WIS-CS-204-74
COMPUTER SCIENCES DEPARTMENT
The University of Wisconsin
1210 West Dayton Street
Madison, Wisconsin 53706

Received January 11, 1974

A MULTIVARIATE LIOUVILLE THEOREM ON INTEGRATION INFINITE TERMS

by

B. F. Caviness and Michael Rothstein

Computer Sciences Technical Report No. 204

January 1974
A Multivariate Liouville Theorem
on
Integration in Finite Terms*

by
B. F. Caviness
and
Michael Rothstein

Computer Sciences Department
University of Wisconsin
Madison, Wisconsin 53706

December 1973

Abstract. A multivariate generalization of the Strong Liouville Theorem due to Risch is presented. The result is an abstract version of the following: Let $K$ be a subfield of the field of complex numbers. Let each $f_i(x_1,\ldots,x_n), 1 \leq i \leq n$, be any function in a field $E$ obtained by algebraic operations and the taking of logarithms and exponentials over $K(x_1,\ldots,x_n)$. If there exists a function $g$ obtained by algebraic operations and the taking of logarithms and exponentials of elements of $E$ such that

$$\nabla g = (\frac{\partial g}{\partial x_1}, \ldots, \frac{\partial g}{\partial x_n}) = (f_1, \ldots, f_n)$$

then $g$ must be of the form

$$d_0 + \sum c_i \log d_i$$
where $d_0$ is in $E$, the $c_i$ are constants in, and the $d_i$ are elements in $E(a)$ where $a$ is a constant algebraic over $E$.

*This research was supported in part by NSF Grant GJ-30125X.*
1. **Introduction**

The main result of this paper is a multivariate generalization of the Strong Liouville Theorem of Risch [5] on integration in finite terms. The motivation for this work comes from the authors' investigations into transcendental function algorithms, i.e., algorithms for symbolic computations with transcendental functions.

The main result can be roughly interpreted in the following way. Let $K$ be a subfield of the field of complex numbers and let each $f_i(x_1, \ldots, x_n)$, $1 \leq i \leq n$, be any function in a field $E$ obtained by algebraic operations and the taking of exponentials and logarithms over $K(x_1, \ldots, x_n)$, i.e., each $f_i$ is an elementary function. If there exists a function $g$ obtained by algebraic operations and the taking of exponentials and logarithms of elements of $E$ such that

$$g = (\partial g/\partial x_1, \ldots, \partial g/\partial x_n) = (f_1, \ldots, f_n)$$

then $g$ must be of the form

$$d_0 + \sum c_i \log d_i$$

where $d_0$ is in $E$, the $c_i$ are constants in, and the $d_i$ are elements in, $E(a)$ where $a$ is a constant algebraic over $E$.

Although the results are obtained in the abstract setting of differential rings and fields, all the arguments are quite simple and require only elementary concepts from algebra.

In section 2 some standard definitions from differential algebra are introduced. In section 3 some lemmas basic to the proof of the
main results are derived. These lemmas are primarily concerned with the behavior of derivatives of elements in a differential overring of a given differential ring.

Section 4 is devoted to the statement of some known results about differential fields and section 5 contains the main results of the paper.
2. **Differential Rings**

Let \( R \) be a commutative ring with unity and let \( D_1, \ldots, D_n \) be mappings from \( R \) to \( R \) with the properties that for any \( a, b \in R \) and for \( 1 \leq i, j \leq n \)

\[
D_i(a+b) = D_i(a) + D_i(b) \tag{1}
\]

\[
D_i(ab) = bD_i(a) + aD_i(b) \tag{2}
\]

and

\[
D_i(D_j(a)) = D_j(D_i(a)) \tag{3}
\]

\( R \) is called a **partial (ordinary) differential ring** if \( n > 1 \) (\( n = 1 \)) with derivation operators \( D_1, \ldots, D_n \).

For \( a \) in \( R \) and positive \( m \) in \( \mathbb{Z} \), the ring of rational integers, it follows by induction that

\[
D_i(a^m) = ma^{m-1}D_i(a), \quad 1 \leq i \leq n. \tag{4}
\]

If \( R \) is a field \( (4) \) holds for non-zero \( a \) in \( R \) and non-zero \( m \) in \( \mathbb{Z} \). Furthermore it follows from \( (4) \) that \( D_i1 = D_i1^2 = 2 \cdot 1 \cdot D_i1 \) and hence that \( D_i1 = 0 \). Thus if \( R \) is a field, \( a \) a non-zero member of \( R \) then \( (4) \) holds for all \( m \) in \( \mathbb{Z} \). If there exists \( b^{-1} \) in \( R \) such that \( bb^{-1} = 1 \), then for any \( a \) in \( R \)

\[
D_i(ab^{-1}) = [bD_i(a) - aD_i(b)](b^{-1})^2. \tag{5}
\]

The terminology **differential field** is used for a field \( F \) that satisfies \( (1) - (3) \).

Let \( S \) be a subring of the ring \( R \). We say that \( S \) is a **differential subring** of \( R \) or that \( R \) is a **differential overring**
of $S$ if $D_i S \subset S$ for $1 \leq i \leq n$. Let $C_i^{(R)} = \{ a \in R \text{ and } D_i(a) = 0 \}$ and let $C^{(R)} = \bigcap_{i=1}^{n} C_i^{(R)}$. It follows from (1) and (2) that $C_i^{(R)}$ and $C^{(R)}$ are differential subrings of $R$. They are called respectively the constant ring of $R$ with respect to the $i$-th variable and the constant ring of $R$. If $R$ is a field it follows from (5) that $C_i^{(R)}$ and $C^{(R)}$ are differential subfields of $R$. We have previously remarked that 1 is in $C^{(R)}$, and in case $R$ is a field, $C^{(R)}$ also contains the prime subfield of $R$.

Let $R$ and $S$ be differential rings with $n$ derivation operators $D_1, \ldots, D_n$ and $E_1, \ldots, E_n$ respectively. Let $\sigma$ be a homomorphism from $R$ to $S$ with the additional property that $\sigma(D_i(a)) = E_i(\sigma(a))$ for all $a$ in $R$ and for $1 \leq i \leq n$. Such a homomorphism is called a differential homomorphism. The concepts of differential isomorphism, differential automorphism and differential embedding can be defined similarly.

Let $a_1, \ldots, a_m$ be elements of the differential ring $R$ and let $n_1, \ldots, n_m$ be in $\mathbb{Z}^+$, the set of positive rational integers. For any derivation operator $D$ on $R$, it follows from (4) and induction on $m$ that

$$D\left(\prod_{i=1}^{m} a_i^{n_i}\right) = \sum_{j=1}^{m} (n_j a_j^{n_j} - 1) \prod_{i \neq j} a_i^{n_i} D a_j.$$  \hspace{1cm} (6)

If $R$ is a field and each $a_i$ is non-zero, (6) may be written

$$\frac{D\left(\prod_{i=1}^{m} a_i^{n_i}\right)}{\prod_{i=1}^{m} a_i^{n_i}} = \sum_{j=1}^{m} n_j \frac{D a_j}{a_j}. \hspace{1cm} (6')$$
In fact (6') holds when each \( n_i \) is in \( Z \). (6) and (6') will be called the logarithmic derivative identity.

The intersection of any family of differential subrings of the differential ring \( R \) is a differential subring of \( R \). If \( S \) is a differential subring of \( R \) and \( \rho \) is a subset of \( R \), there exists a smallest differential subring of \( R \) that contains both \( S \) and \( \rho \) and is called the differential subring generated by \( \rho \) over \( S \) and is denoted by \( S[\rho] \). \( \rho \) is called the set of generators for the ring \( S[\rho] \) over \( S \). A differential overring of a differential ring \( S \) is said to be finitely generated over \( S \) if it has a finite set of generators over \( S \). If \( S \) and \( R \) are differential fields, the smallest differential field containing \( S \) and \( \rho \) will be denoted by \( S<\rho> \).
3. Elementary Overrings of Differential Rings

Throughout this section \( S \) is assumed to be a differential subring of the differential ring \( R \) with derivation operators \( D_1, \ldots, D_n \). We also assume that the characteristic of \( R \) is zero which implies that \( C(S) \) contains a subring isomorphic to \( Z \).

Let us consider \( R^n = \{(a_1, \ldots, a_n) : a_i \text{ is in } R \text{ for } 1 \leq i \leq n\} \). \( R^n \) is a commutative ring with identity when addition and multiplication are inherited in a component-wise manner from \( R \). In fact \( R^n \) is a differential ring with derivation operators \( D_1, \ldots, D_n \) inherited component-wise from \( R \), i.e., \( D_i(a_1, \ldots, a_n) = (D_1a_1, \ldots, D_na_n) \). \( R^n \) contains a subring \( \hat{R} = \{(a_1, \ldots, a_n) : a_i = a_j \text{ for } 1 \leq i, j \leq n\} \) and \( \hat{R} \) is differentially isomorphic to \( R \). It will be convenient to abuse the language and not distinguish between \( R \) and \( \hat{R} \). In a similar fashion \( S \) may be considered as a differential subring of \( R^n \). The constant ring of \( R^n \) is just \((C(R))^n\).

We now introduce a new derivation operator \( \nabla \) on \( R^n \), called the gradient operator, defined by \( \nabla(a_1, \ldots, a_n) = (D_1a_1, \ldots, D_na_n) \) for all \( (a_1, \ldots, a_n) \) in \( R^n \). It is a trivial matter to verify that \( \nabla \) satisfies (1) and (2) on \( R^n \) and that \( \nabla D_i = D_i \nabla \) for \( 1 \leq i \leq n \).

Hence \( R^n \) is a differential ring with derivation operators \( \nabla \), \( D_1, \ldots, D_n \). With these derivation operators the constant ring remains \((C(R))^n\). However \( R \) and \( S \) are no longer necessarily differential subrings of \( R^n \) since they may not be closed under \( \nabla \).

The constants of \( R \) may be characterized in terms of \( \nabla \), namely for \( a \) in \( R \), \( a \) is in \( C(R) \) if and only if \( \nabla a = 0 \). Also for \( a, b \) in \( R \) and \( c_1 \) in \( C(R) \), \( c_1 \nabla a = \nabla b \) if and only if \( c_1a = b + c_2 \) where
\(c_2\) is in \(\mathcal{C}(\mathcal{R})\). This is true simply because \(\forall(c_1a-b) = 0\). We also need to know the relationship between \(a\) and \(b\) when there exists \(m\) in \(\mathbb{Z}^+\) and \(d\) in \(\mathcal{R}^n\) such that \(\forall a = ad\) and \(\forall b = mbd\).

**Lemma 1.** Let \(a, b\) be members of the differential ring \(\mathcal{R}\) as defined above, let \(d\) be in \(\mathcal{R}^n\) and let \(m\) be in \(\mathbb{Z}^+\). If \(\forall a = ad\) and \(\forall b = -mbd\) then \(a^m = c\) for \(c\) in \(\mathcal{C}(\mathcal{R})\). If \(\mathcal{R}\) is an integral domain, \(\forall a = ad\) and \(\forall b = mbd\) then \(a^m = cb\) for \(c\) in \(\mathcal{C}(\mathcal{F})\) where \(\mathcal{F}\) is the quotient field of \(\mathcal{R}\).

**Proof.** If either \(a\) or \(b\) is zero both conclusions may be trivially satisfied by choosing \(c = 0\). So assume \(a\) and \(b\) are non-zero. \(\forall a = ad\) and \(\forall b = -mbd\) implies that \(\forall(a^m b) = 0\) and the first conclusion follows. In the case \(\forall a = ad\) and \(\forall b = mbd\) we have that \(b\forall a^m - a^m \forall b = 0\) and passing to the quotient field of \(\mathcal{R}\), \(\forall(a^m b^{-1}) = 0\), i.e., \(a^m b^{-1} = c\) in \(\mathcal{C}(\mathcal{F})\). □

Suppose that \(a\) is in \(\mathcal{R}\). \(a\) is said to be **primitive** over \(\mathcal{S}\) if \(\forall a\) is in \(\mathcal{S}^n\). If there exists a non-zero \(b\) in \(\mathcal{S}\) such that \(b\forall a = \forall b\) then \(a\) is called a **logarithm** over \(\mathcal{S}\). If \(\mathcal{S}\) is a field, a logarithm over \(\mathcal{S}\) is also primitive over \(\mathcal{S}\). If there exists \(b\) in \(\mathcal{S}\) such that \(\forall a = a\forall b\), \(a\) is called **exponential** over \(\mathcal{S}\). If \(a\) is algebraic, logarithmic or exponential over \(\mathcal{S}\), \(a\) is said to be **simple elementary** over \(\mathcal{S}\). Let \(\mathcal{T}\) be an intermediate ring between \(\mathcal{S}\) and \(\mathcal{R}\), i.e., \(\mathcal{S} \subseteq \mathcal{T} \subseteq \mathcal{R}\). Then \(a\) in \(\mathcal{T}\) and \(\mathcal{T}\) are said to be **elementary** over \(\mathcal{S}\) if \(\mathcal{T} = \mathcal{S}(\alpha_1, \ldots, \alpha_m)\) where each \(\alpha_i\) is simple elementary over \(\mathcal{S}(\alpha_1, \ldots, \alpha_{i-1})\). If \(\mathcal{T}\) is elementary over \(\mathcal{S}\) and \(\mathcal{C}(\mathcal{T}) = \mathcal{C}(\mathcal{S})\) then \(a\) and \(\mathcal{T}\) are said to be **regular elementary** over \(\mathcal{S}\).
Let $a$ be transcendental over $S^n$. We want to consider the ring of polynomials $S^n[a]$. First of all note that $a$ is transcendental over $S^n$ if and only if $a$ is transcendental over $S$. Clearly transcendence over $S^n$ implies transcendence over $S$ since $S^n = S$. Suppose $a$ is transcendental over $S$ and there exist $s_j$ in $S^n$ such that

$$\sum_{j=0}^{k} s_j a^j = 0 .$$

(7)

Let $s_j = (s_{j1}, \ldots, s_{jn})$, then (7) implies that

$$\sum_{j=0}^{k} s_{ji} a^j = 0 \text{ for } 1 \leq i \leq n .$$

But since $a$ is transcendental over $S$, $s_{ji} = 0$ for $1 \leq i \leq n$, $0 \leq j < k$, which implies that $s_j = 0$ for $0 \leq j < k$ and that $a$ is transcendental over $S^n$.

For the proof of the next lemma we need to know that the additive group of $S$ is torsion free, that is, that if $a$ is a non-zero element of $S$ and $m$ is a non-zero integer in $Z$, then $ma \neq 0$.

**Lemma 2.** Suppose that the additive group of $S$ is torsion free. Let $a$ in $R$ be transcendental over $S$ and let $P(a) = \sum_{i=0}^{k} p_i a^i$ be a member of $S[a]$ of degree $k > 0$. If $a$ is primitive over $S$ and $c(S) = c(R)$ then the degree of $VP(a)$ is $k$ or $k-1$ (in $S^n[a]$).

If the degree of $VP(a) = k-1$ then $p_k$ is in $c(S)$.

**Proof.** $VP(a) = \sum_{i=0}^{k} (VP_i a^i + ip_i a^{i-1} Va)$

$$= VP_k a^k + \sum_{i=0}^{k-1} (VP_i + (i+1)p_{i+1} Va) a^i .$$

(8)

If $VP_k = 0$ then $VP_{k-1} + kp_k Va \neq 0$ for otherwise $VP_{k-1} = -kp_k Va$.
which implies that \( p_{k-1} = -kp_k a + c \) where \( c \) is in \( C(S) \). Since the additive group of \( S \) is torsion free \(-kp_k \neq 0\) and hence \( a \) is not transcendental over \( S \) which is a contradiction. \( \square \)

**Lemma 3.** Let \( a \) in \( R \) be transcendental over \( S \) and let \( P(a) \) be a non-zero member of \( S[a] \) of degree \( k \). If \( a \) is exponential over \( S \), and \( C(S) = C(R) \) then the degree of \( \nabla P(a) \) is \( k \).

**Proof.** If \( k = 0 \) the result is trivially true, so assume \( k > 1 \). Since \( a \) is exponential over \( S \) there exists \( b \) in \( S \) such that \( \forall a = a \forall b \). Thus from (8) we have that

\[
\nabla P(a) = \sum_{i=0}^{k} (\nabla p_i + \nabla p_i \forall b) a^i.
\]

If \( \nabla p_k + kp_k b = 0 \) then \( \nabla p_k = -kp_k \forall b \) which by lemma 1 implies that \( p_k a^k = c \) where \( c \) is in \( C(S) \). The last implication contradicts the transcendence of \( a \) and hence the degree of \( \nabla P(a) \) is \( k \). \( \square \)

**Lemma 4.** Let \( R \) be an integral domain. Denote the quotient fields of \( R \) and \( S \) by \( E \) and \( F \) respectively and assume that \( C(E) = C(F) \).

Suppose that \( a \) in \( R \) is transcendental over \( S \) and is either primitive or exponential over \( S \). Let \( P \) be a member of \( S[a] \) with degree of \( P = k > 0 \). If \( P|\nabla P \) (in \( S^n[a] \)) then \( a \) is exponential and \( P = pa^k \) where \( p \) is in \( S \).

**Proof.** If \( P|\nabla P \) then degree \( P = \) degree \( \nabla P \) and there exists \( d \) in \( S^n \) such that \( \nabla P = dP \). Suppose \( P = \sum_{i=0}^{k} p_i a^i \).

If \( a \) is primitive it must be the case that \( \nabla p_k \neq 0 \) and
comparing leading coefficients of $\nabla P$ and $dP$ we have that $p_k d = \nabla p_k$. Thus $p_k \nabla P - P \nabla p_k = 0$ and $\nabla (P p_k^{-1}) = 0$. Hence $P = c p_k$ where $c$ is in $C(E) = C(F)$ which contradicts the transcendence of $a$ over $S$. Thus $a$ is not primitive.

Suppose $a$ is exponential, i.e., there exists $b$ in $S$ such that $a = a \nabla b$. It follows from comparing coefficients of $\nabla P$ and $dP$ that $d p_i = \nabla p_i + i p_i \nabla b$ for $0 \leq i < k$. If there exists $j < k$ such that $p_j \neq 0$ (otherwise the desired result holds) then $d p_j = \nabla p_j + j p_j \nabla b$. Thus $d p_k p_j = p_j (\nabla p_k \nabla b) = p_k (\nabla p_j + j p_j \nabla b)$ which implies that $p_j \nabla p_k - p_k \nabla p_j = (j-k) p_k p_j \nabla b$ or equivalently that $\nabla (p_k p_j^{-1}) = (j-k) p_k p_j^{-k-1} \nabla b$. By lemma 1 $a^{k-j} = c p_k p_j^{-k}$ where $c$ is in $C(R) = C(S)$ and hence $a$ is not transcendental over $S$ which is contrary to the hypotheses. We must conclude that $p_i = 0$ for $0 \leq i < k$. \[\]

Suppose $a$ in $R$ is transcendental over $S$ and that $P$ is in $S^n[a]$. $P$ is called square-free if there does not exist $Q$ in $S^n[a]$ with degree $Q > 0$ such that $Q^2 \mid P$.

**Lemma 5.** Let $R$, $S$, $E$, $F$ and $a$ be as in lemma 4. Let $P$, $Q$ be relatively prime members of $S[a]$ with degree of $Q > 0$. Let $\tilde{P}$, $\tilde{Q}$ be relatively prime members of $S^n[a]$ such that $\tilde{P}/\tilde{Q} = \nabla (P/Q)$. \tilde{Q} is square-free if and only if $a$ is exponential over $S$ and $Q = sa$ where $s$ is in $S$.

**Proof.** If $a$ is exponential and $Q = sa$ it is easy to verify that $\tilde{Q}$ is square-free. So suppose that $\tilde{Q}$ is square-free. Then

$$\nabla (P/Q) = (Q \nabla P - P \nabla Q)/Q^2 = \tilde{P}/\tilde{Q}.$$
Thus
\[
\tilde{P}Q^2 = \tilde{Q}(Q\tilde{V}P-P\tilde{V}Q) .
\]
Since \( \tilde{Q} \) is square-free \( \tilde{Q}|(Q\tilde{V}P-P\tilde{V}Q) \) which implies that \( Q|\tilde{V}Q \) which implies by lemma 4 that \( a \) is exponential and \( Q = sa^m \), \( s \neq 0 \) in \( S \). Now it is necessary to show that \( m = 1 \).

Suppose \( \forall a = a\forall b \) where \( b \) is in \( S \). If \( P = \sum_{i=0}^{k} p_i a_i \) where \( p_i \) is in \( S \), then \( P/Q = s^{-1}P/a^m \). Let \( s^{-1}P = \hat{P} = \sum_{i=0}^{k} \hat{p}_i a_i \). Then \( \forall (P/a^m) = \hat{P}/\hat{Q} \) implies that \( a^m \hat{P} = \hat{Q}(\forall\hat{V}P-m\forall b\hat{P}) \). If \( m > 1 \), \( a|(\forall\hat{V}P-m\forall b\hat{P}) \) which implies that \( \forall\hat{P}_0 - m\forall b\hat{P}_0 = 0 \). Thus by lemma 1 \( a^m = c\hat{P}_0 \) where \( c \) is in \( \mathcal{C}(F) = \mathcal{C}(E) \). But this contradicts the transcendence of \( a \) and hence we must conclude that \( m = 1 \). \( \square \)
4. **Differential Fields**

Throughout this section we assume that $F$ is a differential field of characteristic zero with $n$ derivation operators $D_1, \ldots, D_n$. This section contains well-known results that are needed later.

Let $U$ be a differential extension field of $F$ (i.e., a differential overring that is a field) with the property that any finitely generated differential extension of $F$ can be differentially embedded in $U$. We call $U$ a **universal extension** of $F$. Kolchin proves [2, p. 92] that every differential field of characteristic zero has a universal extension. (Kolchin calls such extensions semiuniversal fields and reserves the terminology universal field for a stronger concept.)

The following lemma is taken from Kaplansky [1, p. 33].

**Lemma 6.** Let $U$ be a universal extension of $F$. Let $\{f_i\}_{1 \leq i \leq m}$ and $g$ be members of $F[x_1, \ldots, x_r]$. If there exist $c_1, \ldots, c_r$ in $C(U)$ such that $f_i(c_1, \ldots, c_r) = 0$ for $1 \leq i \leq m$ and $g(c_1, \ldots, c_r) \neq 0$ then there exist $k_1, \ldots, k_r$ in $\overline{C}(F)$, the algebraic closure of $C(F)$, such that $f_i(k_1, \ldots, k_r) = 0$ for $1 \leq i \leq m$ and $g(k_1, \ldots, k_r) \neq 0$.

**Lemma 7.** Let $G = F(a)$ be an algebraic extension field of the field $F$. Let $R = \sum_{j=0}^{m} r_j a_j$ be the monic, irreducible polynomial of minimal degree over $F$ that is satisfied by $a$. Let $P(a) = \sum_{j=0}^{k} p_j a_j$ be an arbitrary member of $G$, i.e., $P$ is a polynomial over $F$ with $k < m$. Then each of the derivation operators $D_i$, $1 \leq i \leq n$, may be uniquely extended to $G$ to give $G$ a differential
structure compatible with $F$ by defining

$$D_i P(a) = \sum_{j=0}^k (D_i p_j) a^j + (\sum_{j=0}^{k-1} (j+1)p_{j+1} a^j) D_1 a$$

(9)

where

$$D_1 a = \left( -\sum_{j=0}^m (D_1 r_j) a^j \right) / \left( \sum_{j=0}^{m-1} (j+1)r_{j+1} a^j \right).$$

(10)

The proof of Rosenlicht [6, p. 965-6] for ordinary differential fields can be easily generalized to partial differential fields.

We want to observe that for any arbitrary $\sigma$ in the Galois group of automorphisms of $G$ relative to $F$ that $\sigma(D_i a) = D_i (\sigma a)$ for $1 \leq i \leq n$ and for $a$ in $G$. This fact follows in a straightforward way from (9) and (10).

It is an immediate corollary of lemma 7 that when $a$ is algebraic over $F$, $F\langle a \rangle = F(a)$. 
5. **Multivariate Liouville Theorems**

The main results of the paper are presented in this section. Throughout this section \( F \) will denote a differential field of characteristic zero with \( n \) derivation operators \( D_1, \ldots, D_n \). \( U \) will be a universal extension of \( F \). The subfield \( G \) of \( U \) will normally denote a differential extension field of \( F \) which is either elementary or regular elementary over \( F \). As in section 3 we will introduce \( G^n \), \( F^n \) and the derivation operator \( \nabla \). Using the natural (differential) embedding as before, we will consider \( G \) and \( F \) as subfields of \( G^n \).

Now we present a multivariate generalization of the Ostrowski generalization [4] of a theorem originally published by Joseph Liouville [3]. Other proofs of the Ostrowski generalization have been given by Risch [5] and Rosenlicht [6, 7].

**Weak Liouville Theorem.** Let \( G \) be a differential field that is regular elementary over the differential field \( F \). Let \( a \) be in \( F^n \). If there exists \( b \) in \( G \) such that \( \nabla b = a \), then there exist constants \( c_1, \ldots, c_m \) in \( F \) and elements \( d_0, d_1, \ldots, d_m \) in \( F \) such that

\[
a = \nabla d_0 + \sum_{i=1}^{m} c_i \nabla d_i/d_i.
\]

**Proof.** Since \( G \) is regular elementary over \( F \), there exist \( t_1, \ldots, t_k \) in \( G \) such that \( G = F \langle t_1, \ldots, t_k \rangle \) and each \( t_i \) is simple elementary over \( F \langle t_1, \ldots, t_{i-1} \rangle \). Furthermore \( C(G) = C(F) \).

The proof is by induction on \( k \). If \( k = 0 \) the result is trivial since \( G = F \) and one may choose \( c_i = 0 \), \( 1 \leq i \leq m \), and
\[ d_0 = b. \] So assume that \( k > 0 \) and that the desired result holds for \( k - 1 \). By the induction hypothesis we have that

\[
a = \nabla \delta_0 + \sum_{i=1}^{m} \gamma_i \nabla \delta_i / \delta_i
\]

where \( \delta_i, 0 \leq i \leq m, \) is in \( F_1 = F(t_1) \) and \( \gamma_i, 1 \leq i \leq m, \) is in \( \mathcal{C}(F_1) = \mathcal{C}(F) \).

It is necessary to show that \( a \) can be written in the form (11) where the \( \delta_i \)'s are in \( F \). We have three cases to consider, namely (1) when \( t_1 \) is algebraic over \( F \), (2) when \( t_1 \) is a logarithm over \( F \) and (3) when \( t_1 \) is an exponential over \( F \).

First assume that \( t_1 \) is algebraic over \( F \). Let \( \sigma_1, \ldots, \sigma_l \) denote the elements of the Galois group of automorphisms of the normal field belonging to \( F_1 \) relative to \( F \). Since \( \sigma_i D_j \delta = D_j \sigma_i \delta \) for all \( \delta \) in \( F_1 \), it follows that \( \sigma_i \nabla \delta = \nabla \sigma_i \delta \) for all \( \delta \) in \( F_1 \). Applying \( \text{Tr} = \sum_{i=1}^{m} \sigma_i \) to (11) we obtain

\[
\lambda a = \nabla \text{Tr}(\delta_0) + \sum_{i=1}^{m} \gamma_i \sum_{j=1}^{l} \nabla \sigma_j(\delta_i) / \sigma_i(\delta_i).
\]

Applying the logarithmic derivative identity to (12) we obtain

\[
a = \nabla d_0 + \sum_{i=1}^{m} \gamma_i \nabla d_i / d_i
\]

where \( d_0 = \text{Tr}(\delta_0)/\ell \) and \( d_i = \prod_{j=1}^{l} \sigma_j(\delta_i) = \text{norm}(\delta_i) \) for \( 1 \leq i \leq m \). Of course \( \text{Tr}(\delta_0) \) and \( \text{norm}(\delta_1), 1 \leq i \leq l \), are in \( F \) as required.

Now assume that \( t_1 \) is either a logarithm or an exponential over \( F \). Since the case where \( t_1 \) is algebraic over \( F \) has already been considered, we may assume that \( t_1 \) is transcendental.
over \( F \). Each \( \delta_i, 0 \leq i \leq m \), in (11) is a rational function in \( t_1 \) over \( F \). Each \( \delta_i, 0 \leq i \leq m \), can be written as a power product of a non-zero element of \( F \) and monic, irreducible polynomials in \( t_1 \) over \( F \). Then using the logarithmic derivation identity

\[
\sum_{i=1}^{m} \gamma_i \delta_i / \delta_i
\]

may be rewritten in a similar form with each \( \delta_i \) either a member of \( F \) or a monic, irreducible polynomial in \( t_1 \) over \( F \). Thus we assume that each \( \delta_i, 1 \leq i \leq m \), is a distinct element of \( F \) or a distinct monic, irreducible member of \( F[t_1] \).

Furthermore we may assume that each \( \gamma_i \neq 0 \).

Now multiply (11) by \( P = \prod_{i=1}^{m} \delta_i \) to obtain

\[
aP = P \delta_0 + \sum_{j=1}^{m} \gamma_j \delta_j \prod_{i \neq j} \delta_i.
\]

(13)

Thus \( P \delta_0 \) is a member of \( F^n[t_1] \). But by lemma 5 this is possible only if either \( \delta_0 \) is in \( F[t_1] \) with \( t_1 \) logarithmic over \( F \) or \( t_1 \delta_0 \) is in \( F[t_1] \) with \( t_1 \) exponential over \( F \).

Now it is convenient to divide the argument into the case when \( t_1 \) is logarithmic over \( F \) and the case when \( t_1 \) is exponential over \( F \). First suppose \( t_1 \) is logarithmic over \( F \), i.e.,

\[
\forall t_1 = \forall e/e \text{ where } e \text{ is in } F.
\]

Since \( \delta_0 \) is in \( F[t_1] \), \( \forall \delta_0 \) is also in \( F[t_1] \). Thus for each \( j = 1, 2, \ldots, m \) (13) implies that \( \delta_j | \forall \delta_j \) in \( F^n[t_1] \). But this is impossible unless \( \delta_j \) is in \( F \). Thus each \( \delta_j \) for \( 1 \leq j \leq m \) must be in \( F \). But then (13) implies that \( \forall \delta_0 \) is in \( F^n \). If \( \forall \delta_0 \) is in \( F^n \) then lemma 2 implies that either \( \delta_0 \) is in \( F \) or \( \delta_0 = \gamma_0 t_1 + d_0 \) where \( \gamma_0 \) is in \( C(F) \). Now we have shown that (11) has the desired form when \( t_1 \) is logarithmic over \( F \), i.e.,

\[
a = \forall d_0 + \gamma_0 \forall e/e + \sum_{i=1}^{m} \gamma_i \delta_i / \delta_i.
\]
Suppose that $t_1$ is exponential over $F$, i.e., $\forall t_1 = t_1^e$ where $e$ is in $F$. (13) implies that $\delta_i | \forall \delta_i$ for $1 \leq i \leq m$. Thus by lemma 4 $\delta_i$ is in $F$ except for possibly one $\delta_i$, say $\delta_1$, in which case we must have $\delta_1 = t_1$. Hence

$$a = \forall \delta_0 + \gamma_1 \forall e + \sum_{i=2}^{m} \gamma_i \forall \delta_i / \delta_1.$$  \hfill (14)

(14) implies that $\forall \delta_0$ is in $F^n$. Now $\delta_0$ must either be a polynomial or a rational function in $t_1$. If $\delta_0$ is a polynomial, lemma 3 implies that $\delta_0$ must actually be in $F$ since $\forall \delta_0$ is in $F^n$. If $\delta_0$ is not a polynomial we have shown that it must be of the form $Q/t_1$ where $Q = \sum_{i=0}^{k} q_i t_1^i$ is in $F[t_1]$. Since $\forall \delta_0$ is in $F^n$, $t_1 | (\forall Q - Q \forall e)$ which implies that $\forall q_0 - q_0 \forall e = 0$. Thus by lemma 1, $q_0 = ct_1$ where $c$ is in $C(F)$ thus contradicting the transcendence of $t_1$ over $F$. Hence $\delta_0$ must be in $F$. Now $a = \forall (\delta_0 + \gamma_1 e) + \sum_{i=2}^{m} \gamma_i \forall \delta_i / \delta_1$ is in the desired form. 

The condition that $G$ be regular over $F$ can be removed for the multivariate case just as Risch [5, p. 171] did for the univariate case. The proof is similar to the univariate case and is sketched here.

**Strong Liouville Theorem.** Let $G$ be a differential field that is elementary over the differential field $F$. Let $a$ be in $F^n$; if there exists $b$ in $G$ such that $\forall b = a$, then there exist a constant $k$ algebraic over $C(F)$, constants $c_1, \ldots, c_m$ and elements $d_1, \ldots, d_m$ in $F(k)$ and $d_0$ in $F$ such that

$$a = \forall d_0 + \sum_{i=1}^{m} c_i \forall d_i / d_i.$$

**Proof.** Since $G$ is elementary over $F$, there exist $t_1, \ldots, t_k$ in $G$ such that $G = F<t_1, \ldots, t_k>$. If $t_i$ is transcendental over $F_{i-1} = F<t_1, \ldots, t_{i-1}>$ and $F_i = F_{i-1} < t_i >$ is not regular over $F_{i-1}$ then there
exists a constant $c$ in $\mathbb{C}(F_i)$ such that $t_i$ is algebraic over $F_{i-1}(c)$. This follows since $F_i$ not regular over $F_{i-1}$ implies that there exists a constant $c$ in $F_i - F_{i-1}$, i.e., $c = R(t_i)$ where $R$ is a rational function over $F_{i-1}$ which implies that $t_i$ is algebraic over $F_{i-1}(c)$.

Hence it follows that since $b$ is elementary over $F$ there exist constants $y_1, \ldots, y_\ell$ such that $b$ is regular elementary over $F(y_1, \ldots, y_\ell)$. Now we can apply the weak Liouville theorem to obtain polynomials $P_0, \ldots, P_m, Q$ in $y_1, \ldots, y_\ell$ over $F$ and polynomials $r_1, \ldots, r_m, s_1, \ldots, s_m$ in $y_1, \ldots, y_\ell$ over $\mathbb{C}(F)$ such that

$$a = (Q\sqrt{P_0} - P_0 \sqrt{Q})/Q^2 + \sum_{i=1}^m \left( r_i/s_i \right) (\sqrt{P_i}/P_i). \quad (14)$$

Note that it is sufficient to consider the $P_i$, $1 \leq i \leq m$, as polynomials instead of rational functions for if they were rational functions they could be reduced to polynomials by employing the logarithmic derivation identity.

The relation (14) may be written as

$$\bar{p}(y_1, \ldots, y_\ell)/Q(y_1, \ldots, y_\ell) = 0$$

with

$$\bar{Q} = Q^2 \prod_{i=1}^m s_i P_i \neq 0$$

and

$$\bar{p} = (Q\sqrt{P_0} - P_0 \sqrt{Q}) (\bar{Q}/Q^2) + \bar{Q} \sum_{i=1}^m \left( r_i/s_i \right) (\sqrt{P_i}/P_i) - a\bar{Q} = 0$$
Now $\tilde{Q}$ is in $F[y_1,\ldots,y_\ell]$ and $\tilde{P}$ is in $F^n[y_1,\ldots,y_\ell]$.

Suppose $\tilde{P} = (\tilde{P}_1,\ldots,\tilde{P}_n)$ where each $\tilde{P}_i$ is in $F[y_1,\ldots,y_\ell]$.

Now apply lemma 6 to obtain $k_1,\ldots,k_\ell$ algebraic over $C(F)$ such that $\tilde{P}_i(k_1,\ldots,k_\ell) = 0$ and $Q(k_1,\ldots,k_\ell) \neq 0$.

Let $k$ be algebraic over $C(F)$ such that (i) $C(F)(k)$ is a Galois extension of $C(F)$, (ii) $C(F)(k)$ contains $k_1,\ldots,k_\ell$ and (iii) $C(F)(k)$ is the smallest field satisfying (i) and (ii).

Backtracking we obtain

$$a = \frac{Q(k_1,\ldots,k_\ell)}{Q(k_1,\ldots,k_\ell)} + \sum_{i=1}^m \frac{r_i(k_1,\ldots,k_\ell) \tilde{P}_i(k_1,\ldots,k_\ell)}{s_i(k_1,\ldots,k_\ell) \tilde{P}_i(k_1,\ldots,k_\ell)}$$

(15)

Apply the trace function associated with the Galois group of $F(k)$ over $F$ to (15) and then divide by $[F(k):F]$ to obtain the desired result. For example if $[F(k):F] = 2$ and $\sigma_1$ and $\sigma_2$ are the two automorphisms in the Galois group we have that

$$a = 1/2\text{Tr}(P_0/Q) + 1/2 \sum_{i=1}^m \left[ \sigma_1(r_i/s_i) \frac{\sigma_1\tilde{P}_i}{\tilde{P}_i} + \sigma_2(r_i/s_i) \frac{\sigma_2\tilde{P}_i}{\tilde{P}_i} \right].$$

Note the following condition that is necessary for the existence of $b$ in the Liouville theorems. Call $a = (a_1,\ldots,a_n)$ in $F^n$ exact if $D_ia_j = D_ia_j$ for $1 \leq i, j \leq n$. If there exists $b$ such that $\forall b = a$, $a$ must be exact since $D_j(D_i b) = D_i(D_j b)$ implies that $D_j a_i = D_i a_j$.

Acknowledgement

The authors have benefited from numerous discussions with H. I. Epstein. In particular the formulation and proof of lemma 5 are due to him.
REFERENCES


A multivariate generalization of the Strong Liouville Theorem due to Risch is presented. The main result may be roughly stated as follows: Let $f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)$ be members of an elementary function field $F$. Let $G$ be a finitely generated, elementary extension of $F$. That is, $G$ is obtained by adjoining a finite number of elements to $F$ that are obtained by algebraic operations and the taking of logarithms and exponentials. If there exists $g(x_1, \ldots, x_n)$ in $G$ such that the gradient of $g$ is $(f_1, f_2, \ldots, f_n)$, then $g$ must be the sum of an element in $F$ and a linear sum of logarithms where the constant coefficients and the arguments of the logarithms in the linear sum belong to the field $(a)$ where $a$ is a constant that is algebraic over $F$. 

**Key Words and Document Analysis**

- indefinite integration
- antidifferentiation
- potential function
- integration in finite terms
- differential rings
- elementary multivariate functions