Liouville's Theorem on Integration in Terms of Elementary Functions

R.C. Churchill

Prepared for the
Kolchin Seminar on Differential Algebra
(KSDA)
Department of Mathematics, Hunter College and the Graduate Center, CUNY
September, 2006

(This is a corrected and extended version of a lecture originally given in September 2002.)

This talk should be regarded as an elementary introduction to differential algebra. It culminates in a purely algebraic proof, due to M. Rosenlicht [Ros$_2$], of an 1835 theorem of Liouville on the existence of "elementary" integrals of "elementary" functions. The precise meaning of elementary will be specified. As an application of that theorem we prove that the indefinite integral $\int e^{x^2}\,dx$ cannot be expressed in terms of elementary functions.

Contents

§1. Basic (Ordinary) Differential Algebra
§2. Differential Ring Extensions with No New Constants
§3. Extending Derivations
§4. Logarithmic Differentiation
§5. Integration in Finite Terms

References

Throughout the notes "ring" means "commutative ring with (multiplicative) *identity". That identity is denoted by* 1 *when the ring should be clear from context; by* 1_R *when this may not be the case and the ring is denoted* R. *The product* rs *of ring elements* r *and* s *is occasionally denoted* $r \cdot s$.

1. Basic (Ordinary) Differential Algebra

Throughout the section R *is a ring.*

An additive group homomorphism $\delta : r \in R \mapsto r' \in R$ is a *derivation* if the *Leibniz rule*

$$(rs)' = r \cdot s' + r' \cdot s \tag{1.1}$$

holds for all $r, s \in R$; when δ is understood one simply refers to "the derivation $r \mapsto r'$ (on R)". The *kernel* of a derivation refers to the kernel of the underlying group homomorphism, i.e., $\{ r \in R : r' = 0 \}$. Note from (1.1) and induction that

$$(r^n)' = nr^{n-1} \cdot r', \qquad 1 \leq n \in \mathbb{Z}. \tag{1.2}$$

A *differential ring* consists of a ring R and a derivation[1] $\delta_R : R \to R$. When (R, δ_R) and (S, δ_S) are such a ring homomorphism $\varphi : R \to S$ is a *morphism of differential rings* when φ commutes with the derivations, i.e., when

$$\delta_S \circ \varphi = \varphi \circ \delta_R \,. \tag{1.3}$$

Differential rings constitute the objects of a category; morphisms of differential rings form the morphisms thereof.

An ideal $\mathfrak{i}$ of a differential ring R is a *differential ideal* if $\mathfrak{i}$ is "closed under the derivation", i.e., if $r \in \mathfrak{i}$ implies $r' \in \mathfrak{i}$. The kernel of any morphism in the category of differential rings is such an ideal. The quotient of a differential ring by a differential ideal inherits a derivation in the expected way, and the anticipated factorizations and isomorphisms are valid. In particular, when $f : R \to S$ is a morphism with kernel $\mathfrak{i}$ and $\varphi : R \to R/\mathfrak{i}$ is the canonical homomorphism there is a factorization

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle\varphi}\downarrow & \overset{\approx}{\nearrow} & \\ R/\mathfrak{i} & & \end{array} \tag{1.4}$$

[1] More generally, one can consider rings with many derivations. In that context what we have called a differential ring would be called an "ordinary differential ring". We have no need for the added generality.

into morphisms of the category.

When (R, δ_R) is a differential ring and $r \in R$ one often refers to the evaluation $\delta_R r$ as "differentiating r". When $r, s \in R$ satisfy $\delta_R r = s$ one refers to s as the *derivative* of r and to r as a *primitive*[2] of s.

Examples 1.5 :

(a) When x denotes a single indeterminate[3] over $\mathbb{R}$ the usual derivative d/dx gives the polynomial algebra $\mathbb{R}[x]$ the structure of a differential ring. More generally, when $R[x]$ is the polynomial algebra over R in a single indeterminate x the mapping $d/dx : \sum_j r_j x^j \mapsto \sum_j j r_j x^{j-1}$ is a derivation on $R[x]$, and thereby endows $R[x]$ with the structure of a differential ring. This is the *usual derivation* on $R[x]$.

(b) The mapping $r \in R \mapsto 0 \in R$ is a derivation on R, called the *trivial derivation*.

(c) Let F be a field, let x be a single indeterminate over F, and give $R := F[x]$ the usual derivation. Then the only proper differential ideal of R is the zero ideal. This follows immediately from the PID property of R and the fact that the derivative of any generator of a non-zero ideal, being of lower degree than that of the generator, cannot be in the ideal.

(d) The only derivation on a finite field is the trivial derivation. Indeed, when K is a finite field of characteristic $p > 0$ the Frobenius mapping $k \in K \mapsto k^p \in K$ is an isomorphism, and as a result any $k \in K$ has the form $k = \ell^p$ for some $\ell \in K$. By (1.2) we then have $k' = (\ell^p)' = p\ell^{p-1}\ell' = 0$, and the assertion follows.

The usual derivation on the polynomial ring $\mathbb{R}[x]$ is certainly familiar from elementary calculus, where it is primarily used for the analysis of functions. However, readers should also be aware of the fact that this derivative can be useful for purely algebraic reasons, e.g., for investigating the multiplicity of roots.

To recall this application let K be a field, let $p \in K[x]$ be a polynomial, and let $\alpha \in K$ be a root of p. Then we can write

$$p(x) = (x - \alpha)^m q(x) ,$$

[2] One is tempted to refer to primitives as "anti-derivatives" or "indefinite integrals," but that terminology is seldom encountered.

[3] As opposed to an n-tuple $x = (x_1, \ldots, x_n)$ of algebraically independent elements over $\mathbb{R}$.

where $q \in K[x]$ is relatively prime to $x - \alpha$ and $m \geq 1$ is an integer. When $m = 1$ the root is *simple*; otherwise it is *multiple*. In either case m is the *multiplicity* of the root. Applying the usual derivation to the displayed formula we see that

$$p'(x) = (x - \alpha)^m q'(x) + m(x - \alpha)^{m-1} q(x)\,,$$

and therefore

$$\begin{array}{lll} p'(x) = (x - \alpha)q'(x) + q(x) & \text{when} & m = 1\,, \\ p'(x) = (x - \alpha)^{m-1}\big((x - \alpha)q'(x) + mq(x)\big) & \text{when} & m > 1. \end{array}$$

Since $q(\alpha) \neq 0$ we have the following immediate consequence[4].

Proposition 1.6 : *Let K be a field, let x be a single indeterminate over K, assume the usual derivation on $K[x]$, and suppose $p \in K[x]$. Then an element $\alpha \in K$ is a multiple root of p if and only if $p(\alpha) = p'(\alpha) = 0$.*

Corollary 1.7 : *Suppose $L \supset K$ is an extension of fields and $p \in K[x]$ is such that p and p' are relatively prime. Then p has no multiple root in L.*

Proof : From the relatively prime assumption we can find elements $g, h \in K[x]$ such that $gp + hp' = 1$, and if $\ell \in L$ were a multiple root then evaluating at ℓ would yield the contradiction $0 = g(\ell) \cdot 0 + h(\ell) \cdot 0 = g(\ell)p(\ell) + h(\ell)p'(\ell) = 1$. **q.e.d.**

Corollary 1.8 : *Suppose $L \supset K$ is an extension of fields and $p \in K[x]$ is irreducible. Then p has no multiple root in L if and only if $p' \neq 0$.*

Proof :

$\Rightarrow$ If $p' = 0$ and $\ell \in L$ is a root of p then ℓ must be a multiple root by Proposition 1.6.

$\Leftarrow$ Since p is irreducible p' has lower degree than p the two elements p and p' must be relatively prime. We conclude from Corollary 1.7 that p has no multiple root in L.

q.e.d.

We need a characteristic zero consequence of Proposition 1.6 which requires (a) of the following preliminary result. Assertion (b) is never used in our subsequent work, but contrasting the 0 characteristic and positive characteristic cases can be instructive.

[4]The presentation of this result, and the two corollaries that follow, is patterned after [Hun, Chapter III, §6, Theorem 6.10, pp. 161-2].

Proposition 1.9 : *Suppose K is a field, x is a single indeterminate over K, and $p(x) \in K[x]$ has degree $n \geq 1$. Assume the usual derivation on $K[x]$. Then the following statements hold.*

(a) *When* $\mathrm{char}(K) = 0$ *the usual derivative $p'(x)$ of $p(x)$ has degree $n - 1$. In particular, $p'(x) \neq 0$.*

(b) *When* $\mathrm{char}(K) = p > 0$ *the polynomial $p(x)$ satisfies $p'(x) = 0$ if and only if $p(x)$ has the form $p(x) = \sum_{j=0}^{n} k_j x^j$, where $p|j$ whenever $0 \neq k_j \in K$.*

Proof : We have $p(x) = \sum_{j=0}^{n} k_j x^j$ and $p'(x) = \sum_{j=0}^{n} j k_j x^{j-1}$, where $n > 0$ and $k_n \neq 0$.

(a) If $\mathrm{char}(K) = 0$ then $nk_n \neq 0$, hence $p'(x) \neq 0$.

(b) If $\mathrm{char}(K) = p > 0$ then $p'(x) = 0$ if and only if $jk_j = 0$ for $j = 1, \ldots, n$, i.e., if and only if $jk_j \equiv 0 \pmod{p}$ for $j = 1, \ldots, n$, and this is obviously the case if and only if $p|j$ whenever $0 \neq k_j \in K$.

q.e.d.

Theorem 1.10 : *Any algebraic extension of a field of characteristic* 0 *is separable.*

Proof : By Proposition 1.9(a) and Corollary 1.7. **q.e.d.**

Remark 1.11 : Theorem 1.10 is false when the characteristic 0 assumption is dropped. To see a specific example let t be an indeterminate over $\mathbb{Z}/2\mathbb{Z}$, let $K = (\mathbb{Z}/2\mathbb{Z})(t)$ and let $\sqrt{t} \in K^a$ be a root of $p(x) = x^2 - t \in K[x]$. (K^a is used to denote an algebraic closure of K.) The polynomial is irreducible (otherwise t is easily seen to be algebraic over $\mathbb{Z}/2\mathbb{Z}$), but (by straightforward verification) factors in $K^a[x]$ as $(x - \sqrt{t}\,)^2$ (because $-\sqrt{t} = \sqrt{t}$ and $x^2 - t = (x + \sqrt{t}\,)(x - \sqrt{t}\,)$). The extension $K(\sqrt{t}\,) \supset K$ is therefore not separable. (For generalizations of this example see [Ste, p. 84].)

Suppose R is

- a differential ring with derivation δ_R,
- a subring of a differential ring S with derivation δ_S, and
- $\delta_S|_R = \delta_R$;

then R is a *differential subring* of S, $S \supset R$ is a *differential ring extension*, and the derivation δ_R on R is said to *extend* to (the derivation δ_S on) S. Of course "ring" is replaced by "integral domain" or "field" when R and S have those structures. The subscripts on both δ_R and δ_S are generally omitted, e.g., one simply refers to the extension $\delta : S \to S$ of the derivation $\delta : R \to R$.

Examples 1.12 :

(a) The kernel R_C of a derivation on R is a differential subring of R, and is a differential subfield when R is a field. Moreover, R_C contains the image of $\mathbb{Z}$ in R, i.e., the image of $\mathbb{Z}$ under the mapping $n \in \mathbb{Z} \mapsto n \cdot 1 := n \cdot 1_R \in R$. In particular, $0, \pm 1, \pm 2, \cdots \in R_C$. The verifications of these assertions are elementary. R_C is the *ring* (resp. *field*) *of constants* of R. Example: When the usual derivation on $\mathbb{R}[x]$ is assumed one has $\mathbb{R}[x]_C = \{\text{constant polynomials}\} \simeq \mathbb{R}$.

(b) Suppose R is an integral domain and Q_R is the associated quotient field. Then any derivation $\delta : r \to r'$ on R extends to Q_R via the quotient rule $(r/s)' := (sr' - rs')/s^2$, and this is the unique extension of δ to Q_R. The verifications (that this extension is well-defined and unique) are again elementary.

Proposition 1.13 : *Suppose* $L \supset K$ *is a differential field extension and* $\ell \in L \backslash K$. *Then* $K[\ell] \supset K$ *is a differential ring extension if and only if*

(i) $$\ell' \in K[\ell].$$

Proof :

$\Rightarrow$: Condition (i) is a consequence of the definition of a derivation.

$\Leftarrow$: If ℓ is algebraic over K the result follows from $K(\ell) = K[\ell]$ (an algebraic result assumed familiar to readers[5]). If ℓ is transcendental over K and $p(\ell) = \sum_j k_j \ell^j \in K[\ell]$ then $(p(\ell))' = \sum_j k_j' \ell_j + (\sum_j j k_j \ell^{j-1})\ell' \in K[\ell]$.

q.e.d.

[5]For a proof see, e.g., [Hun, Chapter V, §1, Theorem 1.6, p. 234].

2. Differential Ring Extensions with No New Constants

In this section $S \supset R$ is an extension of differential rings with derivations denoted, in both cases, by δ and $r \mapsto r'$.

Note that $S_C \supset R_C$.

Proposition 2.1 : *The following statements are equivalent:*

(a) ("no new constants") $S_C = R_C$*;*

(b) *if* $r \in R$ (already) *admits a primitive in* R *then* r *does not admit a primitive in* $S \backslash R$*; and*

(c) *if* $s \in S \backslash R$ *satisfies* $s' \in R$ *then* s' *has no primitive in* R.

Ring (or field) extensions satisfying any (and therefore all) of these conditions are called *no new constant* extensions. They should be regarded as "economical": they do not introduce primitives for elements of R which already admit primitives in R.

Proof :
(a) $\Rightarrow$ (b) : When $r \in R$ admits a primitive $t \in R$ as well as a primitive $s \in S \backslash R$ the element $s - t \in S \backslash R$ is a constant, thereby contradicting (a).

(b) $\Rightarrow$ (a) : When (a) fails there is a constant $s \in S \backslash R$, i.e., a primitive for $0 \in R$. Since $0 \in R$ is also a primitive for 0 this contradicts (b).

The equivalence of (b) and (c) is clear.

q.e.d.

Examples 2.2 :

(a) When K is any differential field the containment $K \supset K_C$ is a no new constant extension.

(b) Let $U \subset \mathbb{C}$ be any non-empty open set, pick $z_0 \in U$, and let K and L denote the fields of germs at z_0 of meromorphic functions on $\mathbb{C}$ and U respectively. The usual derivative d/dz induces derivations on both K and L, and we can thereby regard $L \supset K$ as an extension of differential fields. It is a no new constant extension since $L_C = K_C \simeq \mathbb{C}$.

(c) For an example of a differential field extension in which the no new constant condition fails consider $L \supset \mathbb{R}[x]$, where $\mathbb{R}[x]$ is the ring of (real-valued) polynomial functions on $\mathbb{R}$ and L is any field of complex-valued differentiable functions (in the standard sense) of the real variable x containing $\exp ix$. Here $\mathbb{R}[x]_C = \mathbb{R}$, and from $i = (\exp ix)'/\exp ix \in L\backslash\mathbb{R}[x]$ we conclude that $L_C \simeq \mathbb{C}$ is a proper extension of $\mathbb{R}[x]_C$.

Proposition 2.3 : *Suppose $L \supset K$ is a no new constant differential extension of fields of characteristic 0 and $\ell \in L\backslash K$ satisfies $\ell' \in K$. Then:*

(a) *ℓ is transcendental over K; and*

(b) *the derivative $(p(\ell))'$ of any polynomial $p(\ell) = \sum_{j=0}^{n} k_j \ell^j \in K[\ell]$ with $n > 0$ and $k_n \neq 0$ is a polynomial in ℓ of degree n if and only if $k_n \notin K_C$, and is of degree $n-1$ otherwise.*

Proof :

(a) Let $b := \ell' \in K$, and note from the no new constant hypothesis that $b \neq 0$.

If the result is false ℓ is algebraic over K and we can write the corresponding irreducible polynomial of $K[t]$ as $t^n + c_m t^m + \cdots + c_0 \in K[t]$, where $n > 1$, $0 \leq m < n$, and $c_m \neq 0$. ($c_m = 0$ would imply $\ell = 0$, resulting in the contradiction $\ell \in K$.) Differentiating

$$\ell^n + c_m \ell^m + \cdots + c_0 = 0$$

then gives

$$bn\ell^{n-1} + c_m' \ell^m + bc_m \ell^{m-1} + \cdots + c_0' = 0\,. \tag{i}$$

There are three cases to consider.

- $n - 1 > m$. In this instance division of (i) by bn (which by the characteristic 0 hypothesis cannot be 0) results in a monic polynomial relation satisfied by ℓ, involving coefficients in K, in which the associated polynomial has degree less than that of the irreducible polynomial. This contradicts the minimality of n.
- $n - 1 = m$ and $bn + c_m' \neq 0$. Then (i) becomes

  $$(bn + c_m')\ell^{m-1} + \cdots + c_0' = 0,$$

  and we can divide by $bn + c_m'$ to achieve the same contradiction as in the previous item.

- $n-1=m$ and $bn+c'_m=0$. Since $bn+c'_m=(\ell n+c_m)'$ and $\ell n+c_m\in L\backslash K$ (again by the characteristic 0 assumption), this contradicts the no new constant hypothesis.

These cases are exhaustive, and (a) is thereby established.

(b) The initial assertion regarding k_n is seen immediately by writing

$$(p(\ell))'=k'_n\ell^n+nk_n\ell^{n-1}\ell'+k'_{n-1}\ell^{n-1}+\cdots+k'_0$$

in the form

$$k'_n\ell^n+(k'_{n-1}+nbk_n)\ell^{n-1}+\cdots+k'_0=0\,.$$

If $k_n\in K_C$ and the final assertion fails then $0=k'_{n-1}+nbk_n=(k_{n-1}+nk_n\ell)'$, forcing $k_{n-1}+nk_n\ell\in K_C\subset K$. However, in view of the characteristic 0 assumption this would imply $\ell\in K$, contradicting (a).

q.e.d.

The following immediate consequence is well-known from elementary calculus, but one seldom sees a proof.

Corollary 2.4 : *The real and complex natural logarithm functions are transcendental over the rational function fields $\mathbb{R}(x)$ and $\mathbb{C}(x)$ respectively, and the real arctangent function is transcendental over $\mathbb{R}(x)$.*

In the subject of differential algebra the characteristic of field under discussion plays a very important role, as is immediately evident from the following result.

Proposition 2.5 : *Suppose K is a differential field and $k\in K\backslash K_C$. Then:*

(a) *k is transcendental over K_C when K has characteristic 0; and*

(b) *k is algebraic over K_C when K has characteristic $p>0$.*

Proof :

(a) Apply Proposition 2.3(a) to the no new constant differential field extension $K\supset K_C$.

(b) From $(k^p)'=pk^{p-1}k'=0$ one sees that $k^p\in K_C$ for any $k\in K\backslash K_C$. The element k is therefore a zero of $x^p-k^p\in K_C[x]$.

q.e.d.

Proposition 2.6 : *Suppose $L \supset K$ is a no new constant differential extension of fields of characteristic 0 and $\ell \in L \backslash K$ satisfies $\ell'/\ell \in K$. Then:*

(a) *ℓ is algebraic over K if and only if $\ell^n \in K$ for some integer $n > 1$; and*

(b) *when ℓ is transcendental over K the derivative $(p(\ell))'$ of any polynomial $p(\ell) = \sum_{j=0}^{n} k_j \ell^j \in K[\ell]$ with $n > 0$ and $k_n \neq 0$ is a polynomial of degree n, and is a multiple of $p(\ell)$ if and only if $p(\ell)$ is a monomial.*

Proof : Let $b := \ell'/\ell \in K$ and note from the no new constant hypothesis that $b \neq 0$.

(a) Assuming ℓ is algebraic over K let $t^n + k_m t^m + \cdots + k_0 \in K[t]$ be the corresponding irreducible polynomial, where $n > 1$ and $0 \leq m < n$. If all k_j vanish then $\ell = 0$, resulting in the contradiction $\ell \in K$, and we may therefore assume $k_m \neq 0$. Differentiating

$$\text{(i)} \qquad \ell^n + k_m \ell^m + \cdots + k_0 = 0$$

then gives

$$\text{(ii)} \qquad bn\ell^n + (k_m' + bmk_m)\ell^m + \cdots + k_0' = 0\,.$$

Multiplying (i) by bn and subtracting from (ii) results in a lower degree polynomial relation for ℓ unless the two polynomials coincide, in which case $k_m' + mbk_m = bnk_m$. This last condition in turn implies $k_m'/k_m = (n-m)b$, and it follows that

$$\begin{aligned} \frac{(k_m \ell^{m-n})'}{k_m \ell^{m-n}} &= \frac{(m-n)k_m \ell^{n-m-1} b\ell + k_m' \ell^{m-n}}{k_m \ell^{m-n}} \\ &= \frac{(m-n)bk_m \ell^{m-n} + k_m' \ell^{m-n}}{k_m \ell^{m-n}} \\ &= (m-n)b + k_m'/k_m \\ &= 0\,. \end{aligned}$$

This gives $k_m \ell^{m-n} \in L_C = K_C \subset K$, hence $\ell^{n-m} \in K$, and from the minimality of n we conclude that $\ell^n \in K$.

The converse is obvious.

(b) Write $(p(\ell))'$ in the form

$$(k_n' + bnk_n)\ell^n + \cdots + k_0'.$$

If $0 = k_n' + bnk_n$ then $(k_n\ell^n)' = (k_n' + bk_n)\ell^n = 0$, and we would therefore have $k_n\ell^n \in K_C \in K$. This gives $\ell^n \in K$, contradicting the transcendency of ℓ over K, and the assertion on the degree of $(p(\ell))'$ is thereby established.

If $p(\ell) = k\ell^n$ is a monomial (with $k \neq 0$, to avoid trivialities) we see from $(k\ell^n)' = (k' + bnk)\ell^n = \frac{k'+bnk}{k} \cdot k\ell^n$ that $(p(\ell))'$ is a multiple of $p(\ell)$.

Conversely, suppose $(p(\ell))' = q(\ell)p(\ell)$. Then then equality of the degrees of $p(\ell)$ and $(p(\ell))'$ implies $k := q(\ell) \in K$. If $p(\ell)$ is not a monomial let $k_n\ell^n$ and $k_m\ell^m$ be two distinct nonzero terms and note from $(p(\ell))' = kp(\ell)$ that

$$k_j' + jk_jb = kk_j \quad \text{for} \quad j = n, m\,.$$

This implies

$$\frac{k_n' + nk_nb}{k_n} = \frac{k_m' + mk_mb}{k_m}\,,$$

which in turn reduces to

$$a := (n-m)k_nk_mb + k_mk_n' - k_nk_m' = 0\,.$$

Direct calculation then gives

$$\left(\frac{k_n\ell^n}{k_m\ell^m}\right)' = \frac{a\,\ell^{n+m}}{(k_m\ell^m)^2} = 0\,,$$

hence $\frac{k_n\ell^n}{k_m\ell^m} \in K_C \subset K$, and once again we contradict the transcendency of ℓ over K. We conclude that $p(\ell)$ must be a monomial when $(p(\ell))'$ is a multiple of $p(\ell)$, and the proof is complete.

q.e.d.

Corollary 2.7 : *For any non zero rational function* $g(x) \in \mathbb{R}(x)$ *the composition* $\exp g(x)$ *is transcendental over the rational function field* $\mathbb{R}(x)$.

Proof : This is immediate from Proposition 2.6(a) since no non zero integer power of $\exp g(x)$ is contained in $\mathbb{R}(x)$. **q.e.d.**

3. Extending Derivations

Throughout the section $L \supset K$ is an extension of fields.

Here we are concerned with extending a derivation on K to a derivation on L, and we first point out that such an extension need not exist.

Example 3.1 : Let t be a single indeterminate over $\mathbb{Z}/2\mathbb{Z}$, set $K := (\mathbb{Z}/2\mathbb{Z})(t)$. Choose a root $\sqrt{t}$ of the polynomial $x^2 - t$ in some algebraic closure K^a of K. We claim that the usual derivation $p \mapsto p'$ cannot be extended to the extension field $K(\sqrt{t}\,)$. Indeed, if so then differentiating $(\sqrt{t}\,)^2 = t$ would give $0 = 2 \cdot \sqrt{t} \cdot (\sqrt{t}\,)' = 1$, which is obviously impossible.

As we will see, the obstruction to extending the derivation in this example is the fact that the algebraic field extension $K(\sqrt{t}) \supset K$ is not separable. A proof of this inseparability is included in Remark 1.11.

To determine when extensions exist it first proves useful to generalize the definition of a derivation. Specially, let R be a ring, let $\mathcal{A}$ be an R-algebra (by which we always mean a left and right R-algebra), and let M be an R-module (by which we always mean a left and right R-module). An additive group homomorphism $\delta : \mathcal{A} \to M$ is a *derivation* (*of* $\mathcal{A}$ *into* M) if the *Leibniz rule*

$$\delta(ab) = a \cdot \delta(b) + \delta(a) \cdot b \tag{3.2}$$

holds for all $a, b \in \mathcal{A}$. Any derivation $\delta : R \to R$ provides an example. Additional examples can be seen from the discussion of CASE I below. The abbreviations δa and a' are also used in this context, and extensions of such mappings have the obvious meaning.

Proposition 3.3 : *Assume, in the notation of the previous paragraph, that $\mathcal{A}$ is an integral domain and M is a vector space over the quotient field K of $\mathcal{A}$. Then any derivation $\delta : \mathcal{A} \to M$ extends to a derivation $\delta : K \to M$ via the quotient rule*

$$\delta(\tfrac{a}{b}) := \tfrac{b \cdot \delta(a) - a \cdot \delta(b)}{b^2}, \qquad a, b \in \mathcal{A}, \qquad b \neq 0,$$

and this is the unique extension to a derivation of K into M.

Proof : The proof is by straightforward verification. **q.e.d.**

For the remainder of the section $\delta : k \in K \mapsto k' \in L$ is a derivation.

Choose any element $\ell \in L\backslash K$. We first investigate extending δ to a derivation $\delta : K(\ell) \to L$. We examine the transcendental and separable algebraic cases individually.

CASE I: *ℓ is transcendental over K.*

If view of Proposition 3.3 it suffices to extend δ to the polynomial algebra $K[\ell]$, and to this end we choose any $m \in L$ and define $\delta : K[\ell] \to L$ by

(i) $$\delta : a = \textstyle\sum_j a_j \ell^j \mapsto \sum_j a_j' \ell^j + m \cdot \sum_j j a_j \ell^{j-1}\,.$$

Note, in particular, that

$$\delta(\ell) = m\,.$$

We claim that δ is a derivation as desired. Indeed, that δ is an additive group homomorphism extending the given derivation is clear; what requires verification is the Leibniz rule. Let $a, b \in K[\ell]$, $a = \sum_i a_i \ell^i$ and $b = \sum_j b_j \ell^j$.

As preliminary observations note that

$$\begin{aligned}(\textstyle\sum_i a_i \ell^i)(\sum_j j b_j \ell^{j-1}) &= \textstyle\sum_{ij} j a_i b_j \ell^{i+j-1} \\ &= \textstyle\sum_k (\sum_{i+j=k} j a_i b_j) \ell^{k-1} \\ &= \textstyle\sum_k (\sum_{i \le k} (k-i) a_i b_{k-i}) \ell^{k-1} \\ &= \textstyle\sum_k k (\sum_{i \le k} a_i b_{k-i}) \ell^{k-1} - \sum_k (\sum_{i \le k} i a_i b_{k-i}) \ell^{k-1}\end{aligned}$$

and that

$$\begin{aligned}(\textstyle\sum_k i a_i \ell^{i-1})(\sum_j b_j \ell^j) &= \textstyle\sum_{ij} i a_i b_j \ell^{i+j-1} \\ &= \textstyle\sum_k (\sum_{i \le k} i a_i b_{k-i}) \ell^{k-1}.\end{aligned}$$

As a consequence we have

$$\begin{aligned}&(\textstyle\sum_i a_i \ell^i)(\sum_j j b_j \ell^{j-1}) + (\sum_k i a_i \ell^{i-1})(\sum_j b_j \ell^j) \\ &= \textstyle\sum_k k (\sum_{i \le k} a_i b_{k-i}) \ell^{k-1} - \sum_k (\sum_{i \le k} i a_i b_{k-i}) \ell^{k-1} + \sum_k (\sum_{i \le k} i a_i b_{k-i}) \ell^{k-1} \\ &= \textstyle\sum_k k (\sum_{i \le k} a_i b_{k-i}) \ell^{k-1},\end{aligned}$$

which is more conveniently expressed as

$$\text{(ii)} \qquad \left\{ \begin{array}{l} \sum_k k(\sum_{i\leq k} a_i b_{k-i})\ell^{k-1} \\ \qquad = (\sum_i a_i\ell^i)(\sum_j j b_j \ell^{j-1}) + (\sum_k i a_i \ell^{i-1})(\sum_j b_j \ell^j)\,. \end{array} \right.$$

Similarly, for any finite collection $c_i, e_j \in R$ we have

$$\begin{aligned} (\textstyle\sum_i c_i\ell^i)(\sum_j e_j\ell^j) &= \textstyle\sum_{ij} c_i e_j \ell^{i+j} \\ &= \textstyle\sum_k(\sum_{i+j=k} c_i e_j)\ell^k \\ &= \textstyle\sum_k(\sum_{i=0}^k c_i e_{k-i})\ell^k. \end{aligned}$$

Taking $c_i = a_i$ and $e_j = b_j'$ this gives

$$\text{(iii)} \qquad \textstyle\sum_k(\sum_i a_i b_{k-i}')\ell^k = (\sum_i a_i\ell^i)(\sum_j b_j'\ell^j),$$

whereas taking $c_i = a_i'$ and $e_j = b_j$ the result is

$$\text{(iv)} \qquad \textstyle\sum_k(\sum_i a_i' b_{k-i})\ell^k = (\sum_i a_i'\ell^i)(\sum_j b_j\ell^j).$$

With the aid of (ii)-(iv) we then see that

$$\begin{aligned} (ab)' &= \Big(\textstyle\sum_k(\sum_{i=0}^k (a_i b_{k-i}))\ell^k\Big)' \\ &= \textstyle\sum_k(\sum_{i=0}^k (a_i b_{k-i})')\ell^k + m\sum_k k(\sum_{i=0}^k(a_i b_{k-i}))\ell^{k-1} \\ &= \textstyle\sum_k(\sum_{i=0}^k(a_i b_{k-i}' + a_i' b_{k-i}))\ell^k \\ &\qquad + (\textstyle\sum_i a_i\ell^i)(\sum_j j b_j\ell^{j-1}m) + (\sum_k i a_i \ell^{i-1}m)(\sum_j b_j\ell^j) \quad \text{(by (ii))} \\ &= \textstyle\sum_k(\sum_{i=0}^k(a_i b_{k-i}'))\ell^k + \sum_k(\sum_{i=0}^k(a_i' b_{k-i}))\ell^k \\ &\qquad + (\textstyle\sum_i a_i\ell^i)(\sum_j j b_j\ell^{j-1}m) + (\sum_k i a_i \ell^{i-1}m)(\sum_j b_j\ell^j) \\ &= (\textstyle\sum_i a_i\ell^i)(\sum_j b_j'\ell^j) + (\sum_i a_i'\ell^i)(\sum_j b_j\ell^j) \quad \text{(by (iii) and (iv))} \\ &\qquad + (\textstyle\sum_i a_i\ell^i)(\sum_j j b_j\ell^{j-1}m) + (\sum_k i a_i \ell^{i-1}m)(\sum_j b_j\ell^j) \\ &= (\textstyle\sum_i a_i\ell^i)(\sum_j b_j'\ell^j + m\sum_j j b_j \ell^{j-1}) \\ &\qquad + (\textstyle\sum_i a_i'\ell^i + m\sum_i i a_i\ell^{i-1})(\sum_j b_j\ell^j) \\ &= ab' + a'b\,, \end{aligned}$$

and the claim is thereby established.

In summary, *when* $\ell \in L\backslash K$ *is transcendental over* K *any derivation from* K *into* L *extends to a derivation of* $K(\ell)$ *into* L*. Moreover, for any* $m \in L$ *there is such an extension satisfying* $\ell' = m$*.*

CASE II: ℓ *is separable algebraic*[6] *over* K.

Recall once again[7] that the algebraic hypothesis on ℓ implies

(i) $$K[\ell] = K(\ell).$$

Let $p(t) = t^n + \sum_{j=0}^{n-1} k_j t^j \in K[t]$ denote the associated monic irreducible polynomial. If a given derivation $k \mapsto k'$ on K can be extended to a derivation of $K[\ell]$ into L then from $p(\ell) = 0$ we see that

$$\begin{aligned} 0 &= (p(\ell))' \\ &= n\ell^{n-1}\ell' + \sum jk_j\ell^{j-1}\ell' + \sum k_j'\ell^j \\ &= \ell'(n\ell^{n-1} + \sum jk_j\ell^{j-1}) + \sum k_j'\ell^j \\ &= \ell'(p'(\ell)) + \sum k_j'\ell^j\,. \end{aligned}$$

From the separability hypothesis and Corollary 1.8 we have $p'(t) \neq 0$, and since $p(t)$ has minimal degree w.r.t. $p(\ell) = 0$ it follows that $p'(\ell) \neq 0$. The calculation thus implies

(ii) $$\ell' = \frac{-\sum_{j=0}^{m} k_j'\ell^j}{p'(\ell)}\,.$$

We conclude that *there is at most one extension of the given derivation on* K *to a derivation of* $K[\ell]$ *into* L, *and if such an extension exists* (ii) *must hold and* (as a result) *the image must be contained in* $K[\ell]$. This is in stark contrast to the situation studied in CASE I, wherein the extensions were parameterized by the elements $m \in L$.

To verify that an extension does exist for each derivation $k \in K \mapsto k' \in L$ it proves convenient to define $\hat{D}q(t) \in K[t]$, for any polynomial $q(t) = \sum_j a_j t^y \in K[t]$, by $\hat{D}q(t) = \sum_j a_j' t^j \in K[t]$. Notice this enables us to write (ii) as

(iii) $$\ell' = \frac{-\hat{D}p(\ell)}{p'(\ell)}\,.$$

In fact $\hat{D} : q(t) \mapsto \hat{D}q(t)$ is a derivation of $K[t]$ into $K[t]$: it is the extension of $k \mapsto k'$ obtained from the choice $m = 0$ in (i) of CASE I (with ℓ in that formula replaced by t).

[6] This is, algebraic over K with separable monic irreducible polynomial in $K[x]$.

[7] See Footnote 5.

Now note from (i) that we can find a polynomial $s(t) \in K[t]$ such that

$$\text{(iv)} \qquad s(\ell) = \frac{-\hat{D}p(\ell)}{p'(\ell)} \in K[\ell]\,;$$

we define a mapping $\check{D} : K[t] \to K[t]$ (read $\check{D}$ as "D check") by

$$\text{(v)} \qquad \check{D} : q(t) \mapsto \hat{D}q(t) + s(t)q'(t)\,.$$

This is a derivation extending the given derivation $k \mapsto k'$ on K: it corresponds to the choice $m = s(t)$ in (i) of CASE I (again with ℓ in that formula replaced by t).

Let $\eta : K[t] \to L$ denote the "substitution" homomorphism $q(t) \in K[t] \mapsto q(\ell) \in L$, set $\mathfrak{i} := \ker(\eta)$, and note that $\mathfrak{i} \subset K[t]$ can also be described as the principal ideal generated by $p(t)$. Any $q(t) \in \mathfrak{i}$ therefore has the form $q(t) = p(t)r(t)$ for some $r(t) \in K[t]$, and from the Leibniz rule we see that

$$\begin{aligned}
\check{D}q(t) &= \check{D}(p(t)r(t)) \\
&= p(t)\hat{D}r(t) + \hat{D}p(t)r(t) + s(t)(p(t)r'(t) + p'(t)r(t))\,.
\end{aligned}$$

Evaluating t at ℓ and using (iv) then gives

$$\begin{aligned}
\check{D}q(\ell) &= p(\ell)\hat{D}r(\ell) + \hat{D}p(\ell)r(\ell) + s(\ell)\left(p(\ell)r'(\ell) + p'(\ell)r(\ell)\right) \\
&= 0 \cdot \hat{D}r(\ell) + \hat{D}p(\ell)r(\ell) + s(\ell) \cdot 0 \cdot r'(\ell) + s(\ell)p'(\ell)r(\ell) \\
&= \left(\hat{D}p(\ell) + s(\ell)p'(\ell)\right) r(\ell) \\
&= \left(\hat{D}p(\ell) + \tfrac{-\hat{D}p(\ell)}{p'(\ell)}p'(\ell)\right) r(\ell) \\
&= 0\,,
\end{aligned}$$

from which we see that $\check{D}(\mathfrak{i}) \subset \mathfrak{i}$. It follows immediately that $\check{D}$ induces a K_C-linear mapping $D : K[\ell] \to K[\ell]$, i.e., that a K_C-linear mapping $D : K[\ell] \to K[\ell]$ is well-defined by

$$\text{(vi)} \qquad Dq(\ell) := \eta(\check{D}q(t))\,, \quad q(\ell) \in K[\ell]\,.$$

Since D is K_C-linear it is, in particular, an additive group homomorphism. We claim it is a derivation. Indeed, using the derivation properties of $\check{D}$ and the ring homomorphism properties of η we see that for any $q(\ell), r(\ell) \in K[\ell]$ we have

$$\begin{aligned} D(q(\ell)r(\ell)) &= \eta(\check{D}(q(t)r(t))) \\ &= \eta(\, q(t)\check{D}r(t) + \check{D}q(t)r(t)\,) \\ &= \eta(q(t))\eta(\check{D}r(t)) + \eta(\check{D}q(t))\eta(r(t)) \\ &= q(\ell)Dr(\ell) + Dq(\ell)r(\ell)\,, \end{aligned}$$

and the claim follows. We conclude that $D : K[\ell] \to K[\ell]$ is a derivation, which from (v), and (vi), and the fact that $\eta|_K : K \to K[\ell]$ is an embedding, is seen to extend $k \mapsto k'$.

In summary: *when $\ell \in L\backslash K$ is separable algebraic over K any derivation $k \mapsto k'$ on K has a unique extension to the field $K(\ell) = K[\ell]$. Moreover, the derivative of ℓ within this extension is given by* (ii)*, wherein $p(t) = t^n + \sum_{j=0}^{n-1} k_j t^j \in K[t]$ denotes the monic irreducible polynomial* of ℓ.

Theorem 3.4 : *When $L \supset K$ is an extension of fields of characteristic zero and $\delta : K \to K$ is a derivation the following statements hold.*

(a) *δ extends to a derivation $\delta_L : L \to L$.*

(b) *When $\ell \in L\backslash K$ is transcendental over K and $m \in L$ is arbitrary one can choose the extension δ_L so as to satisfy $\delta_L(\ell) = m$.*

(c) *When $L \supset K$ is algebraic the extension $\delta_L : L \to L$ of* (a) *is unique.*

Proof :

(a) When $L \supset K$ is a simple extension this is immediate from the preceding discussion. (By Theorem 1.10 the separability condition required in CASE II is a consequence of the characteristic zero assumption.) The remainder of the argument is a routine application of Zorn's lemma.

(b) Immediate from the discussion of CASE I.

(c) Immediate from the discussion of CASE II.

q.e.d.

4. Logarithmic Differentiation

In this section $L \supset K$ is an extension of differential fields.

Here we isolate two technical results needed for the proof of Liouville's Theorem.

For any element $t \in L$ one refers to the element $t'/t \in L$ as the *logarithmic derivative* of t. Using induction and the Leibniz rule one sees that for any nonzero $t_1, \ldots, t_n \in L$ and any (not necessarily positive) integers $m_1, \ldots, m_n$ one has the *logarithmic derivative identity*

$$\frac{(\Pi_{j=1}^{n} t_j^{m_j})'}{\Pi_{j=1}^{n} t_j^{m_j}} = \textstyle\sum_{j=1}^{n} m_j \frac{t_j'}{t_j}\,. \tag{4.1}$$

Proposition 4.2 : *Suppose $L = K(\ell)$, where ℓ is transcendental over K. Suppose $\alpha \in K$ and there are constants $c_1, \ldots, c_m \in K_C$ and elements $r(\ell)$ and $q_j(\ell) \in L$, $j = 1, \ldots, m$, such that*

(i) $$\alpha = \textstyle\sum_{j=1}^{m} c_j \frac{(q_j(\ell))'}{q_j(\ell)} + (r(\ell))'.$$

Then one can assume w.l.o.g. that:

- (a) *all $q_j(\ell)$ are in $K[\ell]$; that*
- (b) *each $q_j(\ell)$ not in K is monic and irreducible; and that*
- (c) *$q_i(\ell)$ and $q_j(\ell)$ are distinct when $i \neq j$ and neither is in K.*

What one *cannot* conclude is that for all $1 \leq j \leq m$ one has $(q_j(\ell))' \in K[\ell]$. For that one needs additional hypotheses.

When conditions (a)-(c) hold we say that equality (i) is *normalized*[8].

Proof : Each $q_j(\ell)$ can be written in the form $k_j \Pi_{i=1}^{n_j} (q_{ji}(\ell))^{n_{ji}}$, where $k_j \in K$, $q_{ji}(\ell) \in K[\ell]$ is monic and irreducible, and the n_j and n_{ji} are integers with $n_j > 0$ (no such restriction occurs for the n_{ij}). The logarithmic identity (4.1) then allows us to assume the $q_j(\ell)$ appearing in (ii) are either non-constant monic irreducible polynomials in $K[\ell]$ or elements of K. This gives (a) and (b); for (c) combine "like terms," e.g., write $c_i \frac{(q_i(\ell))'}{q_i(\ell)} + c_j \frac{(q_j(\ell))'}{q_j(\ell)}$ as $(c_i + c_j)\frac{(q_i(\ell))'}{q_i(\ell)}$ when $q_i(\ell) = q_j(\ell)$. **q.e.d.**

[8] This terminology is not standard, but proves convenient.

Proposition 4.3 : *Assume* $L = K(\ell)$, *where* ℓ *is transcendental over* K *and* $\ell' \in K[\ell]$. *Suppose* $\alpha \in K$, *and that* $p(\ell)$ *is a monic irreducible polynomial such that* $(p(\ell))' \in K[\ell]$ *is not divisible by* $p(\ell)$. *Then in any normalized equality*

(i) $$\alpha = \sum_{j=1}^{m} c_j \frac{(q_j(\ell))'}{q_j(\ell)} + (r(\ell))'.$$

one has $q_j(\ell) \neq p(\ell)$ *for* $j = 1, \ldots, m$.

Proof : We first note, from $\ell' \in K[\ell]$ and Proposition 1.13, that $K[\ell] \supset K$ is a differential ring extension.

Suppose $p(\ell) \in K[\ell]$ has the stated properties. In view of the preceding comment $(p(\ell))'/p(\ell)$ must be in reduced form when regarded as an element of the quotient field $K(\ell)$ of $K[\ell]$. If for some $q_j(\ell)$ appearing in (i) we have $q_j(\ell) = p(\ell)$, it follows that $(p(\ell))'/p(\ell)$ must be a term of the partial fraction expansion of $\sum_{j=1}^{m} c_j \frac{(q_j(\ell))'}{q_j(\ell)}$. Indeed, one sees immediately that this partial fraction expansion contains only one term with denominator involving $p(\ell)$, and that denominator is $p(\ell)$ alone.

Since α has no denominators it is evident from (i) that this last-mentioned term must be canceled by a term in the partial fraction expansion of $(r(\ell))'$. This in turn forces the appearance of $p(\ell)$ as a denominator in the partial fraction expansion of $r(\ell)$. Each such occurrence in the latter expansion has the form $f(\ell)/(p(\ell))^e$, where the degree of $f(\ell)$ is less than that of $p(\ell)$. Let $d \geq 1$ denote the maximal such e. The corresponding terms of the partial fraction expansion of $(r(\ell))'$ then consist of

$$\left(\frac{f(\ell)}{(p(\ell))^d}\right)' = \left(f(\ell)(p(\ell))^{-d}\right)' = \frac{-d \cdot f(\ell) \cdot (p(\ell))'}{(p(\ell))^{d+1}} + \frac{(f(\ell))'}{(p(\ell))^d}$$

together with at most finitely many quotients of the form $q(\ell)/(p(\ell))^h$, each with $1 \leq h < d + 1$. Arguing as at the beginning of the paragraph we conclude that the term $\frac{-d \cdot f(\ell) \cdot (p(\ell))'}{(p(\ell))^{d+1}}$ must be canceled by a term in the partial fraction expansion of $\sum_{j=1}^{m} c_j \frac{(q_j(\ell))'}{q_j(\ell)}$. But this is impossible, since we have already noted that in this latter expansion the relevant denominator only involves $p(\ell)$ to the first power. The result follows. **q.e.d.**

5. Integration in Finite Terms

Throughout the section K denotes a differential field of characteristic 0.

In this section we prove the theorem of Liouville cited in the introduction[9]. Our first order of business is making precise the notion of an "elementary function."

Let K be a differential field. An element $\ell \in K$ is a *logarithm* of an element $k \in K\backslash\{0\}$, and k an *exponential* of ℓ, if $\ell' = k'/k$ or, equivalently, if $k' = k\ell'$. When this is the case it is customary to write ℓ as $\ln k$ and/or k as e^{ℓ}; one then has the expected formulas

$$(\ln k)' = k'/k \quad \text{and} \quad (e^{\ell})' = e^{\ell}\,\ell'\,. \tag{5.1}$$

These definitions are obvious generalizations of concepts from elementary calculus, and examples are therefore omitted.

Let $K(\ell) \supset K$ be a non-trivial simple differential field extension. One says that $K(\ell)$ is obtained from K by

(a) the *adjunction of an algebraic element over* K when ℓ algebraic over K, by

(b) the *adjunction of a logarithm of an element of* K when $\ell = \ln k$ for some $k \in K$, or by

(c) the *adjunction of an exponential of an element of* K when $\ell = e^k$ for some $k \in K$.

A differential field extension $L \supset K$ is *elementary* if there is a finite sequence of intermediate differential field extensions $L = K_n \supset K_{n-1} \supset \cdots \supset K_0 = K$ such that each $K_{j+1} \supset K_j$ has one of these three forms, and when this is the case any $\ell \in L$ is said to be *elementary* over K. By an *elementary function* we mean an element of an elementary differential field extension $L \supset R(x)$ wherein $R = \mathbb{R}$ or $\mathbb{C}$, the elements of L are functions[10] (in the sense of elementary calculus), and the standard derivative is assumed.

[9]Our argument is from [Ros$_2$], which is adapted from [Ros$_1$]. A generalization of Liouville's Theorem 5.2 can be found in [Ros$_3$].

[10]The algebraic treatment is much cleaner when the relevant differential fields are defined in terms of function germs at a point of R. For example, one can then ignore the fact that a rational function $f \in \mathbb{R}(x)$ has a vastly different domain than $\ln x$. Readers familiar with the germ concept should have no trouble formulating such an approach. That framework has been slighted in these notes - it appears only in Example 2.2(b) - since readers are not assumed familiar with function germs, and it is not clear that the benefits would be worth the work involved in presenting the necessary background.

Theorem 5.2 (Liouville) : *Let K be a differential field of characteristic 0 and let $\alpha \in K$. Then α has a primitive within an elementary no new constant differential field extension of K if and only if there are constants $c_1, \ldots, c_m \in K_C$ and elements $\beta_1, \ldots, \beta_m, \gamma \in K$ such that $\beta_j \neq 0$ for $j = 1, \ldots, m$ and*

$$\text{(i)} \qquad \alpha = \textstyle\sum_{j=1}^{m} c_j \frac{\beta_j'}{\beta_j} + \gamma' \, .$$

Proof (M. Rosenlicht) **:**

$\Rightarrow$ By assumption there is a tower $K_n \supset K_{n-1} \supset \cdots \supset K_0 = K$ of differential field extensions such that each K_j with $j \geq 1$ is obtained from K_{j-1} by the adjunction of an algebraic element over K_{j-1}, a logarithm of an element of K, or an exponential of an element in K. Moreover, there is an element $\rho \in K_n$ such that $\rho' = \alpha$.

We argue by induction on the "length" $n \geq 0$ of an elementary extension, first noting that when $n = 0$ the desired equality holds by taking $m = 1$, $c_1 = 0$, and $\gamma := \rho$. If $n > 0$ and the result holds for $n-1$ we can view α as an element of K_1 and thereby apply the induction hypothesis to the elementary extension $K_n \supset K_1$, obtaining a non-negative integer m, constants $c_1, \ldots, c_m \in K_1$ and elements $\beta_1, \ldots, \beta_m, \gamma \in K_1$ such that the displayed equation of the theorem statement holds. Since the extension $K_1 \supset K$ has no new constants we must actually have $c_j \in K_C$ for $j = 1, \ldots, m$, and we are thereby reduced to proving the following result: *If $\alpha \in K$ can be written as displayed above, with all $c_j \in K_C$ and γ and all β_j in $K(\ell) = K_1$, then it can also be expressed in this form, although possibly with a different m and different c_j, γ and β_j, with all c_j again in K_C, but with γ and all β_j now contained in K.*

Case (a) : *ℓ is algebraic over K.*

Choose an algebraic closure K^a for K containing $K(\ell)$ and let $\sigma_i : K(\ell) \to K^a$ be the distinct embeddings of $K(\ell)$ into K^a over K, $i = 1, \ldots, s$, where w.l.o.g. σ_1 is inclusion. Then the images $\ell_i := \sigma_i(\ell)$ are the roots of the monic irreducible polynomial $p \in K[x]$ of ℓ, and the σ_i permute these roots.

Extend the given derivation to K^a. This extension is unique by Theorem 3.4(c), and will again be denoted δ. Since each $\sigma_i \circ \delta \circ \sigma_i^{-1} : K^a \to K^a$ is also a derivation extending $\delta|_K$ this uniqueness forces $\sigma_i \circ \delta \circ \sigma_i^{-1} = \delta$, i.e.,

$$\sigma_i \circ \delta = \delta \circ \sigma_i, \qquad i = 1, \ldots, s.$$

Recall that in this case[11] $K(\ell) = K[\ell]$. For any $q(\ell) \in K[\ell]$ we obviously have

[11] See Footnote 5.

$\sigma_i(q(\ell)) = q(\ell_i)$, and from the displayed formula of the previous paragraph we see that $\sigma_i((q(\ell))') = (q(\ell_i))' \in K[\ell]$ holds as well, $i = 1, \ldots, s$.

Choose polynomials $q_1, \ldots, q_n, r \in K[x]$ such that

$$\beta_j = q_j(\ell), \qquad j = 1, \ldots, n, \qquad \text{and} \qquad \gamma = r(\ell).$$

Write (i) accordingly, i.e., as

$$\alpha = \textstyle\sum_j c_j \frac{(q_j(\ell))'}{q_j(\ell)} + (r(\ell))';$$

then apply σ_i to obtain

$$\begin{aligned} \alpha &= \textstyle\sum_j c_j \frac{\sigma_i(\beta_j')}{\sigma_i(\beta_j)} + \sigma_i(\gamma') \\ &= \textstyle\sum_j c_j \frac{(\sigma_i(\beta_j))'}{\sigma_i(\beta_j)} + (\sigma_i(\gamma))' \\ &= \textstyle\sum_j c_j \frac{(q_j(\ell_i))'}{q_j(\ell_i)} + (r(\ell_i))'. \end{aligned}$$

Summing over i, dividing by s (which requires the characteristic 0 hypothesis), and appealing to the logarithmic derivative identity (4.1) yields

$$\begin{aligned} \alpha &= \tfrac{1}{s} \textstyle\sum_i \left(\sum_j c_j \frac{(q_j(\ell_i))'}{q_j(\ell_i)} \right) + \frac{1}{s} \cdot \sum_i (r(\ell_i))' \\ &= \textstyle\sum_{j=1}^n \frac{c_j}{s} \left(\sum_i \frac{(q_j(\ell_i))'}{q_j(\ell_i)} \right) + \frac{1}{s} \left(\sum_{i=1}^s r(\ell_i) \right)' \\ &= \textstyle\sum_{j=1}^n \frac{c_j}{s} \frac{(\Pi_{i=1}^s q_j(\ell_i))'}{\Pi_{i=1}^s q_j(\ell_i)} + \left(\frac{\sum_{i=1}^s r(\ell_i)}{s} \right)'. \end{aligned}$$

By construction each of the products and sums on the right-hand-side of this equality is fixed by each σ_i, and as a result must belong K (the usual symmetric polynomial argument). This last expression for α therefore has the required form.

Having established Case (a) we may assume, for the remainder of the proof, that ℓ is transcendental over K. We can then find $q_j(\ell), r(\ell) \in K(\ell)$ such that $\beta_j = q_j(\ell)$ and $\gamma = r(\ell)$, and thereby write

$$\text{(ii)} \qquad \alpha = \textstyle\sum_{j=1}^n c_j \frac{(q_j(\ell))'}{q_j(\ell)} + (r(\ell))'.$$

Indeed, we can assume this equality is normalized in the sense of Proposition 4.2.

Case (b) : ℓ *is a logarithm of an element of* K, i.e., $\ell' = k'/k$ for some $k \in K$.

First note from $\ell' = k'/k \in K \subset K[\ell]$, Proposition 1.13 and Example 1.12(b) that $K(\ell) \supset K$ is a differential field extension.

Let $p(\ell) \in K[\ell]$ be non-constant, monic and irreducible. From monotonicity we see that $(p(\ell))'$ has lower degree than $p(\ell)$, and as a result that $p(\ell)$ cannot divide $(p(\ell))' \in K[\ell]$. It follows from Proposition 4.3 that all $q_j(\ell)$ appearing in the sum $\sum_{j=1}^{n} c_j \frac{(q_j(\ell))'}{q_j(\ell)}$ within (ii) are in K, and we therefore only need be concerned with $r(\ell)$.

To that end observe from $(r(\ell))' \in K$ and Proposition 2.3(b) (which requires the no new constant hypothesis) that $r(\ell)$ must have the form $r(\ell) = c\ell + \hat{c}$, where $c \in K_C$ and $\hat{c} \in K$. Equality (ii) is thereby reduced to

$$\alpha = \sum_{j=1}^{n} c_j \frac{q_j'}{q_j} + c\,\frac{k'}{k} + \hat{c}\,',$$

precisely as desired.

Case (c) : ℓ *is an exponential of an element of* K, i.e., $\ell'/\ell = k'$ for some $k \in K$.

In this case we see from $\ell' = \ell k' \in K[\ell]$, Proposition 1.13 and Example 1.12(b) that $K(\ell) \supset K$ is a differential field extension.

As in Case (b) let $p(\ell) \in K[\ell]$ be non-constant, monic, and irreducible. From Proposition 2.6 (and the irreducibility of p) we see that for $p(\ell) \neq \ell$ we have $(p(\ell))' \in K[\ell]$, and that $p(\ell)$ does not divide $(p(\ell))'$; we can then argue as in the previous case to conclude that all $q_j := q_j(\ell)$ in (ii) are in K, with $q_j(\ell) = \ell$ as a possible exception.

On the other hand, in all cases the quotients $(q_j(\ell))'/q_j(\ell)$ are in K, and the same therefore holds for $(r(\ell))'$. A second appeal to Proposition 2.6(b) gives $r := r(\ell) \in K$.

If $q_j(\ell) \neq \ell$ for all j we are done, so assume w.l.o.g. that $q_1(\ell) = \ell$. We can then write

$$\alpha = c_1\,\frac{\ell'}{\ell} + \sum_{j=2}^{n} c_j\,\frac{q_j'}{q_j} + r\,' = \sum_{j=2}^{n} c_j\,\frac{q_j'}{q_j} + (c_1 k + r)\,',$$

which achieves the required form.

$\Leftarrow$ When (i) holds we have $\alpha = \left(\sum_{j=1}^{m} c_j \ln \beta_j + \gamma\right)'$.

q.e.d.

Corollary 5.3 (Liouville) : *Suppose $E \subset K = E(e^g)$ is a no new constant differential extension of fields of characteristic 0 obtained by adjoining the exponential of an element $g \in E$. Suppose in addition that e^g is transcendental over E and let $f \in E$ be arbitrary. Then $fe^g \in K$ has a primitive within some elementary no new constant differential field extension of K if and only if there is an element $a \in E$ such that*

(i) $$f = a' + ag' .$$

Proof : To ease notation write e^g as ℓ.

$\Rightarrow$ By Theorem 5.2 the element $f\ell \in K$ has a primitive as stated if and only if there are elements $c_j \in K_C = E_C$ and elements γ and $\beta_j \in K$, $j = 1, \ldots, m$, such that

(ii) $$f\ell = \sum_{j=1}^{m} c_j \frac{\beta_j'}{\beta} + \gamma'.$$

Write γ as $r(\ell)$ and β_j as $g_j(\ell)$ and assume, as in the discussion surrounding equation (ii) of the proof of Theorem 5.2, that the $q_j(\ell)$ are either non-constant monic irreducible polynomials in $K[\ell]$ or elements of E. Arguing as in Case (c) of that proof (again with K replaced by E) we can then conclude that ℓ is both the only possible monic irreducible factor in a denominator of the partial fraction expansion of $r(\ell)$ as well as the only possibility for a monic irreducible $g_j(\ell) \in K[\ell]\backslash E$. But this gives $(g_j(\ell))'/g_j(\ell) \in E$ for all j as well as $r(\ell) = \sum_{j=-t}^{t} k_j \ell^j$, where $t > 0$ is an integer and the coefficients k_j are in E. In particular, (ii) can now be written

$$f\ell = c + \sum_{j=-t}^{t} k_j' \ell^j + g' \sum_{j=-t}^{t} j k_j \ell^j = c + \sum_{j=-t}^{t} (k_j' + j g' k_j)\ell^j.$$

and upon comparing the K-coefficients of equal powers of ℓ we conclude that $f = k_1' + k_1 g'$. Equation (i) then follows by taking $a = k_1$.

$\Leftarrow$ When (i) holds $ae^g \in K$ is a primitive of fe^g.

q.e.d.

Corollary 5.4 : *For $R = \mathbb{R}$ or $\mathbb{C}$ the function $x \in R \mapsto e^{x^2} \in R$ has no elementary primitive.*

By an *elementary primitive* we mean a primitive within some elementary no new constant differential field extension of $R(x)(e^{x^2})$.

Proof : By Corollaries 2.4 and 5.3 the given function has an elementary primitive if and only if there is a function $a \in R(x)$ such that $1 = a' + 2ax$.

There is no such function. To see this assume $a = p/q \in R(x)$ satisfies this equation, where w.l.o.g. $p, q \in R[x]$ are relatively prime. Then from $1 = \frac{qp' - q'p}{q^2} + 2 \cdot \frac{px}{q} \Rightarrow q - 2px - p' = -\frac{-q'p}{q}$ we see that $q|q'p$. Now choose $s, t \in R[x]$ such that $sq + tp = 1$, whereupon multiplication by q' gives $sqq' + tpq' = q'$. From $q|q'p$ we conclude that $q|q'$, hence $q' = 0$, and q is therefore a constant polynomial, i.e., w.l.o.g. $a = p$. Comparing the degrees in x on the two sides of $1 = a' + 2ax$ now results in a contradiction. **q.e.d.**

Remarks 5.5 :

(a) Additional examples of meromorphic functions without elementary primitives, including $\sin z/z$, are treated on pp. 971-2 of [Ros_2]. The arguments are easy (but not always obvious) modifications of the proof of Corollary 5.4.

(b) One can (easily) produce an elementary differential field extension of the rational function field $\mathbb{R}(x)$ containing $\arctan x$ (we are assuming the standard derivative), but not one with no new constants. Indeed, it is not hard to show that $1/(x^2 + 1)$ cannot be written in the form (i) of the statement Theorem 5.2 (see p. 598 of [Ros_2]). This indicates the importance of the no new constant hypothesis in the statement of Liouville's Theorem.

References

[Hun] T.W. Hungerford, *Algebra*, GTM 73, Springer-Verlag, New York, 1974.

[Ros_1] M. Rosenlicht, Liouville's Theorem on Functions with Elementary Integrals, *Pac. J. Math.*, **24**, (1968), 153-161.

[Ros_2] M. Rosenlicht, Integration in Finite Terms, *Am. Math. Monthly*, **79**, (1972), 963-972.

[Ros_3] M. Rosenlicht, On Liouville's Theory of Elementary Functions, *Pac. J. Math.*, **65**, (1976), 485-492.

[Ste] I. Stewart, *Galois Theory*, 2^{nd}-edition, Chapman and Hall, London, 1989.

R.C. Churchill
Department of Mathematics
Hunter College and Graduate Center, CUNY
695 Park Avenue
New York, New York 10021, USA

Summer address:

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta T2N1N4, Canada

e-mail address (at all times):

rchurchi@math.hunter.cuny.edu