ranges from 1 to s but no further since E is of minimal rank and that $n_{ij}\in\mathbf{Z}$ and not just in $\mathbf{Q}$ since E is a purely transcendental extension of C. We also have

$$u=\left(\sum_{\substack{1\leqq j\leqq m_i\\1\leqq i\leqq s}}n_{ij}u_{ij}+c\right)^{1/2}\tag{7.3}$$

where $c\in C$. We need one more piece of notation. Given any θ_{ij}, we can write γ in its partial fraction decomposition with respect to θ_{ij} over the field $C(x)$ $(\theta_{11},\cdots,\hat{\theta}_{ij},\cdots,\theta_{rm_r})$. (Where $\hat{}$ over an element means this element is omitted). Let

$$\gamma=A_{-m}\theta_{ij}^{-m}+\cdots+A_0+\cdots+A_l\theta_{ij}^l+\sum_{a,b}\frac{P_{ab}(\theta_{ij})}{Q_b(\theta_{ij})^{n_{ab}}}$$

where Q_b is an irreducible polynomial in θ_{ij}. not equal to θ_{ij}. We define $o_{ij}(\gamma)=\max(m,l)$. We claim that given v of rank s appearing in (7.1), we have $|n_{sj}|\leqq o_{sj}(\gamma)$ for $1\leqq j\leqq m_s$. We are saying that if v is of rank s, those θ_{ij}'s which are also of rank s appear to a power of absolute value less than $o_{sj}(v)$ in (7.2). This claim will be proven below, so let us assume it for a moment. We still must bound the other exponents appearing in (7.2). It would be natural to conjecture that $|n_{ij}|\leqq o_{ij}(\gamma)$, but this is not true, as the following example illustrates.

Example 7.1. Let $E=C(x,\exp x,\exp(-\exp(2x)+x))$. This is of minimal rank over $C(x)$. Letting $\gamma=\exp(-\exp(2x)+x)$, $\theta_1=\exp x$ and $\theta_2=\exp(-\exp(2x)+x)$ we have $\gamma=u'v$ where $u=\exp x=\theta_1$, $v=\exp(-\exp(2x))=\theta_2\theta_1^{-1}$ and $v'=(-u^2)'v$. Note that both v and θ_2 are of rank 2 and that the exponent of $\theta 2$ in v is bounded by (in fact equal to) $o_2(\gamma)$. Here θ_1 does not appear in γ, yet it does appear in v, ui.e. $n_1=-1$ while $o_1(\gamma)=0$.

We will bound the n_{ij} for $i<s$ using the results of § 6. Rewrite (7.3) as

$$u=\left(n_{s1}u_{s1}+\cdots+n_{sm_s}u_{sm_s}+\sum_{\substack{1\leqq j\leqq m_i\\1\leqq i< s}}n_{ij}u_{ij}+c\right)^{1/2}.$$

Let

$$P=n_{s1}u_{s1}+\cdots+n_{sm_s}u_{sm_s}\quad\text{and}\quad\alpha=\sum_{\substack{1\leqq j\leqq m_i\\1\leqq i< s}}n_{ij}u_{ij}+c.$$

Note that since E is of minimal rank over $C(x)$, we have that $P\in E_{s-1}$, $P\notin E_{s-2}$, and $\alpha\in E_{s-2}$. This is precisely where the notion of minimal rank is crucial. If we let $K=E_{s-2}$, we can apply Proposition 6.2 and find, for each choice of $(n_{s1},\cdots,n_{sm_s})$ satisfying $|n_{sj}|\leqq o_{sj}(\gamma)$, all $\alpha\in E_{s-2}$ such that $P+\alpha=Q^2$ for some Q in E_{s-1}. Each such α can be written in at most one way as $\sum n_{ij}u_{ij}+c$ since if $\sum n_{ij}u_{ij}+c=\sum\bar{n}_{ij}u_{ij}+\bar{c}$ we would have $\sum(n_{ij}-\bar{n}_{ij})u_{ij}\in C$, so the θ_{ij} would be algebraically dependent over C unless $n_{ij}=\bar{n}_{ij}$ and $c=\bar{c}$. The α's which can be written as such a sum will give us the exponents for the θ_{ij}'s of lower rank. Therefore, using our claim and Proposition 6.2, we can determine for each s, $1 \leqq s \leqq r$, all u and v in E which may appear in (7.1) such that $v' = (-u^2)'v$ and v is of rank s. We now wish to decide if there exist a_i, b_i in C and w_i in E such that

$$\gamma - \left(\sum a_i u_i' v_i \right) = w_0' + \sum b_i \frac{w_i'}{w_i}.$$

A procedure to decide this is presented in [MACK76]. Since this paper has never been published we have included in the Appendix a proof of the relevant theorem.

All that remains to be done is to prove that for v of rank s appearing in (7.1), $|n_{sj}| \leqq o_{sj}(\gamma)$. The proof of this claim follows closely Risch's proof of [RISC69, Main Theorem] and will yield a proof of Theorem 4.2 independent of [MACK76].

We will proceed by induction on the number of generators of E over $C(x)$. If we write $E = E_r = E_{r-1}(\theta_{r1}, \cdots, \theta_{rm_r})$ as before, let $\theta = \exp(u)$ denote one of the θ_{ri} and write $E = K(\theta)$, where $K = E_{r-1}(\theta_{r1}, \cdots, \hat{\theta}_{ri}, \cdots, \theta_{rm_r})$. Expanding γ in partial fractions with respect to θ, and assuming that γ satisfies (7.1) we have

$$\gamma = A_k\theta^k + \cdots + A_i\theta + A_0 + A_{-1}\theta^{-1} + \cdots + A_{-m}\theta^{-m}$$

$$+ \frac{A_{1k_1}}{p_1^{k_1}} + \cdots + \frac{A_{11}}{p_1} + \cdots + \frac{A_{sk_s}}{p_s^{k_s}} + \cdots + \frac{A_{s1}}{p_s}$$

$$(7.4) \qquad = \left\{ \begin{array}{l} B_t\theta^t + \cdots + B_1\theta + B_0 + B_{-1}\theta^{-1} + \cdots + B_{-l}\theta^{-l} \\ + \int \sum_{i \in \mathscr{S}} d_i u_i' v_i + \int \sum_{i \in \mathscr{T}} d_i u_i' v_i + \sum c_j \log D_j \\ + \frac{B_{1k_1}}{p_1^{k_1-1}} + \cdots + \frac{B_{11}}{p_1} + \int \frac{B_{10}}{p_1} \\ + \cdots + \\ + \frac{B_{sk_s}}{p_s^{k_s-1}} + \cdots + \frac{B_{s1}}{p_s} + \int \frac{B_{s0}}{p_s}. \end{array} \right\}$$

where the A's, B's and D's are in K, the p_i's are irreducible polynomials in $K[\theta]$, $B_{i0}/p_i = \sum c_{ij}(q_{ij}/q_{ij})$ where $p_i = \prod q_{ij}$ in $\tilde{K}[\theta]$. $v_i' = (-u_i^2)'v_i$ and $\mathscr{S}$ is the set of i such that $v_i \notin k$ while $\mathscr{T}$ is the set of i such that $v_i \in K$. Note that [ROS76, Thm. 2] implies that in either case u_i in K. Some justification is required for our implicit assumption that p_i^{-1} appears to a power of at most $k_i - 1$ in the second expression. This follows from the fact that for $i \in \mathscr{S}$, $v_i = f_i\theta^{n_i}$ for some $f_i \in K$ (again by [ROS 76, Theorem 2]) and so when differentiating the second expression we get no cancellation in this expression. Note that for $i \in \mathscr{S}$ we can write $v_i = c_i\theta^{n_i} \prod \theta_{ij}^{n_{ij}}$ where $n_i \neq 0$. We shall first prove our claim for v_i with $i \in \mathscr{S}$, that is, that $|n_i| \leqq \max(k, m)$. Assume not and let $n = \max_{i \in \mathscr{S}}(n_i)$. We then have

$$(B_n\theta^n)' + \sum_{\mathscr{S}'} d_i u_i' v_i = 0$$

where $\mathscr{S}'$ is the set of i such that $n_i = n$. This implies that $\sum_{\mathscr{S}'} d_i u_i' v_i$ has an elementary antiderivative, contrary to our assumptions. This proves our claim for the v_i with $i \in \mathscr{S}$. Furthermore, we see by comparing powers of θ in our two expressions that $t = k$ and $l = m$.

We now proceed to determine those v_i with $i \in \mathcal{S}$ which may appear in (7.4). We do this using the results of § 6 as above. Let

$$\sum_{i \in \mathcal{S}} d_i u_i' v_i = \sum_{\substack{j \neq 0 \\ -m \leqq j \leqq k}} C_j \theta^j$$

where C_j is of the form $\sum d_i C_{ij}$ with C_{ij} known elements of K and d_i constants to be determined. Equating powers of θ in (7.4) we get

$$\begin{aligned} A_k &= B_k' + ku' B_k + \sum d_i C_{ik}, \\ &\vdots \\ A_1 &= B_1' + u' B_1 + \sum d_i C_{i1}, \\ A_{-1} &= B_{-1}' - u' B_{-1} + \sum d_i C_{i,-1}. \\ &\vdots \\ A_{-m} &= B_{-m}' - mu' B_{-m} + \sum d_i C_{i,-m}. \end{aligned}$$

For each j we must determine if there exist constants d_i and elements B_j such that

$$B_j' + ju' B_j = A_j - \sum d_i C_{ij}.$$

This can be done using [RISC69, Main Theorem, part (b)]. Note that a solution is uniquely determined if it exists. In this way determine the B_j's and d_i's (for $i \in \mathcal{S}$). Proceeding as in [RISC69, p. 183], we can determine the $B_{i,k-1}, \cdots, B_{i,1}$ until we get down to an equation of the form

$$\sum_{i=1}^{s} \frac{A_{i1}}{p_i} + A_0 = \sum_{i=1}^{s} \frac{B_{i0}}{p_i} + B_0' + \sum_{i \in \mathcal{T}} d_i u_i' v_i + \left(\sum c_j \log D_j\right)'.$$

Again we proceed as in [RISC69] and reduce the problem to deciding if

$$A_0 - u' \sum m_i c_{ij} = \left(B_0 + \sum c_j \log D_j + \int \sum_{i \in \mathcal{T}} d_i u_i' v_i \right)'.$$

This is equivalent to deciding if

$$A_0 = \left(\bar{B}_0 + \sum c_j \log D_j + \int \sum_{i \in \mathcal{T}} d_i u_i' v_i \right)'$$

for some $\bar{B}_0$, D_j, u_i, v_i in K. Note that $o_{ij}(A_0) \leqq o_{ij}(\gamma)$ so by the induction hypothesis we have

$$o_{ij}(v_i) \leqq o_{ij}(A_0) \leqq o_{ij}(\gamma)$$

for all v_i appearing in (7.1). $\square$

Appendix. In this section, we present a proof of the result of Carola Mack alluded to in § 7. We must first recall some definitions from [ROCA79]. Let $k \subset K$ be differential fields. For $t \in K$ with $t' \in k$, we say that t is *simple logarithmic* over k if there exist $u_1, \cdots, u_m$ in $k (m \geqq 1)$ such that for some constant c, $t + c \in k(\log u_1, \cdots, \log u_m)$. We say it is *nonsimple* over k if it is not simple logarithmic over k. K is a *regular log-explicit extension* of k if K and k have the same subfield of constants and there exists a tower $k = K_0 \subset \cdots \subset K_n = K$ such that $K_i = K_{i-1}(\theta_i)$ where θ_i is transcendental over K_{i-1} and either

(i) $\theta_i' \in K_{i-1}$ and θ_i is nonsimple over K_{i-1}, or
(ii) $\theta_i' = u_i'/u_i$ for some $u_i \in K_{i-1}$, or
(iii) $\theta_i' = u_i' \theta_i$ for some $u_i \in K_{i-1}$.

We shall use the following fact several times in the proof of Theorem A1 below. Given a system L_1 of linear equations over a field K in $n+m$ variables $(x_1, \cdots, x_n, y_1, \cdots, y_m)$, there exists a system L_2 of linear equations over K in n variables $(x_1, \cdots, x_n)$ such that $(a_1, \cdots, a_n) \in K^n$ satisfies L_2 if and only if there exists $(b_1, \cdots, b_m) \in K^m$ such that $(a_1, \cdots, a_n, b_1, \cdots, b_m)$ satisfies L_1. This follows from the fact that the projection to K^n of an affine subspace in K^{n+m} is still an affine subspace. We will refer to L_2 as the projection of L_1 onto the first n variables.

THEOREM A1. *Let K be a finitely generated extension of Q and let $F = K(z, \theta_1, \cdots, \theta_n)$ be a regular log-explicit extension of $K(z)$, where $z' = 1$ and $c' = 0$ for all c in K.*

(a) *Let $f_0, f_1, \cdots, f_N$ be elements of F. Then one can determine in a finite number of steps a system L of linear equations in N variables with coefficients in K so that $f_0 + d_1 f_1 + \cdots + d_N f_N$ has an integral in an elementary extension of K for $d_1, \cdots, d_N$ in $\bar{K}$ (the algebraic closure of K) if and only if $(d_1, \cdots, d_N)$ satisfies L. For each $(d_1, \cdots, d_N)$ in $\bar{K}^N$ satisfying L, we can find $v_0 \in F$, $v_i \in \bar{K}F$ for $i = 1, \cdots, m$ and $c_1, \cdots, c_m$ in $\bar{K}$ such that*

$$f_0 + d_1 f_1 + \cdots + d_N f_N = v_0' + \sum_{i=1}^{m} c_i^{v_i'/v_i}.$$

(b) *Let f, g_i, $i = 1, \cdots, m$ be elements of F. Then one can find, in a finite number of steps $h_1, \cdots, h_r$ in F and a set L of linear equations in $m + r$ variables with coefficients in K, such that $y' + fy = \sum_{i=1}^{m} c_i g_i$ holds for $y \in F$ and c_i in K if and only if $y = \sum_{i=1}^{r} y_i h_i$ where y_i are elements of K and $c_1, \cdots, c_m, y_1, \cdots, y_r$ satisfy L.*

Proof. We shall mimic the proof of [RISC69, Main Theorem] (and assume that the reader is familiar with that paper) and so proceed by induction on n. If $n = 0$, then $F = K(z)$ so we may take $L = \{0, 0\}$, since any element in $K(z)$ has an elementary integral. The proof of part (b) is the same as in [RISC69]. To proceed with the induction step, let $D = K(z, \theta_1, \cdots, \theta_{n-1})$ and $F = D(\theta)$ where $\theta = \theta_n$.

(a) *Case* 1. $\theta' \in D$. Let $f = f_0 + d_1 f_1 + \cdots + d_N f_N$. We can write

$$f = \begin{Bmatrix} A_k\theta^k + \cdots + A_0 \\ + \dfrac{A_{1\,k_1}}{p_1^{k_s}} + \cdots + \dfrac{A_{1\,1}}{p_1} \\ \vdots \qquad\qquad \vdots \\ + \dfrac{A_{s\,k_s}}{p_s^{k_s}} + \cdots + \dfrac{A_{s\,1}}{p_s} \end{Bmatrix} = \begin{Bmatrix} B_{k+1}\theta^{k+1} + \cdots + B_0 \quad + \sum e_j \log D_j \\ + \dfrac{B_{1\,k_1-1}}{p_1^{k_1-1}} + \cdots \quad + \dfrac{B_{1\,1}}{p_1} + \displaystyle\int \dfrac{B_{1\,0}}{p_1} \\ \vdots \\ + \dfrac{B_{s\,k_1-1}}{p_s^{k_s-1}} + \cdots \quad + \dfrac{B_{s\,1}}{p_s} + \displaystyle\int \dfrac{B_{s\,0}}{p_s} \end{Bmatrix}'.$$

Here the A's are linear polynomials in $d_1, \cdots, d_N$ with coefficients in D and the B's are to be determined. Equating powers of θ, we have

$$0 = B'_{k+1}$$

so $B_{k+1} \in K$, and

$$A_k = (k+1) B_{k+1} \theta' + B'_k.$$

We can write $A_k = a_{k,0} + d_1 a_{k,1} + \cdots + d_N a_{k,N}$ with $a_{k,i}$ in D for $i = 0, \cdots, N$, so this last equation can be written as

$$B'_k = a_{k,0} + d_1 a_{k,1} + \cdots + d_N a_{k,N} - (k+1) B_{k+1} \theta'. \tag{A.1}$$

Using the induction hypothesis for (b), we conclude that there exist $h_{1k}, \cdots, h_{r_k k}$ in D and L_k, a system of linear equations in $N + r_k + 1$ variables with coefficients in K

such that (A.1) has a solution B_k in D if and only if $B_k=\sum_{i=1}^{r_k} y_{ik}h_{ik}$ where $y_{ik}\in K$ and $(d_1,\cdots,d_N,B_{k+1},y_{1k},\cdots,y_{r_kk})$ satisfies L_k. Notice that for each choice of $d_1,\cdots,d_N$ in K there is at most one choice of B_{k+1} in K for which there exist $y_{1k},\cdots,y_{r_kk}$ in K such that $(d_1,\cdots,d_N,B_{k+1},y_{1k},\cdots,y_{r_kk})$ satisfies L_k. Now let $B_k=\sum_{i=1}^{r_k} y_{ik}h_{ik}$ where the h_{ik} are indeterminants. We then have

$$A_{k-1}=kB_k\theta'+B'_{k-1}=k\left(\sum_{i=1}^{r_k} y_{ik}h_{ik}\right)\theta'+B'_{k-1}.$$

We can write $A_{k-1}=a_{k-1,0}+d_1a_{k-1,1}+\cdots+d_Na_{k-1,N}$, so

$$B'_{k-1}=a_{k-1,0}+d_1a_{k-1,1}+\cdots+d_Na_{k-1,N}+\sum_{i=1}^{r_k} y_{ik}(kh_{ik}\theta'). \tag{A.2}$$

Using the induction hypothesis for (b) allows us to conclude that there exist $h_{1,k-1},\cdots,h_{r_{k-1},k-1}$ in D and L_{k-1}, a system of linear equations in $N+r_k+r_{k-1}$ variables with coefficients in K such that (A.2) has a solution B_{k-1} in D if and only if $B_{k-1}=\sum_{i=1}^{r_{k-1}} y_{i,k-1}h_{i,k-1}$ where $y_{i,k-1}\in K$ and $(d_1,\cdots,d_N,y_{1,k},\cdots,y_{r_k,k},y_{1,k-1},\cdots,y_{r_{k-1}},k-1)$ satisfies L_{k-1}. Again, for each choice of $d_1,\cdots,d_N$, there is at most one choice of $(y_{1k},\cdots,y_{r_kk})$ for which there exists $(y_{1,k-1},\cdots,y_{r_{k-1},k-1})$ satisying L_{k-1}. We continue in this way, getting linear systems $L_{k-2},\cdots,L_2$ whose solutions guarantee the existence of $B_{k-2},\cdots,B_2$. Finally, we have $A_0=B_1\theta'+B'_0+\sum e_j(\log D_j)'$. If we set $A_0=a_{00}+d_1a_{1,0}+\cdots+d_Na_{N,0}$ and $B_1=\sum_{i=1}^{r_1} y_{i,1}h_{i,1}$ we get

$$a_{00}+d_1a_{1,0}+\cdots+d_Na_{N,0}-\sum_{i=1}^{r_1} h_{i,1}(y_{i,1}\theta')=B'_0+\sum e_j\,(\log D_j)'. \tag{A.3}$$

Using the induction hypothesis for part (a), we see that there exists a linear system L^* in $N+r_1$ variables such that an equation of this form holds for some $(d_1,\cdots,d_N,h_{11},\cdots,h_{r_11})$ satisfying L^*.

Now consider

$$\sum_{j=1}^{k_1}\frac{A_{ij}}{p_i^j}=\left[\sum_{j=1}^{k_1-1}\frac{B_{ij}}{p_1^j}+\int\frac{B_{10}}{p_1}\right]'. \tag{A.4}$$

We can find unique R, S, linear in $d_1,\cdots,d_N$ in $D[\theta,d_1,\cdots,d_N]$, with $\deg_\theta R<\deg_\theta p'_1$ and $\deg_\theta S<\deg_\theta p_1$ such that

$$Rp_1+Sp'_1=A_{1,k_1}.$$

Let $-(k-1)B_{1,k-1}=S$, substitute into (A.4), and obtain a new relation

$$\sum_{j=1}^{k_1-1}\frac{A_{ij}^{(*)}}{p_1^j}=\left[\sum_{j=1}^{k_1-2}\frac{B_{1\,j}}{p_1^j}+\int\frac{B_{1\,0}}{p_1}\right]'.$$

Continuing in this manner, we determine $B_{1\,k-2},\cdots,B_{1,1}$, all linear in $d_1,\cdots,d_N$. We are left with an equation of the form

$$\frac{A_{11}^{(**\cdots)}}{p_1}=\left[\int\frac{B_{1\,0}}{p_1}\right]'.$$

Here $B_{1\,0}/p_1=\sum_{j=1}^{s_1} c_{1j}q_{1j}/q'_{1j}$ where $p_1=\prod_{j=1}^{t_1} q_{1j}$ is a factorization of p_1 into monic irreducible factors over $\bar{K}D$. We must determine if c_{ij} exist in $\bar{K}$ such that the equation holds. Let

$$\frac{A_{11}^{(**\cdots)}}{p_1}=\sum_{j=1}^{t_1}\frac{Q_{ij}}{q_{ij}}$$

where Q_{ij} is linear in $d_1, \cdots, d_N$ and let L_1^{**} be the system of linear equations in $d_1, \cdots, d_N, c_1, \cdots, c_{s_1}$ gotten by equating terms in the partial fraction decomposition of

$$\sum \frac{Q_{ij}}{q_{ij}} = \sum c_{ij} \frac{q'_{ij}}{q_{ij}}.$$

Similarly we get $L_2^{**}, \cdots, L_s^{**}$ for $p_2, \cdots, p_s$. We now get L by projecting $L_k \cup \cdots \cup L_2 \cup L^* \cup L_1^{**} \cup \cdots \cup L_s^{**}$ onto the first N variables (see the remark preceding the statement of the Theorem 5.

Case 2. $\theta = \exp \zeta$. Let

$$f = \left\{ \begin{array}{lll} A_k\theta^k + \cdots & + A_0\theta & \\ + A_{-m}\theta^{-m} + \cdots + A_{-1}\theta^{-1} + A_0 & & \\ + \dfrac{A_{1k_1}}{p_1^{k_1}} + \cdots & + \dfrac{A_{11}}{p_1} & \\ \vdots & \vdots & \\ + \dfrac{A_{sk_s}}{p_s^{k_s}} + \cdots & + \dfrac{A_{s1}}{p_s} & \end{array} \right\} = \left\{ \begin{array}{lll} B_k\theta^k + \cdots & + B_1\theta & \\ + B_{-m}\theta^{-m} + \cdots + B_{-1}\theta^{-1} + B_0 + \sum e_j \log D_j & & \\ + \dfrac{B_{1k_1-1}}{p_1^{k_1-1}} + \cdots & + \dfrac{B_{11}}{p_1} + & \displaystyle\int \frac{B_{10}}{p_1} \\ \vdots & & \vdots \\ + \dfrac{B_{sk_s-1}}{p_s^{k_s-1}} + \cdots & + \dfrac{B_{s1}}{p_s} + & \displaystyle\int \frac{B_{s0}}{p_0} \end{array} \right\}$$

where the A's are linear polynomials in $d_1, \cdots, d_N$. We have

$$A_i = B'_i + i\zeta' B_k$$

for all i, $-m \leqq i \leqq k$, $i \neq 0$. Setting $A_i = a_{i0} + a_{i1}d_1 + \cdots + a_{iN}d_N$ we get for each i, $-m \leqq i \leqq k$, $i \neq 0$,

$$B'_i + i\zeta' B_i = a_{i1} + a_{i1}d_1 + \cdots + a_{iN}d_N. \tag{A.5}$$

Using the induction hypothesis for (b), there exists T_{ij} in D and linear systems L_i such that $B_i = \sum y_{ij}T_{ij}$ is a solution of (A.5) for y_{ij} in U if and only if the $d_1, \cdots, d_N$ and y_{ij} satisfy L_i.

Determine $B_{1k_1-1}, \cdots, B_{11}$; $B_{2k_1-1}, \cdots, B_{2,1}$; $\cdots$; $B_{sk_1-1}, \cdots, B_{si}$ as before until we obtain

$$\sum_{i=1}^{s} \frac{A_{i1}^{(**\cdots)}}{p_i} + A_0 = \sum_{i=1}^{s} \frac{B_{i0}}{p_i} + B'_0 + (\sum e_j \log D_j)'.$$

The $A_{i1}^{(**\cdots)}$ and A_0 are linear polynomials in $d_1, \cdots, d_N$. Let $p_i = \prod q_{ij}$ be the factorization of p_i into monic irreducible factors over $\bar{K}D$ and let degree $q_{ij} = n_i$. We then have for each i

$$\frac{A_{i1}^{(**\cdots)} + n_i\zeta'(\sum c_{ij})p_i}{p_i} = \frac{B_{i0}}{p_i} = \sum c_{ij}\frac{q'_{ij}}{q_{ij}}.$$

For each i, we get a linear system L_i^* in the c_{ij} and $d_1, \cdots, d_N$ by equating terms in the partial fraction decomposition. We finally must check to see that

$$A_0 - \zeta' \sum n_i c_{ij} = (B_0 + \sum e_j \log D_j)'.$$

Using the induction hypothesis for part (a), this gives a linear system L^{**} in $d_1, \cdots, d_N$ and the c_{ij}. We now get L by projecting $L_{-m} \cup \cdots \cup L_k \cup L_1^* \cup \cdots \cup L_s^* \cup L^{**}$ onto the first N variables $d_1, \cdots, d_N$.

(b) *Case* 1. $\theta' \in D$. For $y = A/p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ we proceed as in [RISC69, p. 184] to determine bounds for the α_i. Using these bounds we can set $y = Y/p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, substitute in $y'+fy=\sum c_i q_i$, clear denominators and get

$$RY'+SY=\sum c_i T_i. \tag{A.6}$$

We set

$$\begin{aligned} Y &= y_\alpha \theta^\alpha + y_{\alpha-1}\theta^{\alpha-1}+\cdots+y_0,\\ R &= r_\beta \theta^\beta+\cdots+r_0,\\ S &= s_\gamma\theta^\gamma+\cdots+s_0,\\ \sum c_i T_i &= t_\delta \theta^\delta+\cdots+t_0, \end{aligned}$$

with y_j, r_j, s_j in D and t_j linear in the c_i with coefficients in D. Substituting these expressions in (A.6) and comparing powers of θ, we get: (1) when $y'_\alpha \neq 0$, either (a) $\alpha+\beta \leqq \delta+1$ or (b) $\alpha+\gamma\leqq\delta+1$ or (c) $\alpha+\beta=\alpha+\gamma>\delta+1$; (2) when $y'_\alpha=0$, either (a) $\alpha+\beta-1\leqq\delta$ or (b) $\alpha+\gamma\leqq\delta$ or (c) $\alpha+\beta-1=\alpha+\gamma>\delta$. Case (1a), (1b), (2a), and (2b) yield bounds for α.

Case (1c) occurs when $r_\beta y'_\alpha+s_\gamma y_\alpha=0$ and $r_\beta y'_{\alpha-1}+s_\gamma y_{\alpha-1}+r_{\beta-1}y'_\alpha+(\alpha\theta' r_\beta+s_{\gamma-1})y_\alpha=0$. Letting $y_{\alpha-1}=vy_\alpha$ with $v\in D$ we have

$$\begin{aligned} &r_\beta y_\alpha v'+(r_\beta y'_\alpha+s_\gamma y_\alpha)v+r_{\beta-1}y'_\alpha+(\alpha\theta' r_\beta+s_{\gamma-1})y_\alpha=0,\\ &v'-r_{\beta-1}s_\alpha/r_\beta^2+s_{\gamma-1}/r_\beta+\alpha\theta'=0,\\ &\left(\int\frac{r_{\beta-1}s_\gamma-r_\beta s_{\gamma-1}}{r_\beta^2}\right)-\alpha\theta=v. \end{aligned}$$

We now deal with the cases when θ is nonsimple over D and when $\theta=\log\eta$ for some η in D (this is the only place where the hypothesis of a log-explicit extension comes into play). If θ is nonsimple over D, then using the induction hypothesis we find a linear system L in one indeterminate α such that α satisfies L if and only if

$$\left(\int\frac{r_{\beta-1}s_\gamma-r_\beta s_{\gamma-1}}{r_\beta^2}\right)-\alpha\theta$$

is elementary over D. Furthermore, there is at most one α in K satisfying L, since the existence of two such values would imply θ is simple. Therefore we can bound α in this case. if $\theta=\log\eta$ for some η in D, we use the original Risch Algorithm to determine α such that

$$\int\frac{r_{\beta-1}s_\gamma-r_\beta s_{\gamma-1}}{r_\beta^2}=v+\alpha\log\eta$$

for some v in D. If such an α exists it must be unique, otherwise $\log\eta$ would be in D. This allows us to again bound α.

To bound α in Case (2c), note that this case occurs when $r_\beta(y'_{\alpha-1}+\alpha\theta' y_\alpha)+s_\gamma y_\alpha=0$, or

$$\left(\int\frac{s_\gamma}{r_\beta}\right)+\alpha\theta=\frac{-y_{\alpha-1}}{y_\alpha}.$$

Treating the nonsimple and logarithmic cases separately as in Case (1c) above yields the bound for α. The rest of the proof is the same as [RISC69, pp. 185–186]. □

We can deduce the following corollary from Theorem A.1. By a regular Liouvillian extension we mean a Liouvillian extension (see the definition in § 4) where each θ used in building up the tower is transcendental over the preceding field.

COROLLARY A.2. *Let K be a finitely generated extension of Q and let $F = U(z, \theta_1, \cdots, \theta_n)$ be a regular Liouvillian extension of $K(z)$, where $z' = 1$ and $c' = 0$ for all c in U. Let $f_0, f_1, \cdots, f_N$ be elements of F. Then one can determine in a finite number of steps a system of linear equations in N variables with coefficients in K so that $f_0 + d_1 f_1 + \cdots + d_N f_N$ has an elementary integral for $d_1, \cdots, d_N$ in $\bar{K}$ if and only if $(d_1, \cdots, d_N)$ satisfies L. For each $(d_1, \cdots, d_N)$ in $\bar{K}^N$ satisfying L, we can find $v_0 \in F$, $v_i \in \bar{K}F$ for $i = 1, \cdots, m$ and $c_1, \cdots, c_m$ in $\bar{K}$ such that*

$$f_0 + d_1 f_1 + \cdots + d_N f_N = v_0' + \sum_{i=1}^{m} c_i \frac{v_i'}{v_i}.$$

Proof. This follows from Theorem A.1 and the fact, shown in [ROCA79], that one can effectively embed a regular Liouvillian extension of $K(z)$ into a regular log-explicit extension of $K(z)$. □

Since any purely exponential extension of $K(z)$ is a regular log-explicit extension of $K(z)$, Theorem A.1 gives the result needed in § 7. A result similar to Theorem A.1, for regular elementary extensions of $K(z)$ was stated and proven in [MACK76].

REFERENCES

[KOL73] E. KOLCHIN, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.

[LANG65] S. LANG, *Algebra*, Addison-Wesley, Reading, MA, 1965.

[MACK76] C. MACK, *Integration of affine forms over elementary functions*, Computer Science Dept., Univ. of Utah, Technical Report, VCP-39, 1976.

[MUM76] D. MUMFORD, *Algebraic Geometry* I, *Complex Projective Varieties*, Springer-Verlag, New York, 1976.

[MOSE69] J. MOSES, *The integration of a class of special functions with the Risch algorithm*, SIGSAM Bull. 13 (1969), pp. 14–27.

[MOZI79] J. MOSES AND R. ZIPPEL, *An extension of Liouville's Theorem* in Symbolic and Algebraic Computation, E. W. Ng, ed, Springer-Verlag, New York, 1979, pp. 426–430.

[RISC69] R. H. RISCH, *The problem of integration in finite terms*, Trans. Amer. Math. Soc., 139 (1969), pp. 167–189.

[RITT48] J. F. RITT, *Integration in Finite Terms*, Columbia Univ. Press, New York, 1948.

[ROCA79] M. ROTHSTEIN AND B. F. CAVINESS, *A Structure theorem for exponential and primitive functions*, this Journal, 8 (1979), pp. 357–367.

[ROS75] M. ROSENLICHT, *Differential extension fields of exponential type*, Pacific J. Math., 57 (1975), pp. 289–300.

[ROS76] ———, *On Liouville's theory of elementary functions*, Pacific J. Math., 65 (1976), pp. 485–492.

[ROSI77] M. ROSENLICHT AND M. F. SINGER, *On elementary, generalized elementary and Liouvillian extension fields*, in Contributions to Algebra, Bass, Cassidy and Kovacic, ed, Academic Press, New York, pp. 329–342.

[SING77] M. F. SINGER, *Functions satisfying elementary relations*, Trans. Amer. Math. Soc., 227 (1977), pp. 185–206.

[SSC81] M. F. SINGER, B. D. SAUNDERS AND B. F. CAVINESS, *An extension of Liouville's theorem on integration in finite terms*, Proc. 1981 ACM Symposium on Symbolic and Algebraic Computation, P. S. Wang, ed., Association for Computing Machinery, New York, 1981.

[VDW50] B. L. VAN DER WAERDEN, *Modern Algebra*, *Vol.* II, Second Edition, Frederick Ungar, New York, 1950.