Dissertação apresentada para obtenção do título de Mestre em Matemática pelo
Instituto Nacional de Matemática Pura e Aplicada

# O Teorema de Liouville sobre Integrais Elementares

por

Débora Rampanelli

Orientador: Luiz Henrique de Figueiredo

Rio de Janeiro
23 de novembro de 2009

# O TEOREMA DE LIOUVILLE SOBRE INTEGRAIS ELEMENTARES

DÉBORA RAMPANELLI

## CONTEÚDO


1. Introdução 1
2. Fundamentos Algébricos 3
3. O Teorema de Liouville 6
4. Liouville Racional 9
5. Apêndice 12

Referências 16


## 1. INTRODUÇÃO

Liouville provou que certas integrais não podem ser expressas em termos elementares. Neste trabalho apresentaremos uma demonstração puramente algébrica, devida a Rosenlicht [4], dessa impossibilidade para $\int e^{-x^2}\,dx$. Essa integral possui importante papel na Teoria da Probabilidade, na forma da *função erro*:

$$\operatorname{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-u^2}\,du.$$

Informalmente falando, por "termos elementares", nos referimos a funções construídas a partir de funções racionais, juntamente com repetidas operações algébricas (isto é, resolvendo equações polinomiais cujos coeficientes são funções elementares previamente definidas), além de aplicações de exponenciais, logaritmos, funções trigonométricas e suas inversas. Veremos uma definição algébrica de funções elementares na seção 2.

O resultado em questão é consequência direta do seguinte resultado geral:

**Teorema 1.** *Seja* $g$ *um polinômio. Se* $\int e^g$ *é elementar, então* $\operatorname{grau}(g) \leq 1$.

Por sua vez, esse teorema é obtido a partir de versões restritas do teorema de Liouville:

**Teorema 2** (Liouville Polinomial)**.** *Sejam* $f$ *e* $g$ *polinômios. Se* $\int fe^g$ *é elementar, então* $\int fe^g = Pe^g$*, onde* $P$ *é um polinômio.*

**Teorema 3** (Liouville Racional)**.** *Sejam* $f$ *e* $g$ *funções racionais, com* $g$ *não constante. Se* $\int fe^g$ *é elementar, então* $\int fe^g = Re^g$*, onde* $R$ *é uma função racional.*

*Prova do teorema 1.* Pelo teorema 2, com $f = 1$, temos que $\int e^g = Pe^g$, com $P$ um polinômio.

Derivando ambos os lados, temos:

$$e^g = P'e^g + Pg'e^g$$

Cancelando $e^g$:

$$1 = P' + Pg'$$

Se $\text{grau}(g) > 1$, teríamos $\text{grau}(g') \geq 1$ e portanto $0 = \text{grau}(1) = \text{grau}(P' + Pg') = \text{grau}(Pg')$, pois $\text{grau}(P) > \text{grau}(P')$. Assim, $Pg'$ é constante e $g'$ também. Mas isso implica $\text{grau}(g') = 0$ ou $g' = 0$, uma contradição. Portanto $\text{grau}(g) \leq 1$. □

O teorema 3 será provado na seção 4, a partir do teorema de Liouville, que está enunciado no teorema 4 e será provado na seção 3. Provaremos agora o Liouville Polinomial supondo válido o Liouville Racional.

*Prova do teorema 2.* Sejam $f$ e $g$ polinômios tais que $\int fe^g$ é elementar. Como polinômios são também funções racionais, o teorema 3 diz que $\int fe^g = Re^g$, onde $R$ é uma função racional.

Derivando ambos os lados, temos:

$$fe^g = R'e^g + Rg'e^g$$

Cancelando $e^g$:

$$f = R' + Rg'$$

Escrevendo $R = \frac{P}{Q}$ com $P$ e $Q$ polinômios relativamente primos e $Q$ mônico, temos:

$$f = \frac{P'Q - PQ'}{Q^2} + \frac{P}{Q}g'$$

e portanto

$$Q^2 f = P'Q - PQ' + PQg'$$

donde

$$Q(Qf - P' - Pg') = -PQ'$$

Como esta é uma equação envolvendo apenas polinômios e $P$ e $Q$ são relativamente primos, concluímos que $Q$ divide $Q'$ e portanto $Q = 1$ (pois $Q$ é mônico). Logo $R = P$ e $R$ é um polinômio. □

O teorema 3 é consequência do teorema de Liouville:

**Teorema 4** (Liouville)**.** *Seja* $h$ *uma função em algum corpo de funções* $F$*. Se* $h$ *tem uma integral elementar sobre* $F$*, então sua integral é da forma*

$$\int h = v + \sum_{i=1}^{n} \alpha_i \log(u_i),$$

*onde* $\alpha_1, \ldots, \alpha_n$ *são constantes e* $u_1, \ldots, u_n, v$ *são funções em* $F$*.*

O enunciado desse teorema será apresentado com precisão na seção 3, onde o provaremos de forma algébrica. Os conceitos e resultados necessários para essa formulação serão explicados na seção 2.

## 2. Fundamentos Algébricos

**Definição 1** (derivação)**.** *Seja* $F$ *um corpo. Uma* derivação *em* $F$ *é uma aplicação* $F \to F$*, geralmente denotada por* $a \mapsto a'$*, que satisfaz* $(a+b)' = a' + b'$ *e* $(ab)' = a'b + ab'$*,* $\forall a, b \in F$*.*

**Definição 2** (corpo diferencial)**.** *Um* corpo diferencial *é um corpo munido de uma derivação.*

Se $F$ é um corpo diferencial, chamaremos de *constantes* de $F$ os elementos $\alpha \in F$ tais que $\alpha' = 0$.

**Proposição 1.** *Seja* $F$ *um corpo diferencial. Então*

(i) *Para todo* $a \in F$ *e todo inteiro* $n$ *vale:* $(a^n)' = na^{n-1}a'$*.*

(ii) *Para todos* $a, b \in F$*, com* $b \neq 0$*, vale a "regra do quociente":*

$$\left(\frac{a}{b}\right)' = \frac{a'b - ab'}{b^2}.$$

(iii) *O conjunto das constantes de* $F$ *é um subcorpo de* $F$*.*

*Prova.* (i) Note que $0' = 0$ pois $0' = (0+0)' = 0' + 0'$. De modo análogo, $1' = 0$ pois $1' = (1 \cdot 1)' = 1' \cdot 1 + 1 \cdot 1' = 1' + 1'$. Assim, para $a = 0$ vale o afirmado. Suponha $a \neq 0$. Se $n = 0$ temos $(a^0)' = 1' = 0 = 0a^{0-1}a'$. Se $n = 1$ temos $(a^1)' = a' = 1a^{1-1}a'$. Por indução, suponha válido para $n > 0$. Então $(a^{n+1})' = (a^n a)' = (a^n)'a + a^n a' = na^{n-1}a'a + a^n a' = (na^n + a^n)a' = (n+1)a^n a'$. Isso prova a afirmação para todos os inteiros $n \geq 0$. Por outro lado, se $n > 0$, então

$$0 = 1' = (a^{-n}a^n)' = (a^{-n})'a^n + a^{-n}(a^n)' = (a^{-n})'a^n + a^{-n}na^{n-1}a'.$$

Então $(a^{-n})' = -na^{-n-1}a'$, e o resultado também é válido para inteiros negativos.

(ii) Pelo item (i), $(b^{-1})' = -b^{-2}b'$. Assim,

$$\left(\frac{a}{b}\right)' = (ab^{-1})' = a'b^{-1} + a(b^{-1})' = a'b^{-1} + a(-b^{-2}b') = \frac{a'b - ab'}{b^2}.$$

(iii) Já provamos que $0$ e $1$ são constantes. Sejam $\alpha$ e $\beta$ constantes de $F$. Então $(\alpha + \beta)' = \alpha' + \beta' = 0 + 0 = 0$ e $(\alpha\beta)' = \alpha'\beta + \alpha\beta' = 0$, e o conjunto das constantes é fechado por soma e produto. Além disso, se $\alpha$ é uma constante não nula então $(\alpha^{-1})' = -\alpha^{-2}\alpha' = 0$ e portanto o inverso de uma constante é constante. Temos também $0 = 0' = (-\alpha + \alpha)' = (-\alpha)' + \alpha' = (-\alpha)'$ e o conjunto das constantes é fechado para o inverso aditivo, concluindo a prova de que é um corpo. □

Note que se $\alpha$ é constante e $a \in F$ então $(\alpha a)' = \alpha a'$.

**Definição 3.** *Seja* $F$ *um corpo diferencial e* $a, b \in F$*, com* $a \neq 0$*. Dizemos que* $a$ *é* uma exponencial de $b$*, ou que* $b$ *é* um logaritmo de $a$*, se* $b' = \frac{a'}{a}$.

Essa terminologia é conveniente pois as únicas propriedades das exponenciais e logaritmos que estamos interessados são as suas propriedades diferenciais.

Aplicando indução e as propriedades da derivação é fácil obter a *identidade da derivada logarítmica*:

$$\frac{(a_1^{\nu_1} \cdots a_n^{\nu_n})'}{a_1^{\nu_1} \cdots a_n^{\nu_n}} = \nu_1 \frac{a_1'}{a_1} + \cdots + \nu_n \frac{a_n'}{a_n}$$

onde $a_1, \ldots, a_n$ são elementos não nulos de $F$ e $\nu_1, \ldots, \nu_n$ são inteiros, positivos ou negativos. Essa identidade será muito útil a seguir.

**Definição 4** (extensão diferencial)**.** *Uma* extensão diferencial $K/F$ *de um corpo diferencial* $F$ *é um corpo diferencial* $K$ *que estende* $F$ *e cuja derivação estende a derivação de* $F$*.*

**Definição 5** (extensão elementar)**.** *Seja* $F$ *um corpo diferencial. Uma* extensão elementar *de* $F$ *é uma extensão diferencial de* $F$ *obtida por sucessivas adjunções de elementos que são algébricos, exponenciais ou logaritmos, ou seja, uma extensão diferencial da forma* $F(t_1, \ldots, t_N)$*, onde cada* $t_i$ *é algébrico sobre o corpo* $F(t_1, \ldots, t_{i-1})$ *ou é o logaritmo ou é a exponencial de um elemento de* $F(t_1, \ldots, t_{i-1})$*.*

Note que cada corpo intermediário $F(t_1, \ldots, t_{i-1})$ é um corpo diferencial e uma extensão elementar de $F$.

Essa definição captura a noção de função elementar: as funções elementares são as funções contidas em extensões elementares do corpo das funções racionais.

Os lemas a seguir serão fundamentais para a prova do teorema de Liouville na seção 3:

**Lema 1.** *Sejam* $F$ *um corpo diferencial e* $F(t)$ *uma extensão diferencial de* $F$ *tendo o mesmo subcorpo de constantes, com* $t$ *transcendente sobre* $F$ *e com* $t' \in F$. *Então, para todo "polinômio"*[1] $f(t) \in F[t]$ *de grau positivo,* $(f(t))'$ *é um "polinômio" em* $F[t]$ *de mesmo grau que* $f(t)$*, ou de um grau a menos, dependendo se o coeficiente do termo de maior grau de* $f(t)$ *não é, ou é, uma constante.*

*Prova.* Sejam $b = t' \in F$ e $n$ o grau de $f(t)$. Se $f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0$, com $a_0, \ldots, a_n \in F$, e $a_n \neq 0$, então
$(f(t))' = (a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0)'$
$= (a_n t^n)' + (a_{n-1}t^{n-1})' + \cdots + (a_1 t)' + a_0'$
$= (a_n' t^n + a_n n t^{n-1} t') + (a_{n-1}' t^{n-1} + a_{n-1} t') + \cdots + (a_1' t + a_1 t') + a_0'$
$= a_n' t^n + (n a_n b + a_{n-1}')t^{n-1} + \cdots$

Se $a_n$ não é constante então $a_n' \neq 0$ e $(f(t))'$ tem grau $n$.

Se $a_n$ é constante, então $a_n' = 0$ e queremos provar que o coeficiente $n a_n b + a_{n-1}'$ de $t^{n-1}$ não é zero. Se fosse, teríamos

$$(n a_n t + a_{n-1})' = n a_n b + a_{n-1}' = 0$$

e então $n a_n t + a_{n-1}$ seria constante, logo um elemento de $F$, pois $F$ e $F(t)$ têm as mesmas constantes, contrariando a transcendência de $t$ sobre $F$. □

**Lema 2.** *Sejam* $F$ *um corpo diferencial e* $F(t)$ *uma extensão diferencial de* $F$ *tendo o mesmo subcorpo de constantes, com* $t$ *transcendente sobre* $F$ *e com* $\frac{t'}{t} \in F$. *Então, para todo* $a \in F$, $a \neq 0$ *e todo inteiro não nulo* $n$*, temos* $(at^n)' = dt^n$ *para algum* $d \in F$, $d \neq 0$. *Além disso, para todo "polinômio"* $f(t) \in F[t]$ *de grau positivo,* $(f(t))'$ *é um "polinômio" em* $F[t]$ *de mesmo grau, e é um múltiplo de* $f(t)$ *somente se* $f(t)$ *é um monômio.*

*Prova.* Seja $b = \frac{t'}{t} \in F$. Seja $a \in F$, $a \neq 0$, e seja $n$ um inteiro não nulo. Temos

$$(at^n)' = a' t^n + n a t^{n-1} t' = a' t^n + n a t^{n-1} b t = (a' + nab)t^n = dt^n,$$

onde $d = a' + nab \in F$.

Se $d = 0$ temos $(at^n)' = 0$, e $at^n$ é constante, contrariando a transcendência de $t$ sobre $F$. Logo $d \neq 0$.

[1] Estritamente falando, $f(t)$ não é um polinômio, mas sim o valor de um polinômio em $t$. Como $t$ é transcendente, podemos identificar $F[t]$ com o anel de polinômios $F[X]$.

Seja $f(t) \in F[t]$ de grau positivo. Pelo que acabamos de ver, o grau é preservado pela derivação, e portanto $(f(t))'$ tem o mesmo grau que $f(t)$.

Se $(f(t))'$ é um múltiplo de $f(t)$, deve ser por um fator em $F$, já que ambos têm o mesmo grau. Então existe $c \in F$ tal que $(f(t))' = cf(t)$. Suponha que $f(t)$ não é um monômio, e que $a_n t^n$ e $a_m t^m$ são dois de seus termos distintos. Como a derivação preserva o grau de cada termo, temos $(a_n t^n)' = c a_n t^n$ e $(a_m t^m)' = c a_m t^m$. Assim,

$$\left(\frac{a_n t^n}{a_m t^m}\right)' = \frac{(a_n t^n)' a_m t^m - a_n t^n (a_m t^m)'}{(a_m t^m)^2} = \frac{c a_n t^n a_m t^m - a_n t^n c a_m t^m}{(a_m t^m)^2} = 0.$$

Portanto, $\frac{a_n t^n}{a_m t^m}$ é constante, novamente contrariando a transcendência de $t$ sobre $F$. □

## 3. O Teorema de Liouville

A versão algébrica do teorema de Liouville, que vamos provar agora, não usa a noção de integral e sim a noção de primitiva.

**Definição 6** (primitiva)**.** *Seja $h$ um elemento de um corpo diferencial $F$. Uma* primitiva *de $h$ é um elemento $y$ de alguma extensão diferencial de $F$ tal que $y' = h$.*

**Teorema 5** (Liouville)**.** *Seja $F$ um corpo diferencial de característica zero e $h \in F$. Se $h$ tem primitiva em alguma extensão elementar de $F$ tendo o mesmo subcorpo de constantes, então existem constantes $\alpha_1, \ldots, \alpha_n \in F$ e elementos $u_1, \ldots, u_n, v \in F$ tais que*

$$h = v' + \sum_{i=1}^{n} \alpha_i \frac{u_i'}{u_i}.$$

*Prova.* Por hipótese, existe uma torre de corpos diferenciais

$$F \subset F(t_1) \subset \cdots \subset F(t_1, \ldots, t_N),$$

todos com o mesmo subcorpo de constantes, onde cada $t_i$ é algébrico sobre $F(t_1, \ldots, t_{i-1})$, ou é o logaritmo ou é a exponencial de um elemento desse corpo, e existe um elemento $y \in F(t_1, \ldots, t_N)$ com $y' = h$. Provaremos o teorema por indução em $N$. O caso $N = 0$ é trivial, pois $y' = h$ com $y \in F$ e basta tomar $v = y$ que teremos $h = v'$, com $v \in F$. Supomos então $N > 0$ e o teorema válido para extensões elementares de altura menor que $N$.

Como $h \in F \subset F(t_1)$, temos $h \in F(t_1)$. Pela hipótese de indução aplicada à extensão elementar $F(t_1) \subset F(t_1, \ldots, t_N)$, podemos escrever

$$h = v' + \sum_{i=1}^{n} \alpha_i \frac{u_i'}{u_i},$$

com $\alpha_1, \ldots, \alpha_n$ constantes e $u_1, \ldots, u_n, v \in F(t_1)$. Note que os $\alpha_i$ estão em $F$ pois todos os corpos da torre têm o mesmo subcorpo de constantes. O que falta então é encontrar uma expressão semelhante para $h$, possivelmente com outro "$n$", mas com todos os $u_1, \ldots, u_n, v$ em $F$. Denotando $t = t_1$, temos que $t$ é algébrico sobre $F$, ou é exponencial ou logaritmo de elemento de $F$. Consideraremos esses três casos a seguir.

Suponha que $t$ é *algébrico* sobre $F$. Nesse caso, temos $F(t) = F[t]$ e então existem polinômios $U_1, \ldots, U_n, V \in F[X]$ tais que $u_1 = U_1(t), \ldots, u_n = U_n(t), v = V(t)$:

$$h = (V(t))' + \sum_{i=1}^{n} \alpha_i \frac{(U_i(t))'}{U_i(t)}$$

Sejam $\tau_1 (= t), \tau_2, \ldots, \tau_s$ os conjugados de $t$ sobre $F$ (demais raízes do polinômio minimal). Aplicando o automorfismo que leva $t$ em $\tau_j$ (ver apêndice), obtemos:

$$h = (V(\tau_j))' + \sum_{i=1}^{n} \alpha_i \frac{(U_i(\tau_j))'}{U_i(\tau_j)}.$$

Somando todas essas equações obtemos:

$$h = \left( \frac{V(\tau_1) + \cdots + V(\tau_s)}{s} \right)' + \sum_{i=1}^{n} \frac{\alpha_i}{s} \frac{(U_i(\tau_1) \cdots U_i(\tau_s))'}{U_i(\tau_1) \cdots U_i(\tau_s)}.$$

Observe que aqui entra a hipótese da característica zero, pois poderíamos ter divisão por zero caso $s$ fosse múltiplo da característica.

Cada $U_i(\tau_1) \cdots U_i(\tau_s)$ e $V(\tau_1) + \cdots + V(\tau_s)$ está em $F$ pois ficam fixos por qualquer automorfismo que permute os $\tau_i$ e deixe $F$ fixo. Portanto a última equação é uma expressão de $h$ na forma desejada.

Nos casos restantes, onde $t$ é o logaritmo ou a exponencial de um elemento de $F$, podemos supor que $t$ é *transcendente* sobre $F$, pois o caso algébrico já foi tratado acima. Nesse caso, temos:

$$h = (v(t))' + \sum_{i=1}^{n} \alpha_i \frac{(u_i(t))'}{u_i(t)}, \tag{1}$$

com $u_1(t), \ldots, u_n(t), v(t) \in F(t)$.

Cada $u_i(t)$ pode ser escrito como $u_i(t) = aP_1(t)^{e_1} \cdots P_k(t)^{e_k}$ onde $a \in F$, cada $P_j$ é um "polinômio" mônico irredutível de $F[t]$, e os $e_j$ são inteiros (possivelmente negativos). Usando a identidade da derivada logarítmica, temos:

$$\frac{(u_i(t))'}{u_i(t)} = \frac{(aP_1(t)^{e_1} \cdots P_k(t)^{e_k})'}{aP_1(t)^{e_1} \cdots P_k(t)^{e_k}} = \frac{a'}{a} + e_1\frac{(P_1(t))'}{P_1(t)} + \cdots + e_k\frac{(P_k(t))'}{P_k(t)}.$$

Podemos, portanto, reescrever $\sum \alpha_i \frac{(u_i(t))'}{u_i(t)}$ numa forma semelhante, porém com cada $u_i(t)$ ou em $F$ ou um elemento mônico irredutível de $F[t]$. Naturalmente, também podemos supor que os $u_i(t)$ são distintos (combinando constantes se necessário).

Agora olhamos para a decomposição de $v(t)$ em frações parciais (ver apêndice), que expressa $v(t)$ como a soma de um elemento de $F[t]$ mais vários termos da forma $\frac{g(t)}{(f(t))^r}$, onde $f(t)$ é um elemento mônico irredutível de $F[t]$, $r$ um inteiro positivo, e $g(t)$ é um elemento não nulo de $F[t]$ de grau menor que o grau de $f(t)$.

Como $h$ está em $F$, o lado direito da equação 1 não deve envolver $t$, exigindo que os $u_1(t), \ldots, u_n(t), v(t)$ tenham uma forma especial. Para investigar esta forma, é conveniente separar os casos exponencial e logaritmo, pois em cada caso um dos lemas da seção 2 será necessário.

Suponha que $t$ é o *logaritmo* de um elemento de $F$. Então $t' = \frac{a'}{a}$, para algum $a \in F$. Seja $f(t)$ um elemento mônico irredutível de $F[t]$. Pelo lema 1, $(f(t))'$ também está em $F[t]$ e tem grau menor que o de $f(t)$, pois $f(t)$ é mônico. Logo $f(t)$ não divide $(f(t))'$.

Assim, se $u_i(t) = f(t)$, então a fração $\frac{(u_i(t))'}{u_i(t)}$ já está reduzida, com denominador $f(t)$. Se $\frac{g(t)}{(f(t))^r}$ ocorre na expressão em frações parciais de $v(t)$, com $g(t) \in F[t]$ de grau menor que o de $f(t)$, e $r > 0$ e maximal para dado $f(t)$, então $(v(t))'$ consistirá de vários termos tendo $f(t)$ no denominador no máximo $r$ vezes mais $g(t)\left(\frac{1}{(f(t)^r)}\right)' = \frac{-rg(t)(f(t))'}{f(t)^{r+1}}$. Como $f(t)$ não divide $g(t)(f(t))'$, vemos que um termo com denominador $(f(t))^{r+1}$ de fato aparece em $(v(t))'$. Então, se $f(t)$ aparece como um denominador na expansão em frações parciais de $v(t)$, aparecerá em $h$, o que é impossível, pela unicidade da decomposição em frações parciais. Portanto, $f(t)$ não aparece no denominador de $v(t)$. Assim, $f(t)$ não pode ser um dos $u_i(t)$ também.

Como isso é verdade para todo $f(t)$ irredutível mônico, concluímos que cada $u_i(t) \in F$ e $v(t) \in F[t]$. Da expressão de $h$, concluímos que

$(v(t))' \in F$. Usando novamente o lema 1 (agora para $v(t)$), temos que $v(t) = \beta t + d$, com $\beta$ constante e $d \in F$. Então

$$h = \beta\frac{a'}{a} + d' + \sum_{i=1}^{n} \alpha_i \frac{u_i'}{u_i} = d' + \sum_{i=0}^{n} \alpha_i \frac{u_i'}{u_i}$$

com $\alpha_0 = \beta$ e $u_0 = a$, é uma expressão para $h$ da forma desejada.

Finalmente, consideremos o caso onde $t$ é a *exponencial* de um elemento de $F$. Então $\frac{t'}{t} = b'$, com $b \in F$. Seja $f(t)$ um elemento mônico irredutível de $F[t]$, diferente do monômio $t$. Pelo lema 2, $(f(t))' \in F[t]$ e $f(t)$ não divide $(f(t))'$ pois não é um monômio ($f(t) \neq t^k$ pois esse é redutível). Exatamente o mesmo argumento usado acima mostra que $f(t)$ não pode ocorrer no denominador de $v(t)$, nem pode ser um dos $u_i(t)$. Logo $v(t)$ é da forma $v(t) = \sum_j a_j t^j$, onde cada $a_j \in F$ e $j$ varia num conjunto finito de inteiros, que podem ser positivos, negativos ou zero e cada um dos $u_1(t), \ldots, u_n(t)$ está em $F$, com a possível exceção de um deles, que pode ser igual a $t$. Como cada $\frac{(u_i(t))'}{u_i(t)}$ está em $F$, temos $(v(t))' \in F$, pois $h \in F$. Como $v(t) = \sum_j a_j t^j$, temos

$$(v(t))' = \left(\sum_j a_j t^j\right)' = \sum_j \left(a_j t^j\right)' = \sum_j d_j t^j.$$

Na última igualdade, pelo lema 2, os inteiros $j$ variam no mesmo conjunto de índices e $d_j \neq 0$ se $a_j \neq 0$. Mas $(v(t))' \in F$, então o único expoente de $t$ que pode aparecer na soma é zero, pois $t$ é transcendente sobre $F$. Logo $(v(t))' = d_0$ e portanto $v(t) = a_0 \in F$.

Se cada $u_i(t)$ está em $F$, já temos $h$ na forma desejada. Caso contrário, somente um deles, digamos, $u_1(t)$ não está em $F$. Daí $u_1(t) = t$ e $u_2(t), \ldots, u_n(t) \in F$ e podemos escrever:

$$h = v' + \alpha_1\frac{t'}{t} + \sum_{i=2}^{n} \alpha_i \frac{u_i'}{u_i} = (v + \alpha_1 b)' + \sum_{i=2}^{n} \alpha_i \frac{u_i'}{u_i}$$

com $u_2, \ldots, u_n, v + \alpha_1 b$ todos em $F$, como queríamos. Isso conclui a prova do teorema de Liouville. □

## 4. Liouville Racional

Consideraremos agora funções na variável real $x$, com valores complexos. Para a demonstração do teorema de Liouville racional, precisaremos da seguinte proposição:

**Proposição 2.** *Seja $g$ uma função no corpo de funções racionais $\mathbf{C}(x)$, não constante. Então $e^g$ é transcendente sobre $\mathbf{C}(x)$.*

*Prova.* Se $e^g$ fosse algébrica, considerando o seu polinômio minimal teríamos uma equação da forma:

$$e^{ng} + a_1 e^{(n-1)g} + \cdots + a_n = 0,$$

com $a_1, \ldots, a_n \in \mathbf{C}(x)$ e $a_n \neq 0$. Derivando, obtemos:

$$ng' e^{ng} + (a_1' + (n-1)a_1 g') e^{(n-1)g} + \cdots + a_n' = 0,$$

que deve ser proporcional à primeira equação, pois tem o mesmo grau (já que $g' \neq 0$) e o polinômio minimal divide todos os outros que tenham $e^g$ como raiz. Então

$$\frac{ng'}{1} = \frac{a_n'}{a_n}. \tag{2}$$

Como $a_n \in \mathbf{C}(x)$, podemos escrever $a_n = P_1^{e_1} \cdots P_k^{e_k}$ com os $P_i$ polinômios de grau 1 distintos e os $e_i$ inteiros (positivos ou negativos), pois os elementos irredutíveis de $\mathbf{C}[x]$ são os polinômios de grau 1. Então

$$\frac{a_n'}{a_n} = \frac{(P_1^{e_1} \cdots P_k^{e^k})'}{(P_1^{e_1} \cdots P_k^{e^k})} = \sum_{i=1}^{k} e_i \frac{P_i'}{P_i} = \sum_{i=1}^{k} \frac{\alpha_i}{P_i},$$

onde os $\alpha_i = e_i P_i'$ são constantes ($P_i'$ é constante pois $P_i$ tem grau 1).

Como $g \in \mathbf{C}(x)$, temos $g = \frac{P}{Q}$ com P e Q polinômios relativamente primos, e obtemos:

$$g' = \left(\frac{P}{Q}\right)' = \frac{P'Q - PQ'}{Q^2}.$$

Portanto, pela equação 2:

$$n(P'Q - PQ') = Q^2 \sum_{i=1}^{k} \frac{\alpha_i}{P_i}$$

Note que

$$\sum \frac{\alpha_i}{P_i} = \frac{\alpha_1}{P_1} + \frac{\alpha_2}{P_2} + \cdots + \frac{\alpha_k}{P_k} = \frac{\alpha_1 \widehat{P_1} P_2 \cdots P_k + \cdots + \alpha_k P_1 P_2 \cdots \widehat{P_k}}{P_1 P_2 \cdots P_k},$$

onde $\widehat{P_i}$ denota que o elemento $P_i$ não aparece no produto.

Então

$$n(P'Q - PQ') = Q^2 \frac{A}{B}$$

onde $A = \alpha_1 \widehat{P_1} P_2 \cdots P_k + \cdots + \alpha_k P_1 P_2 \cdots \widehat{P_k}$ e $B = P_1 P_2 \cdots P_k$.

Logo

$$nB(P'Q - PQ') = Q^2 A \tag{3}$$

Agora, para qualquer um dos $P_i$, temos que $P_i$ não divide $A$, pois exatamente um termo em $A$ não é múltiplo de $P_i$. Mas $P_i$ divide $B$, e pela equação 3, concluímos que $P_i$ divide $Q$. Escrevendo $Q = P_i^m C$, onde $C$ é um polinômio não divisível por $P_i$, obtemos

$$Q' = mP_i^{m-1}P_i'C + P_i^m C'.$$

Substituindo essas expressões para $Q$ e $Q'$ na equação 3, obtemos:

$$nB(P'P_i^m C - mPP_i^{m-1}P_i'C - PP_i^m C') = P_i^{2m}C^2A$$

Evidenciando $P_i^{m-1}$, temos:

$$nBP_i^{m-1}(P'P_iC - mPP_i'C - PP_iC') = P_i^{2m}C^2A$$

Mas $B = P_1P_2\cdots P_k$, logo:

$$n\widehat{B}P_i^m(P'P_iC - mPP_i'C - PP_iC') = P_i^{2m}C^2A,$$

onde $\widehat{B} = P_1P_2\cdots\widehat{P_i}\cdots P_k$ é o elemento $B$ sem o termo $P_i$. Observe que o termo entre parênteses não é divisível por $P_i$, pois $P_i$ não divide $PP_i'C$ (lembre que $P$ e $Q$ são relativamente primos e $P_i'$ é constante). Logo, no lado esquerdo da igualdade, o termo $P_i$ aparece com expoente exatamente $m$, enquanto no lado direito aparece com expoente exatamente $2m$. Então $m = 2m$, o que implica $m = 0$, e portanto $P_i$ não divide $Q$, uma contradição, a menos que os $P_i$ sejam todos constantes, o que implicaria $a_n$ constante, $a_n' = 0$ e, pela equação 2, $g' = 0$, contrariando a hipótese de $g$ não ser constante. □

Agora estamos prontos para provar a versão racional do teorema de Liouville.

**Teorema 3** (Liouville Racional)**.** *Sejam $f$ e $g$ funções racionais, com $g$ não constante. Se $\int fe^g$ é elementar, então $\int fe^g = Re^g$ onde $R$ é uma função racional.*

*Prova.* Denotando $t = e^g$, temos $\frac{t'}{t} = g'$. Note que $fe^g$ pertence ao corpo diferencial $\mathbf{C}(x,t)$. Pelo teorema de Liouville, podemos escrever:

$$ft = v' + \sum_{i=1}^{n} \alpha_i \frac{u_i'}{u_i},$$

com $\alpha_1,\ldots,\alpha_n \in \mathbf{C}$ e $u_1,\ldots,u_n,v \in \mathbf{C}(x,t)$.

Denotando $F = \mathbf{C}(x)$, temos $f,g \in F$ e $u_1,\ldots,u_n,v \in F(t)$. A proposição 2 é importante aqui, pois usamos o fato de que $e^g$ é transcendente sobre $\mathbf{C}(x)$ para poder aplicar o lema 2 com $t = e^g$ e $F = C(x)$. O raciocínio é exatamente o mesmo usado na demonstração da parte exponencial do teorema de Liouville. Fatoramos cada $u_i$ como

produto de polinômios mônicos irredutíveis de $F[t]$, elevados a expoentes inteiros e aplicamos a identidade da derivada logarítmica para concluir que podemos considerar os $u_i$ que não estão em $F$ como sendo polinômios mônicos irredutíveis distintos. Em seguida, consideramos a decomposição de $v$ em frações parciais com respeito a $F[t]$ e aplicamos o lema 2 para concluir que o único fator irredutível mônico possível em um denominador de $v$ é $t$, que é também a única possibilidade para algum $u_i$ que não esteja em $F$. Portanto $v$ é da forma $v = \sum b_j t^j$, para $j$ variando em algum conjunto finito de inteiros e cada $b_j \in F$.

Como $\sum \alpha_i \frac{u_i'}{u_i} \in F$, temos $v' = ft + a$, onde $a \in F$. Da expressão de $v$, obtemos $v' = \sum (b_j' + j b_j g') t^j$ e portanto $f = b_1' + b_1 g'$. Denotando $R = b_1$, temos $f = R' + Rg'$, com $R \in \mathbf{C}(x)$. Multiplicando por $e^g$ ambos os lados, temos $fe^g = R'e^g + Rg'e^g = (Re^g)'$ e portanto $\int fe^g = Re^g$ onde $R$ é uma função racional.

□

## 5. APÊNDICE

**Proposição 3.** *Sejam $F$ um corpo diferencial de característica zero e $K$ uma extensão algébrica de $F$. Então a derivação em $F$ pode ser estendida a uma derivação em $K$ e essa extensão é única.*

Observamos que a restrição a característica zero não é essencial. Basta supor $K$ separável sobre $F$, e a prova a seguir continuará válida.

*Prova.* Seja $X$ uma indeterminada e defina os mapas $D_0$, $D_1$ do anel de polinômios $F[X]$ em si mesmo por

$$D_0\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} a_i' X^i, \quad D_1\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} i a_i X^{i-1}$$

para $a_0, a_1, \ldots, a_n \in F$.

Suponha que $K$ tem uma derivação estendendo a derivação de $F$. Então para qualquer $x \in K$ e $A(X) \in F[X]$, temos:

$$(A(x))' = (D_0 A)(x) + (D_1 A)(x) \cdot x'.$$

Seja $f(X)$ o polinômio minimal de $x$ sobre $F$. Então $(D_1 f)(x) \neq 0$ pois $x$ é raiz simples de $f(X)$. Substituímos $A(X)$ por $f(X)$ na igualdade acima e obtemos

$$x' = -\frac{(D_0 f)(x)}{(D_1 f)(x)}\,. \tag{4}$$

Isso prova a unicidade.

Agora provaremos a existência. Vamos supor $K = F(x)$ para algum $x \in K$. Os demais casos seguem por argumentos usuais da teoria de corpos.

Seja $D : F[X] \to F[X]$ um mapa definido por:

$$DA = D_0A + g(X)D_1A,$$

para todo $A \in F[X]$. O polinômio $g(X) \in F[X]$ será determinado mais adiante.

Note que vale $D(A + B) = DA + DB$ e $D(AB) = (DA)B + A(DB)$ para todo $A, B \in F[X]$ pois as mesmas igualdades valem para $D_0$ e $D_1$. Além disso, $Da = a'$ para todo $a \in F$. Considere agora o homomorfismo sobrejetivo $F[X] \to F[x]$, que é a identidade em $F$ e leva $X$ em $x$. Seu núcleo é o ideal $f(X)F[X]$, onde $f(X)$ é o polinômio minimal de $x$ sobre $F$. Como $x$ é algébrico, temos $F[x] = F(x) = K$. Logo, $F[X]/f(X)F[X]$, que é o anel quociente de $F[X]$ pelo núcleo do homomorfismo, é isomorfo a $K$. Assim, precisamos mostrar que $D$ mapeia $f(X)F[X]$ em si mesmo para poder passar ao quociente e obter $D$ como um mapa de $K$ em si mesmo que será uma derivação em $K$ que estende a de $F$, pois $D$ satifaz a definição de derivação e $Da = a'$ se $a \in F$. Para isso, é suficiente verificar que $D$ leva $f(X)$ em um múltiplo de si mesmo, ou seja, que $Df$ seja um elemento de $F[X]$ do qual $x$ é uma raiz, ou que $(Df)(x) = 0$. Essa última condição é equivalente a $(D_0f)(x) + g(x)(D_1f)(x) = 0$. Como $(D_1f)(x) \neq 0$ e $F(x) = F[x]$, um polinômio $g(X) \in F[X]$ pode de fato ser encontrado de forma que $(Df)(x) = 0$, concluindo o que queríamos. □

**Proposição 4.** *Sejam* $F$ *um corpo diferencial de característica zero,* $t$ *algébrico sobre* $F$, $\tau$ *um conjugado de* $t$, *e* $\varphi$ *o homomorfismo que leva* $t$ *em* $\tau$ *e deixa* $F$ *fixo. Então para todo* $A(X) \in F[X]$ *temos* $\varphi(A(t)) = A(\tau)$ *e* $\varphi((A(t))') = (A(\tau))'$.

Note que a derivação que estamos considerando nos corpos $F(t)$ e $F(\tau)$ é a que estende a de $F$. Ela existe e é única pela proposição 3.

*Prova.* A igualdade $\varphi(A(t)) = A(\tau)$ é óbvia pela própria definição de $\varphi$.

Para provar a outra igualdade, seja $f(X)$ o polinômio minimal de $t$ sobre $F$. Note que $f(X)$ também é o polinômio minimal de $\tau$ pois $t$ e $\tau$ são conjugados. Usamos a equação 4 da proposição anterior para obter $t' = -\frac{(D_0f)(t)}{(D_1f)(t)}$. Como $D_0f$ e $D_1f$ são polinômios, podemos aplicar a primeira igualdade da proposição para obter

$$\varphi(t') = \varphi\left(-\frac{(D_0f)(t)}{(D_1f)(t)}\right) = -\frac{\varphi((D_0f)(t))}{\varphi((D_1f)(t))} = -\frac{(D_0f)(\tau)}{(D_1f)(\tau)} = \tau'.$$

Portanto $\varphi(t') = \tau'$.

Agora observe que se $a_n t^n$ é um termo de $A(t)$, então $(a_n t^n)' = a_n' t^n + n a_n t^{n-1} t'$. Aplicando $\varphi$, temos:

$$\varphi((a_n t^n)') = \varphi(a_n' t^n + n a_n t^{n-1} t') = a_n' \tau^n + n a_n \tau^{n-1} \varphi(t')$$
$$= a_n' \tau^n + n a_n \tau^{n-1} \tau' = (a_n \tau^n)'.$$

Como isso vale para cada termo do polinômio $A(t)$, vale para o polinômio $A(t)$, concluindo assim o afirmado. □

Agora provaremos o resultado sobre expansão em frações parciais usado na demonstração do teorema de Liouville, seguindo a exposição de Bronstein [1].

A expansão em frações parciais é válida para domínios euclidianos, portanto vale para o anel de polinômios com coeficientes num corpo (que é um domínio euclidiano via a função grau).

**Proposição 5.** *Sejam* $D$ *um domínio euclidiano,* $\nu$ *sua função norma e* $d \in D$, $d \neq 0$. *Seja* $d = d_1 \cdots d_n$ *uma fatoração de* $d$ *em fatores primos entre si, não necessariamente em irredutíveis. Então, para todo* $a \in D$, $a \neq 0$, *existem* $a_0, a_1, \ldots, a_n \in D$ *tais que ou* $a_i = 0$ *ou* $\nu(a_i) < \nu(d_i)$ *e*

$$\frac{a}{d} = \frac{a}{d_1 \cdots d_n} = a_0 + \sum_{i=1}^{n} \frac{a_i}{d_i}.$$

Tal decomposição é chamada decomposição em frações parciais de $\frac{a}{d}$ com respeito à fatoração $d = d_1 \cdots d_n$.

*Prova.* Usamos a divisão euclidiana para escrever $a = d a_0 + r$, onde ou $r = 0$ ou $\nu(r) < \nu(d)$. Se $n = 1$, então $\frac{a}{d} = a_0 + \frac{r}{d}$ já está na forma desejada. Por indução, suponha o resultado válido para $n-1$. Como $\mathrm{mdc}(d_i, d_j) = 1$ se $i \neq j$, temos que $\mathrm{mdc}(d_1, d_2 \cdots d_n) = 1$, e então existem $a_1, b \in D$, tais que

$$r = a_1(d_2 \cdots d_n) + b d_1$$

e ou $a_1 = 0$ ou $\nu(a_1) < \nu(d_1)$. Pela hipótese de indução, existem $b_0, a_2, \ldots, a_n \in D$ tais que ou $a_i = 0$ ou $\nu(a_i) < \nu(d_i)$ e

$$\frac{b}{d_2 \cdots d_n} = b_0 + \sum_{i=2}^{n} \frac{a_i}{d_i}.$$

Portanto,

$$\frac{a}{d} = a_0 + \frac{r}{d} = a_0 + \frac{a_1}{d_1} + \frac{b}{d_2 \cdots d_n} = (a_0 + b_0) + \sum_{i=1}^{n} \frac{a_i}{d_i}.$$

□

Note que no caso de anéis de polinômios, como $\text{grau}(r) < \text{grau}(d) = \text{grau}(d_1) + \text{grau}(d_2 \cdots d_n)$ e $\text{grau}(a_1) < \text{grau}(d_1)$, então $\text{grau}(b) < \text{grau}(d_2 \cdots d_n)$ e então $b_0 = 0$.

Precisamos mais uma proposição para concluir o que queremos:

**Proposição 6.** *Seja* $m \geq 1$ *e* $d \in D$, $d \neq 0$. *Então, para todo* $a \in D$, $a \neq 0$, *existem* $a_0, a_1, \ldots, a_m \in D$, *tais que ou* $a_j = 0$ *ou* $\nu(a_j) < \nu(d)$, *e*

$$\frac{a}{d^m} = a_0 + \sum_{j=1}^{m} \frac{a_j}{d^j}.$$

*Prova.* Pela divisão euclidiana, escrevemos $a = dq + a_m$, onde ou $a_m = 0$ ou $\nu(a_m) < \nu(d)$. Então

$$\frac{a}{d^m} = \frac{dq + a_m}{d^m} = \frac{q}{d^{m-1}} + \frac{a_m}{d^m}.$$

Se $m = 1$, então acima temos a igualdade desejada, com $a_0 = q$. Caso contrário, novamente por argumento indutivo, temos que existem $a_0, a_1, \ldots, a_{m-1} \in D$ tais que ou $a_j = 0$ ou $\nu(a_j) < \nu(d)$, para $j \geq 1$ e

$$\frac{q}{d^{m-1}} = a_0 + \sum_{j=1}^{m-1} \frac{a_j}{d^j}.$$

Portanto,

$$\frac{a}{d^m} = \frac{q}{d^{m-1}} + \frac{a_m}{d^m} = a_0 + \sum_{j=1}^{m} \frac{a_j}{d^j}.$$

□

Agora, se temos $d = d_1^{e_1} \cdots d_n^{e_n}$ uma fatoração de $d$, não necessariamente em irredutíveis, onde $\text{mdc}(d_i, d_j) = 1$ se $i \neq j$, e os $e_i$ são inteiros positivos, e $a \in D$, $a \neq 0$, expressamos a decomposição em frações parciais de $\frac{a}{d}$ com respeito a $d = b_1 \cdots b_n$, onde $b_i = d_i^{e_i}$:

$$\frac{a}{d} = a_0 + \sum_{i=1}^{n} \frac{a_i}{b_i} = a_0 + \sum_{i=1}^{n} \frac{a_i}{d_i^{e_i}}.$$

Aplicamos a última proposição para cada termo da soma e obtemos:

$$\frac{a}{d} = \frac{a}{d_1^{e_1} \cdots d_n^{e_n}} = \tilde{a} + \sum_{i=1}^{n} \sum_{j=1}^{e_i} \frac{a_{ij}}{d_i^j},$$

onde $\tilde{a} \in D$ e ou $a_{ij} = 0$ ou $\nu(a_{ij}) < \nu(d_i)$ para todo $i$ e $j$.

Essa decomposição é chamada a *decomposição em frações parciais completa* de $\frac{a}{d}$ com respeito a fatoração $d = d_1^{e_1} \cdots d_n^{e_n}$, ou simplesmente a decomposição em frações parciais completa de $\frac{a}{d}$ quando a fatoração de $d$ em irredutíveis é usada.

## REFERÊNCIAS

As principais referências são o artigo de Rosenlicht [4] e o livro de Bronstein [1]. Os artigos de Potts [3] e de Kasper [2] contêm uma outra abordagem do assunto.

[1] Manuel Bronstein. *Symbolic integration. I*, volume 1 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, second edition, 2005. Transcendental functions.

[2] Toni Kasper. Integration in finite terms: the Liouville theory. *Math. Mag.*, 53(4):195–201, 1980.

[3] D. H. Potts. Elementary integrals. *Amer. Math. Monthly*, 63:545–554, 1956.

[4] Maxwell Rosenlicht. Integration in finite terms. *Amer. Math. Monthly*, 79:963–972, 1972.