UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

INSTITUTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Exemplos de Derivações Simples do Anel de Polinômios $k[x, y]$

Dissertação de Mestrado

Batista Nunes de Oliveira

Porto Alegre, Outubro de 2006.

Dissertação submetida por Batista Nunes de Oliveira como requisito parcial para a obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professora Orientadora:

Dr^{a}. Cydara Cavedon Ripoll

Banca Examinadora:

Dr^{a}. Ada Maria de Souza Doering

Dr. Antônio Paques

Dr^{a}. Cydara Cavedon Ripoll

Dr. Yves Lequain

Data Da Defesa: 30 de Outubro de 2006.

Agradecimentos

À minha família, principalmente a minha mãe, pelo incentivo, amor, compreensão e orações.

Especialmente à professora Ada Doering, que dispensou uma atenção especial, ajuda e apoio nos estudos.

À minha orientadora, Cydara Ripoll, pelo auxílio, dedicação e paciência para que este sonho se realizasse.

Aos colegas e professores do Programa de Pós-Graduação em Matemática da UFRGS, pela convivência e amizades realizadas.

Aos amigos: "Pelo incentivo e força, os quais guardo no lado esquerdo do peito."

Agradeço ao programa de Pós-Graduação em Matemática Pura da UFRGS, pela oportunidade que me foi dada.

À Rosane, secretária do Programa de Pós-Graduação, pela presteza em todos os momentos.

A Deus, que sempre está conosco e ilumina nossos caminhos.

E, por fim, a meu filho Renan e a minha esposa Margarete pela paciência e compreensão de alguns momentos, não poder dar toda a atenção e amor que merecem.

Resumo

Neste trabalho, apresentamos um algoritmo que nos permite decidir quando derivações de $k[x, y]$, do tipo Shamsuddin (isto é, derivações da forma

$$\partial_x + (a(x)y + b(x))\,\partial_y,$$

onde $a(x), b(x) \in k[x]$ e k é um corpo de característica zero) são simples.

Provamos também a simplicidade das derivações *do tipo quadráticas*

$$\Delta_p = \partial_x + (y^2 - p(x))\partial_y,$$

quando k é um corpo algebricamente fechado, onde $p(x) \in k[x]$ é um polinômio de grau ímpar.

Abstract

In this work, we present an algorithm that allows us to decide when derivations of $k[x, y]$ of Shamsuddin type (that is, derivations of the form

$$\partial_x + (a(x)y + b(x))\,\partial_y,$$

where $a(x), b(x) \in k[x]$ and k is a field of characteristic zero) are simple.

We also prove the simplicity of derivations of quadratic type

$$\Delta_p = \partial_x + (y^2 - p(x))\partial_y,$$

where k is an algebraically closed field and $p(x) \in k[x]$ is a polynomial of odd degree.

Sumário

1 INTRODUÇÃO

Sejam k um corpo de característica zero, $x_1, ..., x_n$ indeterminadas sobre k e $k[x_1, ..., x_n]$ o anel de polinômios sobre k. Denotamos por $End_k\left(k\left[x_1, ..., x_n\right]\right)$ a álgebra dos endomorfismos lineares de $k[x_1, ..., x_n]$. Exemplos de elementos pertencentes a esta álgebra são os operadores $\widehat{x_i}$, cuja ação sobre um polinômio de $k[x_1, ..., x_n]$ é dada pelo produto pela indeterminada x_i. Também são elementos de $End_k\left(k\left[x_1, ..., x_n\right]\right)$ os operadores $\partial_1, ..., \partial_n$, definidos por $\partial_i(f) = \partial f/\partial x_i$, para todo $f \in k[x_1, ..., x_n]$.

A $n-$*ésima Álgebra de Weyl sobre* k é definida como sendo a sub-álgebra de $End_k\left(k\left[x_1, ..., x_n\right]\right)$, gerada pelos operadores lineares $\widehat{x_1}, ..., \widehat{x_n}$ e $\partial_1, ..., \partial_n$. Denotaremos a mesma por

$$\mathbb{A}_n = k[\widehat{x_1}, ..., \widehat{x_n}]\left\langle \partial_1, ..., \partial_n \right\rangle.$$

Uma *derivação* de $k\left[x_1, ..., x_n\right]$ é uma aplicação

$$d : k\left[x_1, ..., x_n\right] \to k\left[x_1, ..., x_n\right]$$

que satisfaz

$$\begin{aligned} &(i) \qquad d(a+b) = d(a) + d(b) \\ &(ii) \qquad d(ab) = d(a)b + ad(b), \end{aligned}$$

para todos $a, b \in k\left[x_1, ..., x_n\right]$. Prova-se que toda derivação de $k\left[x_1, ..., x_n\right]$ é da forma $\alpha_1\partial_1 + \alpha_2\partial_2 + ... + \alpha_n\partial_n$, com $\alpha_i \in k[x_1, ..., x_n]$ para todo $i = 1, ..., n$.

Uma derivação d de $k\left[x_1, ..., x_n\right]$ é dita *simples* se não existem ideais próprios de $k[x_1, ..., x_n]$ estáveis por d.

Dado o importante papel das Álgebras de Weyl, é natural tentar conhecer sua estrutura. Sobre ideais maximais cíclicos da álgebra de Weyl conhecem-se já os seguintes resultados:

Teorema 1.1 ([4], Corollary 3.3) *Seja* $d = \partial_1 + \alpha_2\partial_2 + ... + \alpha_n\partial_n$ *uma derivação de* $k[x_1, ..., x_n]$, *com* $\alpha_i \in k[x_1, ..., x_n]$, *para todo* $i = 2, ..., n$. *Suponha que existe* $\gamma \in k[x_1, ..., x_n]$ *tal que* $\mathbb{A}_n \cdot (d + \gamma)$ *é um ideal maximal à esquerda de* $\mathbb{A}_n$. *Então* d *é uma derivação simples se* $\alpha_i \in k[x_1, ..., x_i]$, *para todo* $i = 2, ...n$.

Corolário 1.2 *Seja* $d = \partial_1 + \alpha_2\partial_2$ *uma derivação de* $k[x_1, x_2]$, *com* $\alpha_2 \in k[x_1, x_2]$. *Se* $\gamma \in k[x_1, x_2]$ *é tal que* $\mathbb{A}_2 \cdot (d + \gamma)$ *é um ideal maximal à esquerda de* $\mathbb{A}_2$ *então* d *é simples.*

O resultado a seguir garante a validade da recíproca do corolário acima:

Teorema 1.3 ([1], Main Th.) *Seja* $d = \partial_1 + \alpha_2\partial_2$ *uma derivação simples de* $k[x_1, x_2]$, *com* $\alpha_2 \in k[x_1, x_2]$. *Então existe* $\gamma \in k[x_1, x_2]$ *tal que* $\mathbb{A}_2 \cdot (d+\gamma)$ *é um ideal maximal à esquerda de* $\mathbb{A}_2$.

Estes resultados nos mostram que o problema de se gerar ideais maximais para $k[x_1, x_2]$ é bastante contemplado se sabemos reconhecer se uma dada derivação é ou não simples. Apesar de saber-se ser simples a maioria das derivações de $k[x_1, x_2]$, o problema de saber-se reconhecer se uma dada derivação é ou não simples não é amplamente resolvido.

O objetivo deste trabalho é:

- provar a simplicidade das derivações *do tipo quadráticas*

$$\Delta_p = \partial_x + (y^2 - p(x))\partial_y,$$

quando k é um corpo algebricamente fechado, onde $p(x) \in k[x]$ é um polinômio de grau ímpar

- apresentar um algoritmo que nos permite decidir quando derivações de $k[x, y]$ do tipo Shamsuddin são simples.

Tais resultados são devidos a A.Maciejewski, J.Moulin-Ollagnier e A.Nowicki, e podem ser encontrados em [5] e em [6].

Esta dissertação estrutura-se então da seguinte forma:

No capítulo 2, introduzimos algumas definições e resultados que são úteis ao desenvolvimento deste trabalho. Em especial, tratamos de algumas extensões de uma derivação.

No capítulo 3, estudamos extensões de uma derivação d de R a $R[t]$ e provamos o Teorema de Shamsuddin, principal resultado deste capítulo, que nos dá condições de decidir se conseguimos manter a simplicidade quando estendemos uma derivação simples de $k[x]$ a $k[x, y]$. Definimos derivações de Shamsuddin e apresentamos um algoritmo que nos permite decidir se uma derivação de $k[x, y]$ do tipo Shamsuddin é ou não simples.

No capítulo 4, definimos polinômio de Darboux para uma derivação de $k[x, y]$ e apresentamos a relação entre simplicidade e existência de polinômios de Darboux, bem como a relação entre existência de polinômios de Darboux e existência de soluções algébricas para certas equações diferenciais de primeira ordem com coeficientes em $k(x)$.

No capítulo 5, considerando ainda a equação de Riccati da forma

$$t' = t^2 - p(x),$$

onde $p = p(x)$ é um polinômio pertecente a $k[x]$, provamos que, no caso de k ser algebricamente fechado, suas soluções em $\overline{k(x)}$ (cuja existência, como será mostrado no capítulo 4, está relacionada com a simplicidade da derivação $\partial_x + (y^2 - p(x))\partial_y$), já são elementos de $k(x)$.

Finalmente no capítulo 6, abordamos a simplicidade das $k-$derivações de $k[x, y]$, da forma

$$\Delta_p = \partial_x + (y^2 - p(x))\partial_y,$$

onde $p(x) \in k[x]$ e provamos o resultado mais importante deste trabalho: se $p(x)$ é um polinômio não nulo de grau ímpar, então Δ_p é uma derivação simples. Provamos também que nenhuma derivação d de $k[x, y]$ da forma

$$d = \frac{\partial}{\partial x} + (y^2 - x^{2m} + mx^{m-1})\frac{\partial}{\partial y}, \quad m \in \mathbb{N}^*.$$

é simples .

Em todo este trabalho, denotamos por

- k um corpo de característica zero (que, a partir do Capítulo 5, passa a ser considerado algebricamente fechado);
- $k[x]$ o anel de polinômios com coeficientes em k a uma variável, considerando $grau\ 0 = -\infty$;
- $k[x, y]$ o anel de polinômios com coeficientes em k a duas variáveis;
- $k(x)$ o corpo das funções racionais com coeficientes em k em uma variável x;
- $\overline{k(x)}$ o fecho algébrico de $k(x)$;
- cfR o corpo de frações de um domínio R;
- R_P a localização de um domínio R pelo sistema multiplicativo determinado por um ideal primo P de R, isto é,

$$R_P = \left\{ \frac{c}{s} \mid s \in R \backslash P,\ c \in R \right\};$$

- $\frac{d}{dx}$, o operador derivada em relação à variável x no anel $k[x]$;
- $f' = \frac{df}{dx}$ a derivada de $f \in k[x]$;

- $\dfrac{\partial}{\partial x}$ e $\dfrac{\partial}{\partial y}$ os operadores derivadas parciais em relação às variáveis x e y, respectivamente (ou ainda, resumidamente, ∂_x e ∂_y) no anel $k[x, y]$.

Finalmente, por facilidade de escrita, denotamos simplesmente por $\sum_{i,j=o}^{n,m}$ o duplo somatório $\sum_{i=o}^{n}\sum_{j=o}^{m}$.

2 PRELIMINARES

Neste capítulo, estabeleceremos vários resultados que serão úteis para os resultados principais. Tomaremos a liberdade de, em alguns deles, omitirmos sua demonstração.

Definição 2.1 *Seja S um anel. Uma aplicação $d : S \to S$ é dita* ***derivação de*** *S, se para todo $a, b \in S$, d satisfaz*

$$\begin{aligned} &(i) \qquad d(a+b) = d(a) + d(b) \\ &(ii) \qquad d(ab) = d(a)b + ad(b), \end{aligned}$$

Proposição 2.2 *A soma de derivações de um anel S é uma derivação.*

Prova. Sejam d_1, d_2 derivações em S.

É claro que $d_1 + d_2$ preserva a soma. Ainda, para $a, b \in S$, temos

$$\begin{aligned} (d_1 + d_2)(ab) &= d_1(ab) + d_2(ab) \\ &= d_1(a)b + ad_1(b) + d_2(a)b + ad_2(b) \\ &= (d_1 + d_2)(a)b + a(d_1 + d_2)(b), \end{aligned}$$

e portanto $(d_1 + d_2)$ é uma derivação de S. ■

Definição 2.3 *Uma derivação d de $k[x]$ é uma* ***k-derivação*** *se $d(r) = 0$, para todo $r \in k$.*

Exemplo 2.4 *$\frac{d}{dx}$ é uma k-derivação de $k[x]$.*

Proposição 2.5 *Se d é uma derivação de um anel comutativo com unidade R , então para todo $i \in \mathbb{N}^*$, temos $d(a^i) = ia^{i-1}d(a)$ para todo $a \in R$.*

Prova. Mostraremos por indução. Para $i = 1$ temos que $d(a) = 1a^0 d(a)$.

Suponhamos que para $i \geq 1$ vale $d(a^i) = ia^{i-1}d(a)$; então

$$\begin{aligned} d(a^{i+1}) = d(aa^i) &= d(a)a^i + ad(a^i) \\ &= d(a)a^i + aia^{i-1}d(a) \\ &= (i+1)a^i d(a), \end{aligned}$$

já que R é comutativo. ■

Proposição 2.6 *Se d é uma k-derivação de $k[x]$, então $d = d(x)\dfrac{d}{dx}$.*

Prova. Seja $g(x) \in k[x]$, digamos $g(x) = \sum_{i=0}^{n} a_i x^i$, com $a_i \in k$. Então

$$\begin{aligned} d(g(x)) = d\left(\sum_{i=0}^{n} a_i x^i\right) &= \sum_{i=0}^{n} d\left(a_i x^i\right) \\ &\overset{d \text{ é } k\text{-derivação}}{=} \sum_{i=0}^{n} a_i d\left(x^i\right) \\ &\overset{\text{Proposição 2.5}}{=} \sum_{i=1}^{n} a_i i x^{i-1} d\left(x\right) \\ &= d(x)\sum_{i=1}^{n} a_i i x^{i-1} = d(x)\sum_{i=0}^{n} a_i \frac{d}{dx}\left(x^i\right) \\ &\overset{d \text{ é } k\text{-derivação}}{=} d(x)\textstyle\sum_{i=0}^{n} \dfrac{d}{dx}\left(a_i x^i\right) = d(x)\dfrac{d}{dx}\left(g(x)\right). \end{aligned}$$ ■

Proposição 2.7 *Se d é uma k-derivação de $k[x, y]$, então*

$$d = d(x)\frac{\partial}{\partial x} + d(y)\frac{\partial}{\partial y}.$$

Prova. Seja $h(x, y) \in k[x, y]$, digamos $h(x, y) = \sum_{i,l=0}^{n,l} a_{ij} x^i y^j$, com $a_{ij} \in k$, para cada i e cada j.

Então

$$
\begin{aligned}
d(h(x,y)) &= d\left(\sum_{i,j=0}^{n,l} a_{ij}x^i y^j\right) = \sum_{i,j=0}^{n,l} d(a_{ij}x^i y^j) \\
&\overset{d \text{ é } k\text{-derivação}}{=} \sum_{i,j=0}^{n,l} a_{ij} d(x^i y^j) \\
&= \sum_{i,j=0}^{n,l} a_{ij}(d(x^i)y^j + x^i d(y^j)) \\
&\overset{\text{Proposição 2.5}}{=} \sum_{i,j=1}^{n,l} a_{ij}(ix^{i-1}d(x)y^j + x^i j y^{j-1} d(y)) \\
&= \sum_{i,j=0}^{n,l} a_{ij}(d(x)\frac{\partial}{\partial x}x^i y^j + x^i d(y)\frac{\partial}{\partial y}y^j) \\
&= d(x)\frac{\partial}{\partial x}\left(\sum_{i,j=0}^{n,l} a_{ij}x^i y^j\right) + d(y)\frac{\partial}{\partial y}\left(\sum_{i,j=0}^{n,l} a_{ij}x^i y^j\right) \\
&= d(x)\frac{\partial}{\partial x}h(x,y) + d(y)\frac{\partial}{\partial y}h(x,y). \quad \blacksquare
\end{aligned}
$$

Observação 2.8 *O resultado acima pode ser generalizado para $k[x_1, ..., x_n]$. Maiores detalhes podem ser encontrados em [7].*

Definição 2.9 *Seja d uma derivação de um anel comutativo R. Um ideal I de R é um d-**ideal** se $d(I) \subseteq I$. Dizemos que R é d-**simples** ou que d é uma **derivação simples de** R, se R não contém d-ideais além dos triviais $\{0\}$ e R.*

Proposição 2.10 *Seja I um ideal de um anel comutativo R, gerado pelos elementos $g_1, ..., g_s$ e seja d uma derivação de R. Então I é um d-ideal se, e somente se, $d(g_i) \in I$, para todo $i = 1, ..., s$.*

Prova. Se I é um d-ideal então obviamente $d(g_i) \in I$, para todo $i = 1, ..., s$. Agora suponhamos que $d(g_i) \in I$ para todo i. Daí, para todo

$g \in I$, digamos $g = \sum_{i=1}^{n} r_i g_i$, com $r_i \in R$, temos

$$\begin{aligned} d(g) &= d\left(\sum_{i=1}^{n} r_i g_i\right) = \sum_{i=1}^{n} d(r_i g_i) \\ &= \sum_{i=1}^{n} (d(r_i) g_i + r_i d(g_i)) \\ &= \sum_{i=1}^{n} d(r_i) g_i + \sum_{i=1}^{n} r_i d(g_i) \in I, \end{aligned}$$

pois $d(g_i) \in I$, para todo i, por hipótese. ■

Proposição 2.11 *Seja d uma k-derivação não nula de $k[x]$. Então d é uma k-derivação simples se, e só se, $d(x) \in k^*$. Em outras palavras as únicas k-derivações simples de $k[x]$ são da forma $d = c\dfrac{d}{dx}$, com $c \in k^*$.*

Prova. ($\Rightarrow$) Seja d uma k-derivação simples não nula. Pela proposição 2.6 temos que $d = d(x)\dfrac{d}{dx}$, mas sendo d não nula, temos necessariamente $d(x) \neq 0$ e conseqüentemente *grau* $d(x) \geq 0$. Suponhamos por absurdo que *grau* $d(x) \geq 1$.

Ora, para todo $h \in k[x]$, $d(h) = d(x)\dfrac{dh}{dx} \in d(x)k[x]$; então o ideal $I = d(x)k[x]$ gerado por $d(x)$ é um d-ideal de $k[x]$.

Mas *grau* $(d(h))$ = *grau* $(d(x)\dfrac{dh}{dx})$ = *grau* $d(x)$ + *grau* $\dfrac{dh}{dx} \geq 1$, para todo $h \in k[x]$; daí, para todo $r \in k^*$, temos $r \notin I$. Portanto I é um d-ideal próprio de $k[x]$, absurdo.

($\Leftarrow$) Sejam $d = c\dfrac{d}{dx}$, $c \in k^*$e I um d-ideal não-nulo de $k[x]$. A mostrar $I = k[x]$.

Sendo $k[x]$ um domínio principal, existe $g(x) \in k[x]$, tal que $I = (g(x))$ e como I é não nulo temos *grau* $g(x) \geq 0$.

Suponhamos, por absurdo, que $grau\ g(x) = n$, $n \geq 1$. Como I é d-ideal temos $d(g(x)) \in I$. Mas ,

$$grau\ d(g(x)) = grau\ \left(c\frac{dg}{dx}\right) = grau\ c + grau\ g'(x) = grau\ g'(x) = n - 1.$$

Por outro lado, como $d(g(x)) \in I$, existe $h(x) \in k[x]$ tal que $d(g(x)) = g(x)h(x)$, logo $grau\ d(g(x)) \geq grau\ g(x) = n$, o que é um absurdo.

Portanto $grau\ g(x) = 0$ e conseqüentemente $I = (g(x)) = k[x]$, donde concluímos que d é simples. ■

Queremos agora falar sobre extensões de derivações. Para isto, relembramos dois resultados sobre extesões de corpos.

Proposição 2.12 *Seja L uma extensão algébrica do corpo k. Dado $l \in L$, seja*

$$n = \min\{grau\ f(x) \mid f(x) \in k[x]\backslash\{0\} \quad e \quad f(l) = 0\}.$$

Se $p(x) \in k[x]$ é tal que $p(l) = 0$ então $grau\ p(x) = n$ se e somente se $p(x)$ é irredutível.

Proposição 2.13 *Sejam L uma extensão algébrica de k e $l \in L$. Então $k[l]$ é um corpo.*

Notação 2.14 *Se d é uma derivação de k e $f(x) \in k[x]$, então denotaremos por $f^d(x)$ o polinômio obtido aplicando d a todos os coeficientes de f. Ou seja: se $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ então*

$$f^d(x) = d(a_n)x^n + d(a_{n-1})x^{n-1} + ... + d(a_1)x + d(a_0).$$

Proposição 2.15 *Sejam $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in k[x]$ e $d : k \longrightarrow k$, uma derivação de k. Então a aplicação $\Lambda^d : k[x] \longrightarrow k[x]$, dada por*

$$\Lambda^d(f(x)) = d(a_n)x^n + d(a_{n-1})x^{n-1} + ... + d(a_1)x + d(a_0) = f^d(x)$$

é uma derivação de $k[x]$ que estende d.

Prova. É claro que Λ^d estende d. Sejam $f(x), g(x) \in k[x]$, tais que

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

e

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0,$$

sem que m e n sejam necessariamente seus graus. Assim, podemos supor $n = m$.

É fácil ver que $\Lambda^d(f(x) + g(x)) = f^d(x) + g^d(x)$.

Afirmamos que $\Lambda^d(f(x)g(x)) = \Lambda^d(f(x))g(x) + f(x)\Lambda^d(g(x))$. De fato,

$$\begin{aligned}
\Lambda^d(f(x)g(x)) &= \Lambda^d(\sum_{i,j=o}^{n,m} a_i b_j x^{i+j}) \\
&= \sum_{i,j=o}^{n,m} d(a_i b_j)x^{i+j} \\
&= \sum_{i,j=o}^{n,m} (d(a_i)b_j + a_i d(b_j))x^{i+j} \\
&= \sum_{i,j=o}^{n,m} d(a_i)b_j x^{i+j} + \sum_{i,j=o}^{n,m} a_i d(b_j)x^{i+j} \\
&= \sum_{i,j=o}^{n,m} d(a_i)x^i b_j x^j + \sum_{i,j=o}^{n,m} a_i x^i d(b_j)x^j \\
&= f^d(x)g(x) + f(x)g^d(x) \\
&= \Lambda^d(f(x))g(x) + f(x)\Lambda^d(g(x)).
\end{aligned}$$

Logo, Λ^d é uma derivação de $k[x]$. ■

Teorema 2.16 *Sejam d uma derivação de k e α um elemento algébrico sobre k. Então existe uma única derivação d^* do corpo $k[\alpha]$ que estende d (isto é, tal que $d^*|_k = d$). Tal derivação é induzida por $d^*(\alpha) = -\dfrac{p^d(\alpha)}{p'(\alpha)}$, onde $p(x)$ é o polinômio mínimo de α em $k[x]$.*

Prova. Suponhamos que $grau\ p(x) = n$, digamos,

$$p(x) = x^n + b_{n-1}x^{n-1} + ... + b_1x + b_0.$$

Se existir uma derivação d^* de $k[\alpha]$ tal que $d^*|_k = d$, então deveremos ter, pondo $b_n = 1$ e lembrando que $p(\alpha) = 0$,

$$\begin{aligned}
0 &= d^*(0) \\
&= d^*\left(\sum_{i=0}^{n} b_i\alpha^i\right) = \sum_{i=0}^{n} d^*(b_i\alpha^i) \\
&= \sum_{i=0}^{n} d^*(b_i)\alpha^i + \sum_{i=0}^{n} b_i d^*(\alpha^i) \\
&= \sum_{i=0}^{n} d^*(b_i)\alpha^i + \sum_{i=0}^{n} b_i i\alpha^{i-1} d^*(\alpha) \\
&\overset{d^*|_k=d}{=} \sum_{i=0}^{n} d(b_i)\alpha^i + d^*(\alpha)\sum_{i=0}^{n} b_i i\alpha^{i-1} \\
&= p^d(\alpha) + d^*(\alpha)p'(\alpha).
\end{aligned}$$

Pelo caráter minimal de n, temos $p'(\alpha) \neq 0$, e conseqüentemente

$$d^*(\alpha) = -\frac{p^d(\alpha)}{p'(\alpha)}. \tag{1}$$

Ou seja: se existir uma derivação de $k[\alpha]$ estendendo d então necessariamente ela deverá ser induzida por (1).

Sendo α algébrico sobre k, sabemos que $\{1, \alpha, ..., \alpha^{n-1}\}$ é base do $k-$espaço vetorial $k[\alpha]$ e, para todo $\beta \in k[\alpha]$, existe um único $f(x) \in k[x]$, com $grau\ f(x) \leq n-1$ e tal que $\beta = f(\alpha)$.

Definimos então, para tal $\beta \in k[\alpha]$ e tal $f(x) \in k[x]$,

$$d^*(\beta) = f^d(\alpha) + f'(\alpha)d^*(\alpha).$$

Afirmamos d^* é derivação.

Dados $\beta, \gamma \in k[\alpha]$, sejam $f(x), g(x) \in k[x]$, tais que $grau\ f < n$, $grau\ g < n$, $\beta = f(\alpha)$ e $\gamma = g(\alpha)$.

Daí:

$$\begin{aligned} d^*(\beta+\gamma) &= (f+g)^d(\alpha) + (f+g)'(\alpha)d^*(\alpha) = \\ &= (f^d(\alpha) + g^d(\alpha)) + [f'(\alpha) + g'(\alpha)]d^*(\alpha) \\ &= f^d(\alpha) + f'(\alpha)d^*(\alpha) + g^d(\alpha) + g'(\alpha)d^*(\alpha) = d^*(\beta) + d^*(\gamma). \end{aligned}$$

Falta-nos mostrar que $d^*(\beta\gamma) = d^*(\beta)\gamma + \beta d^*(\gamma)$, e para tal precisamos saber quem é o polinômio de $grau$ menor do que n que reproduz $\beta\gamma$ quando avaliado em α. Afirmamos que tal polinômio é o resto da divisão de $f(x)g(x)$ pelo polinômio minimal $p(x)$. De fato, pelo algoritmo da divisão euclidiana em $k[x]$, existem únicos $h(x)$ e $r(x)$ tais que

$$f(x)g(x) = p(x)h(x) + r(x), \tag{2}$$

com $r(x) = 0$ ou $grau\ r < grau\ p = n$.

Assim temos

$$\beta\gamma = f(\alpha)g(\alpha) = p(\alpha)h(\alpha) + r(\alpha) \overset{p(\alpha)=0}{=} r(\alpha),$$

logo $\beta\gamma = r(\alpha)$ e $r(x)$ é o único polinômio de $k[x]$ de $grau$ menor que n tal que $\beta\gamma = r(\alpha)$.

Daí:

$$\begin{aligned} & d^*(\beta)\gamma + \beta d^*(\gamma) \\ &= \left[f^d(\alpha) + f'(\alpha)d^*(\alpha)\right] g(\alpha) + f(\alpha)\left[(g^d(\alpha) + g'(\alpha)d^*(\alpha)\right] \\ &= f^d(\alpha)g(\alpha) + f(\alpha)g^d(\alpha) + [f'(\alpha)g(\alpha) + f(\alpha)g'(\alpha)]d^*(\alpha) \\ &\overset{\text{Prop. 2.15}}{=} [f(x)g(x)]^d(\alpha) + [f(x)g(x)]'(\alpha)d^*(\alpha) \end{aligned}$$

$$\overset{(2)}{=} [p(x)h(x)]^d(\alpha) + r^d(\alpha) + [p(x)h(x)]'(\alpha)d^*(\alpha) + r'(\alpha)d^*(\alpha)$$

$$\overset{\text{Prop. 2.15}}{=} p^d(\alpha)h(\alpha) + p(\alpha)h^d(\alpha) + p'(\alpha)h(\alpha)d^*(\alpha) + p(\alpha)h'(\alpha)d^*(\alpha) + r^d(\alpha) + r'(\alpha)d^*(\alpha)$$

$$\overset{p(\alpha)=0}{=} [p^d(\alpha) + p'(\alpha)d^*(\alpha)]h(\alpha) + r^d(\alpha) + r'(\alpha)d^*(\alpha)$$

$$= 0.h(\alpha) + d^*(\beta\gamma) = d^*(\beta\gamma).$$

Concluímos então que d^* é uma derivação.

Pela unicidade de $r(x)$ temos que d^* é a única derivação de $k[\alpha]$ tal que $d^* \mid_k = d$ e é dada por $d^*(\alpha) = -\dfrac{p^d(\alpha)}{p'(\alpha)}$. ■

Corolário 2.17 *Sejam d uma derivação de k e L uma extensão algébrica de k. Existe uma única extensão de d a uma derivação de L.*

Prova. Vamos aqui aplicar o lema de Zorn à família

$$\mathcal{F} = \{(U, \widetilde{d}) \mid U \text{ corpo, } k \subseteq U \subseteq L, \ \widetilde{d} \text{ é uma derivação de } U \text{ que estende } d\}.$$

Pelo teorema anterior, $\mathcal{F}$ é não vazio. Definimos em $\mathcal{F}$ a seguinte ordem parcial: dados $(U, \widetilde{d})$ e $(U_1, \widetilde{d_1}) \in \mathcal{F}$,

$$(U, \widetilde{d}) \leq (U_1, \widetilde{d_1}) \overset{\text{def.}}{\Leftrightarrow} U \subseteq U_1 \text{ e } \widetilde{d_1} \mid_U = \widetilde{d}.$$

Seja $\mathcal{F}'$ um subconjunto totalmente ordenado de $\mathcal{F}$. Queremos mostrar que existe $(\bar{A}, \bar{d}) \in \mathcal{F}$ tal que $(A', d') \leq (\bar{A}, \bar{d})$, para qualquer $(A', d') \in \mathcal{F}'$.

Seja

$$\bar{A} = \cup_{(A',d') \in \mathcal{F}'} A'.$$

Como $\mathcal{F}'$ é totalmente ordenado, é fácil ver que $\bar{A}$ é corpo. Além disso, $k \subseteq \bar{A} \subseteq L$.

Definimos $\bar{d} : \bar{A} \longrightarrow \bar{A}$ da seguinte maneira: pela definição de $\bar{A}$, dado $\bar{a} \in \bar{A}$, existe $(A', d') \in \mathcal{F}'$ tal que $\bar{a} \in A'$. Então definimos $\bar{d}(\bar{a}) = d'(\bar{a})$.

Notemos que $\bar{d}$ está bem definido, pois se $\bar{a} \in A'$ e $\bar{a} \in A''$, com (A', d'), $(A'', d'') \in \mathcal{F}'$, sendo $\mathcal{F}'$ totalmente ordenado temos $(A', d') \leq (A'', d'')$ ou $(A', d') \geq (A'', d'')$. Em qualquer caso, temos $d'(\bar{a}) = d''(\bar{a})$. Podemos então dizer que $\bar{d}|_{A'} = d'$. Em particular, $\bar{d}$ estende d.

Afirmamos que $\bar{d}$ é uma derivação de $\bar{A}$ que estende d.

De fato, sejam $\bar{a}, \bar{b} \in \bar{A}$. Como $\bar{A} = \cup_{(A',d') \in \mathcal{F}'} A'$ sabemos que existem (A', d'), $(A'', d'') \in \mathcal{F}'$ tais que $\bar{a} \in A'$ e $\bar{b} \in A''$. Sabemos também que $(A', d') \leq (A'', d'')$ ou $(A', d') \geq (A'', d'')$. Supondo, sem perda de generalidade, que $(A', d') \leq (A'', d'')$, temos que

$$\bar{d}(\bar{a}) = d'(\bar{a}) = d''(\bar{a}) \;\; e \;\; \bar{d}(\bar{b}) = d''(\bar{b}),$$

Ainda, como $\bar{a} + \bar{b} \in A''$ e $\bar{a}\bar{b} \in A''$, temos que

$$\bar{d}(\bar{a} + \bar{b}) = d''(\bar{a} + \bar{b}) = d''(\bar{a}) + d''(\bar{a}) = \bar{d}(\bar{a}) + \bar{d}(\bar{b})$$

e

$$\bar{d}(\bar{a}\bar{b}) = d''(\bar{a}\bar{b}) = d''(\bar{a})\bar{b} + \bar{a}d''(\bar{b}) = \bar{d}(\bar{a})\bar{b} + \bar{a}\bar{d}(\bar{b})$$

Conseqüentemente temos que $(\bar{A}, \bar{d}) \in \mathcal{F}$. Ainda, como $A' \subseteq \bar{A}$, $\bar{d}\,|_{A'} = d'$ e $(A', d') \leq (\bar{A}, \bar{d})$ para todo $(A', d') \in \mathcal{F}'$, conclui-se que $(\bar{A}, \bar{d})$ é cota superior para $\mathcal{F}'$.

Mostramos assim que $\mathcal{F}$ é um sistema indutivo. Portanto, pelo Lema de Zorn, existe $(\bar{U}, \hat{d})$ elemento máximo em $\mathcal{F}$.

Afirmamos que $\bar{U} = L$. Ora, se $\bar{U} \subsetneq L$ então existe $l \in L \backslash \bar{U}$ e $\bar{U}[l]$ é uma extensão algébrica de $\bar{U}$. Pelo teorema anterior, existe uma derivação $\widetilde{d_l}$ de $\bar{U}[l]$ estendendo $\hat{d}$, tal que $\bar{U} \subset \bar{U}[l]$ e $\widetilde{d_l}\,|_{\bar{U}} = \hat{d}$, o que é um absurdo, pois $(\bar{U}, \hat{d})$ é elemento máximo de F. Logo, $\bar{U} = L$.

Como $\hat{d}$ é extensão de todas as outras derivações, é fácil ver que é única, e isto completa a prova. ■

Teorema 2.18 *Sejam R um domínio e d uma derivação de R. Então existe uma única extensão de d a uma derivação no corpo de frações de R, a saber: para cada $\frac{u}{v} \in cfR$,*

$$\widetilde{d} : cfR \longrightarrow cfR, \quad \widetilde{d}\left(\frac{u}{v}\right) = \frac{d(u)v - ud(b)}{v^2}. \tag{3}$$

Prova. Mostraremos primeiramente que $\widetilde{d}$ definida por (3) é uma derivação. Dados $\frac{x}{y}, \frac{u}{v} \in cfR$, temos que

$$\widetilde{d}\left(\frac{x}{y} + \frac{u}{v}\right) = \widetilde{d}\left(\frac{xv + yu}{yv}\right) = \frac{d(xv + yu)yv - (xv + yu)d(yv)}{(yv)^2}$$

$$= \frac{(d(x)v + xd(v) + d(y)u + yd(u))yv - xvd(yv) - yud(yv)}{y^2v^2}$$

$$= \frac{d(x)vyv + xd(v)yv + d(y)yv + yd(u)yv}{y^2v^2}$$

$$+ \frac{-xvd(y)v - xvyd(v) - yud(y)v - yuyd(v)}{y^2v^2}$$

$$= \frac{d(x)v^2y - xv^2d(y) + d(u)y^2v - uy^2d(v)}{y^2v^2}$$

$$= \frac{d(x)yv^2 - xv^2d(y)}{y^2v^2} + \frac{d(u)y^2v - uy^2d(v)}{y^2v^2}$$

$$= \frac{d(x)y - xd(y)}{y^2} + \frac{d(u)v - ud(v)}{y^2v^2} = \widetilde{d}\left(\frac{x}{y}\right) + \widetilde{d}\left(\frac{u}{v}\right)$$

e

$$\widetilde{d}\left(\frac{x}{y}\frac{u}{v}\right) = \widetilde{d}\left(\frac{xu}{yv}\right) = \frac{d(xu)yv - xud(yv)}{(yv)^2}$$

$$= \frac{(d(x)u + xd(u))yv - xu(d(y)v - y(d(v))}{(yv)^2}$$

$$= \frac{d(x)uyv + xd(u)yv - xud(y)v - xuy(d(v))}{y^2v^2}$$

$$= \frac{(d(x)y - xd(y))uv}{y^2v^2} + \frac{xy(d(u)v - u(d(v))}{y^2v^2}$$

$$= \frac{(d(x)y - xd(y))}{y^2}\left(\frac{u}{v}\right) + \left(\frac{x}{y}\right)\frac{(d(u)v - u(d(v))}{v^2}$$
$$= \widetilde{d}\left(\frac{x}{y}\right)\frac{u}{v} + \frac{x}{y}\widetilde{d}\left(\frac{u}{v}\right).$$

Logo, $\widetilde{d}$ é derivação.

Agora note que, como $1 \in R$, temos que $\dfrac{u}{1} = u$, e portanto

$$\widetilde{d}\left(\frac{u}{1}\right) = \frac{d(u)1 - ud(1)}{1^2} = \frac{d(u) - u0}{1} = d(u).$$

Assim $\widetilde{d}$ é uma derivação que estende d a cfR.

Para mostrar a unicidade, suponhamos que existam derivações $\widetilde{d}$ e $\bar{d}$ no corpo de frações de R que estendem d.

Observamos que, para cada $\dfrac{u}{v} \in cfR$, como $\widetilde{d}$ estende d, temos

$$0 = \widetilde{d}(1) = \widetilde{d}(vv^{-1}) = \widetilde{d}(v)v^{-1} + v\widetilde{d}(v^{-1}) = d(v)v^{-1} + v\widetilde{d}(v^{-1}),$$

daí

$$\widetilde{d}(v^{-1}) = \frac{-d(v)}{v^2};$$

analogamente obtemos

$$\bar{d}(v^{-1}) = \frac{-d(v)}{v^2},$$

o que implica

$$\bar{d}(v^{-1}) = \widetilde{d}(v^{-1}).$$

Daí,

$$\begin{aligned}\widetilde{d}\left(\frac{u}{v}\right) &= \widetilde{d}(u)v^{-1} - u\widetilde{d}(v^{-1}) \\ &= d(u)v^{-1} - u\widetilde{d}(v^{-1}) \overset{\bar{d}(v^{-1})=\widetilde{d}(v^{-1})}{=} \\ &= \bar{d}(u)v^{-1} - u\bar{d}(v^{-1}) = \bar{d}(\frac{u}{v}),\end{aligned}$$

portanto $\widetilde{d} = \bar{d}$. ■

Corolário 2.19 *Sejam R um domínio e P um ideal primo de R. Se $\widetilde{d}$ é a derivação de cfR que estende d, então $\widetilde{d}|_{R_P}$ é uma derivação de R_P.*

Prova. Pela proposição acima, temos que, dado $\frac{c}{s} \in R_P$,

$$\widetilde{d}\left(\frac{c}{s}\right) = \frac{d(c)s - cd(s)}{s^2} \in R_P,$$

visto que, sendo P ideal primo e $s \in R\backslash P$, tem-se $s^2 \in R\backslash P$. ■

Proposição 2.20 *Seja I um d-ideal de R. Então IR_P é um $\widetilde{d}$-ideal de R_P.*

Prova. Como $IR_P = \left\{\frac{i}{s} \mid i \in I, s \in R\backslash P\right\}$, temos que

$$\widetilde{d}\left(\frac{i}{s}\right) = \frac{d(i)s - id(s)}{s^2}.$$

Mas sendo I um d-ideal de R, obtemos que $d(i)s$, $id(s) \in I$ e conseqüentemente $d(i)s - id(s) \in I$. Assim, como $s^2 \in R\backslash P$, temos que $\widetilde{d}\left(\frac{i}{s}\right) \in IR_P$.

Logo, IR_P é um $\widetilde{d}$-ideal de R_P. ■

Antes de encerrarmos este capítulo, damos a seguir mais alguns exemplos de d-ideais que nos serão úteis neste trabalho.

Teorema 2.21 *Seja R um domínio que contém os racionais e que possui um único ideal maximal M. Se M for radical de algum d-ideal de R então M é um d-ideal.*

Prova. Suponhamos que A é um d-ideal de R tal que $\sqrt{A} = M$.

Dado $x \in M$, afirmamos que $d(x) \in M$. De fato,

$$n = \min\{t \in \mathbb{N}^* \mid x^t \in A\} \Rightarrow$$
$$x^n \in A \overset{A \text{ é } d\text{-ideal}}{\Rightarrow}$$
$$nx^{n-1}d(x) = d(x^n) \in A$$

Como $R \supseteq \mathbb{Q}$, temos que n é inversível em R, e portanto

$$nx^{n-1}d(x) \in A \Rightarrow$$
$$x^{n-1}d(x) \in A.$$

Daí note que, se $d(x) \notin M$, temos que $d(x)$ é inversível em R, visto que M é o único maximal de R; mas então $x^{n-1} \in A$, o que contraria o caráter minimal de n. Logo, concluímos que $d(x) \in M$. ■

Corolário 2.22 *Sejam R domínio que contém $\mathbb{Q}$, A um d-ideal de R e P um primo mínimo de A. Então P é d-ideal de R.*

Prova. Como A d-ideal de R então AR_P é $\widetilde{d}$-ideal de R_P pela Proposição 2.20.

Como P é um primo mínimo de A, o único ideal primo de R_P que contém AR_P é PR_P. Logo, $\sqrt{AR_P} = PR_P$, que sabemos ser ideal máximo de R_P. Então, pelo teorema 2.21, PR_P é um $\widetilde{d}$-ideal de R_P.

Note agora que, se $x \in P$, então $\frac{x}{1} \in PR_P$ e $\frac{d(x)}{1} = \widetilde{d}(\frac{x}{1}) \in PR_P$, e conseqüentemente $d(x) \in P$. Logo P é d-ideal. ■

3 EXTENSÃO DE UMA DERIVAÇÃO DE R A $R[t]$ E O TEOREMA DE SHAMSUDDIN

Neste capítulo, abordamos algumas maneiras de estender uma derivação de um domínio ao anel de polinômios. O Teorema de Shamsuddin nos dá condições de decidir se conseguimos manter a simplicidade. Finalmente, definimos derivações de Shamsuddin e apresentamos um critério que nos permite decidir se uma derivação de Shamsuddin é ou não simples. Encerramos então o capítulo com vários exemplos de derivações simples e não seimples.

Neste capítulo supomos que todos os domínios considerados contêm Q.

Proposição 3.1 *Sejam R um anel comutativo com unidade, t uma indeterminada sobre R e d uma derivação de R. Então podemos estender d a uma única derivação $\widetilde{d}$ do anel de polinômios $R[t]$ pondo $\widetilde{d}(t) = h(t)$, onde $h(t) \in R[t]$.*

Prova. Considere d^* uma derivação de $R[t]$ que estende d e satisfaz $d^*(t) = h(t)$.

Dado $f = \sum_{i=0}^{n} a_i t^i \in R[t]$, temos

$$d^*(f) = \sum_{i=0}^{n} d^*(a_i t^i) = \sum_{i=0}^{n} \left(d^*(a_i) t^i + a_i i t^{i-1} d^*(t) \right) \overset{d^*|_R = d}{=}$$
$$= \sum_{i=0}^{n} d(a_i) t^i + \sum_{i=1}^{n} a_i i t^{i-1} d^*(t) = f^d(t) + \frac{df}{dt} h(t).$$

Decorre daí que se existir uma derivação $\tilde{d}$ de $R[t]$ que estende d e tal que $\tilde{d}(t) = h(t)$, então ela é única e

$$\tilde{d}(f) = f^d(t) + \frac{df}{dt} h(t), \tag{4}$$

para todo $f \in R[t]$.

Resta mostrar que $\tilde{d}$ dada por (4) é de fato uma derivação. Dados $f, g \in R[t]$.

$$\begin{aligned}\tilde{d}(f+g) &= (f+g)^d(t) + \frac{d(f+g)}{dt}h(t) \overset{\text{Prop. 2.15}}{=} \\ &= f^d(t) + g^d(t) + \frac{df}{dt}h(t) + \frac{dg}{dt}h(t) = \tilde{d}(f) + \tilde{d}(g)\end{aligned}$$

Além disto

$$\begin{aligned}\tilde{d}(fg) &= (fg)^d(t) + \left(\frac{dfg}{dt}\right)h(t) \\ &= f^d(t)g + fg^d(t) + \frac{df}{dt}h(t)g + f\frac{dg}{dt}h(t) \\ &= \left(f^d(t) + \frac{df}{dt}h(t)\right)g + f\left(g^d(t) + \frac{dg}{dt}h(t)\right) \\ &= \tilde{d}(f)g + f\tilde{d}(g)\end{aligned}$$

Portanto, $\widetilde{d}$ dada por (4) é a única derivação do anel de polinômios $R[t]$ que estende d e satisfaz a condição $\widetilde{d}(t) = h(t)$ ∎

Quando $grau\ h(t) \leq 1$ podemos também preservar a simplicidade quando passamos de R a $R[t]$, como mostra o seguinte teorema:

Teorema 3.2 *([6], Teorema de Shamsuddin): Seja R um anel comutativo contendo $\mathbb{Q}$ e seja d uma derivação simples de R. Dados $a, b \in R$ estenda d a única derivação $\widetilde{d}$ do anel de polinômios $R[t]$ tal que $\widetilde{d}(t) = at + b$.*

As seguintes condições são equivalentes.

(i) $\widetilde{d}$ não é simples;

(ii) existe elemento r de R tal que $d(r) = ar + b$.

Prova. *(ii)⇒(i):* Afirmamos que o ideal gerado por $(t - r)$ é um $\widetilde{d}$-ideal próprio de $R[t]$, logo $\widetilde{d}$ não é simples. De fato,

$$\widetilde{d}(t-r) = \widetilde{d}(t) - \widetilde{d}(r) = at + b - ar - b = a(t-r) \in (t-r)R.$$

Logo, como R é por hipótese comutativo, pela proposição 2.10 temos que o ideal gerado por $t-r$ é um $\widetilde{d}$-ideal. Além disso $(t-r)R$ é $\widetilde{d}$-ideal próprio, visto que $1 \notin (t-r)R$, pois se $1 \in (t-r)R$ então existiria $u \in R[t]\backslash\{0\}$ tal que $1 = (t-r)u$; daí

$$0 = grau\ 1 = grau\ ((t-r)u) \overset{r\in R,\ u\neq 0}{=} 1 + grau\ u \geq 1.$$

Logo, $\widetilde{d}$ não é simples.

(i)⇒(ii): Seja I um $\widetilde{d}$-ideal não trivial de $R[t]$.

Afirmação 1: $I \cap R = (0)$.

Inicialmente note que $I \cap R$ é um d-ideal de R. De fato, tomando $m \in I \cap R$, temos $d(m) \in R$, pois d é derivação em R e como $m \in I \cap R$, e I é $\widetilde{d}$-ideal próprio de $R[t]$, segue que $d(m) = \widetilde{d}(m) \in I$, portanto $d(m) \in I \cap R$. Além disso, $I \cap R$ é d-ideal próprio de R, pois como I é próprio, temos $1 \notin I$ e conseqüentemente $I \cap R \neq R$. Sendo d simples concluímos que $I \cap R = (0)$.

Sejam agora

$$n = \min\{grau f\ ;\ f \in I,\ f \neq 0\}$$

e

$$\sigma(I) = \{0\} \ \cup\ \{r \in R;\ r \text{ é coeficiente líder de } f \text{ e } grau f = n\}.$$

Afirmação 2: $\sigma(I) \neq \{0\}$, $n \geq 1$ e $\sigma(I)$ é um ideal de R.

Por hipótese, I é ideal próprio; então, para qualquer $f \in I$, com $f \neq 0$ temos que $grau\ f \geq 1$ e portanto $n \geq 1$.

Seja $g \in I$ tal que $grau\ g = n$ e seja r coeficiente líder de g; então $r \neq 0$ e $r \in \sigma(I)$, portanto $\sigma(I) \neq \{0\}$.

Além disso $\sigma(I)$ é ideal de R. De fato:

- Dados $r, s \in \sigma(I)$, se r ou s é igual a zero, claramente $r + s \in \sigma(I)$. Se

forem ambos não nulos então existem $f, g \in I$, da forma

$$f = rt^n + \sum_{i=0}^{n-1} r_i t^i \quad \text{e} \quad g = st^n + \sum_{i=0}^{n-1} s_i t^i.$$

Como I é um ideal, segue que $f + g \in I$, mas

$$f + g = (r + s)t^n + \sum_{i=0}^{n-1} (r_i + s_i)t^i.$$

Se $r + s = 0$ então $r + s \in \sigma(I)$. Se $r + s \neq 0$, temos $grau\ f + g = n$ e $r + s$ é o coeficiente líder de $f + g$, e portanto $r + s \in \sigma(I)$. Assim, mostramos que, em qualquer caso, se $r, s \in \sigma(I)$ tem-se $r + s \in \sigma(I)$.

- Sejam $s \in R$ e $r \in \sigma(I)$, então existe $f \in I$ da forma

$$f = rt^n + r_{n-1}t^{n-1} + ... + r_1 t + r_0,$$

com $r_i \in R$, para $i \in \{0, 1, ..., n-1\}$; então

$$sf = srt^n + sr_{n-1}t^{n-1} + ... + sr_1 t + sr_0 \in I.$$

Daí, se $s = 0$, segue que $sr = 0$ e portanto $sr \in \sigma(I)$. Se $s \neq 0$, então $grau\ sf = n$ e sr é o coeficiente líder de sf, portanto $rs \in \sigma(I)$. Assim, mostramos que, em qualquer caso, se $s \in R$ e $r \in \sigma(I)$ tem-se $sr \in \sigma(I)$, o que conclui a prova da Afirmação 2.

Afirmação 3: $\sigma(I)$ é um d-ideal de R. Sejam $r \in \sigma(I)$, $f = \sum_{i=o}^{n} r_i t^i \in I$ tal que $grau\ f = n$ e $r_n = r$ e

$$g = \widetilde{d}(f) - naf,$$

onde a é tal que $\widetilde{d}(t) = at + b$. Como $f \in I$ e I é $\widetilde{d}$-ideal, é claro que $g \in I$. Além disso

$$\begin{aligned} g = \widetilde{d}(f) - naf &= \widetilde{d}\left(\sum_{i=0}^{n} r_i t^i\right) - na\sum_{i=0}^{n} r_i t^i \\ &= \sum_{i=0}^{n} \widetilde{d}(r_i)t^i + \sum_{i=1}^{n} r_i \widetilde{d}(t^i) - na\sum_{i=0}^{n} r_i t^i \overset{prop.\ 2.5}{=} \end{aligned}$$

$$= \sum_{i=0}^{n} d(r_i)t^i + \sum_{i=1}^{n} r_i i t^{i-1}\widetilde{d}(t) - na\sum_{i=0}^{n} r_i t^i =$$
$$= \sum_{i=0}^{n} d(r_i)t^i + \sum_{i=1}^{n} r_i i t^{i-1}(at+b) - na(\sum_{i=0}^{n} r_i t^i),$$

que tem para os coeficientes de t^n e t^{n-1} as respectivas expressões

$$d(r) + rna - nar = d(r)$$

e

$$d(r_{n-1}) + ar_{n-1}(n-1) + rnb - nar_{n-1} = rnb + d(r_{n-1}) - ar_{n-1}.$$

Se $d(r) \neq 0$, temos que $grau\ g = n$, donde concluímos que $d(r) \in \sigma(I)$ e se $d(r) = 0$ então obviamente $d(r) \in \sigma(I)$. Assim $\sigma(I)$ é um d-ideal de R.

A simplicidade de d e o fato que $\sigma(I) \neq \{0\}$ implicam que $\sigma(I) = R$. Portanto existe um polinômio mônico $p \in I$ tal que $grau\ p = n$, isto é, $p = t^n + r_{n-1}t^{n-1} + ... + r_1 t + r_0$, onde $r_{n-1}, ..., r_1, r_0 \in R$. Considere o polinômio $h = \widetilde{d}(p) - nap$, refazendo os cálculos da afirmação 3, obteremos que $h \in I$ e

$$h = d(1)t^n + [nb + d(r_{n-1}) - ar_{n-1}]t^{n-1} + s_{n-2}t^{n-2} + ... + s_1 t + s_0,$$

onde $s_{n-2}, ..., s_1, s_0 \in R$. Como $d(1) = 0$ então $h = [nb+d(r_{n-1})-ar_{n-1}]t^{n-1}+$ $s_{n-2}t^{n-2} + ... + s_1 t + s_0$.

Agora pela minimalidade de n, nós deduzimos que $h = 0$, que implica $nb+d(r_{n-1})-ar_{n-1} = 0$. Considere $l = -n^{-1}r_{n-1}$. Daí temos $nb+d(-nl)-a(-nl) = 0$. Segue que $nb - (d(n)l + nd(l)) + anl = 0$; como $d(n) = 0$, obtemos $nb - nd(l) + anl = 0$.

Ainda, como $\mathbb{Q} \subset R$, temos que $b - d(l) + al = 0$, ou seja, $d(l) = al + b$.

Assim, provamos que se d não for uma derivação simples, então existe $l \in R$ tal que $d(l) = al + b$.

Pela proposição 3.1 temos a unicidade, o que finaliza a prova. ■

Definição 3.3 *Dados $a(x), b(x) \in k[x]$, denotaremos por $D(a,b)$ a k-derivação de $k[x,y]$, definida por:*

$$\begin{cases} D(a,b)(x) = 1 \\ D(a,b)(y) = a(x)y + b(x) \end{cases},$$

que é chamada ***derivação de Shamsuddin****.*

Em outras palavras, uma derivação de Shamsuddin em $k[x,y]$ é uma derivação da forma

$$\partial_x + (a(x)y + b(x))\,\partial_y,$$

onde $a(x), b(x) \in k[x]$.

Note inicialmente que $D(a,b)|_{k[x]} = \frac{d}{dx}$, ou seja, $D(a,b)$ é uma extensão da derivação $\frac{d}{dx}$ de $k[x]$. Além disso, como $\frac{d}{dx}$ é uma k-derivação simples de $k[x]$, temos, pelo Teorema de Shamsuddin (Teorema 3.2):

Corolário 3.4 *Para cada $a, b \in k[x]$, a derivação $D(a,b)$ de $k[x,y]$ é simples se e somente se não existe $f \in k[x]$ tal que*

$$f' = af + b.$$

Prova. Basta tomar, no teorema de Shamsuddin, $R = k[x]$, $t = y$, $d = \frac{d}{dx}$ e $\widetilde{d} = D(a,b)$. ■

Nos próximos resultados, apresentamos alguns exemplos de derivações $D(a,b)$, as quais sabemos decidir se são ou não simples. Salientamos que de [3], sabe-se que a "grande maioria" das derivações de Shamsuddin são simples.

Proposição 3.5 *Dados $a, b \in k[x]$ tem-se:*

(i) $D(a,0)$ não é simples;

(ii) $D(0,b)$ não é simples;

(iii) se $b \neq 0$ *e grau* $b <$ *grau* a*, então* $D(a,b)$ *é simples;*

(iv) se $a \neq 0 \neq b$ *e grau* $b =$ *grau* a*, então* $D(a,b)$ *é simples se e somente se* $b \neq \alpha a$*, para todo* $\alpha \in k^*$*.*

Prova. *(i)* Visto que

$$D(a,0)(y) = ay + 0 = ay \in (y) = yk[x,y],$$

concluímos que o ideal gerado por y é um $D(a,0)$-ideal próprio de $k[x,y]$. Logo, $D(a,0)$ não é uma derivação simples de $k[x,y]$.

(ii) Seja h um polinômio de $k[x]$ tal que $h' = b$. Afirmamos que o ideal gerado por $y - h$ é um $D(0,b)$-ideal prórpio de $k[x,y]$. De fato,

$$D(0,b)(y-h) = D(0,b)(y) - D(0,b)(h) = b - b = 0 \in (y-h).$$

Portanto, $D(0,b)$ não é simples.

(iii) Suponhamos que $b \neq 0$, *grau* $b <$ *grau* a e que $D(a,b)$ não é simples. Então $a \neq 0$, pois *grau* $a >$ *grau* b. Ainda, sendo $D(a,b)$ não simples, temos, pelo Corolário 3.4, que existe um polinômio $f \in k[x]$ tal que

$$f' = af + b. \tag{5}$$

Se $f = 0$ teríamos $0 = f' = a0 + b = b \neq 0$, absurdo. Portanto, $f \neq 0$; mas novamente neste caso chegamos a uma contradição analisando o *grau* em (5):

$$\begin{aligned}(grau f) - 1 &= grau f' \\ &= grau(af+b) \overset{\text{grau } b<\text{grau } a \text{ e } f\neq 0}{=} grau(af) \geq \ grau f.\end{aligned}$$

(iv) Suponhamos $a \neq 0 \neq b$ e *grau* $b =$ *grau* a.

Se $b = \alpha a$ com $\alpha \in k^*$, então afirmamos que o ideal gerado por $y + \alpha$ é um $D(a, b)$-ideal próprio de $k[x, y]$. De fato,

$$\begin{aligned} D(a,b)(y+\alpha) &= D(a,b)(y) + D(a,b)(\alpha) \\ &= ay + b + 0 = ay + \alpha a = a(y+\alpha) \in (y+\alpha)k[x,y], \end{aligned}$$

e como $1 \notin (y + \alpha)k[x, y]$, então $(y + \alpha)k[x, y]$ é próprio de $k[x, y]$.

Logo, $D(a, b)$ não é uma derivação simples.

Para mostrar a recíproca, suponhamos que $D(a, b)$ não é simples. Pelo Corolário 3.4, existe $f \in k[x]$ tal que

$$f' = af + b.$$

Inicialmente, afirmamos que $f \in k^*$. De fato, se $grau\ f \geq 1$, então obtemos uma contradição analisando o $grau$ nesta última igualdade:

$$\begin{aligned} (grau\ f) - 1 = grau\ f' = grau\ (af+b) &\overset{grau\ b = grau\ a \text{ e } grau\ f \geq 1}{=} \\ = grau\ (af) &\geq grau\ f. \end{aligned}$$

Agora se $f = 0$ então $0 = f' = a0 + b = b$, absurdo.

Portanto, $grau\ f = 0$, ou seja, $f \in k^*$. Daí $0 = f' = af + b$, isto é, $b = (-f)a$, ou seja, $b = \alpha a$ com $\alpha \in k^*$, a saber, $\alpha = -f$. ■

A partir do conhecimento de derivações não simples, podemos ainda gerar outras derivações não simples:

Proposição 3.6 *Sejam $a, b, b_1, b_2 \in k[x]$ e $\alpha \in k$. Então:*

(i) Se $D(a, b_1)$ e $D(a, b_2)$ não são simples então $D(a, b_1+b_2)$ não é simples

(ii) Se $D(a, b)$ não é simples então $D(a, \alpha b)$ não é simples.

Prova. Se $D(a, b_1)$, $D(a, b_2)$ e $D(a, b)$ não são simples então, pelo Corolário 3.4, existem $f_1,\ f_2,\ f$ polinômios de $k[x]$ tais que

$$f_1' = af_1 + b_1, \quad f_2' = af_2 + b_2 \quad \text{e} \quad f' = af + b.$$

Então

$$(f_1 + f_2)' = f_1' + f_2' = af_1 + b_1 + af_2 + b_2 = a(f_1 + f_2) + (b_1 + b_2)$$

e

$$(\alpha f)' = \alpha f' = \alpha(af + b) = a(\alpha f) + \alpha b.$$

Como $(f_1 + f_2),\ ab,\ af,\ b_1 + b_2 \in k[x]$ concluímos, pelo Corolário 3.4, que $D(a, b_1 + b_2)$ e $D(a, \alpha b)$ não são derivações simples. ■

Imediatamente da Proposição 3.5, obtemos os seguintes exemplos de k-derivações simples de $k[x, y]$.

Exemplo 3.7 *Seja $d = D(x, 1)$, isto é, $d(y) = xy + 1$. Como $1 \neq 0$ e grau $x >$ grau 1, temos, pela Proposição 3.5 (iii), que d é uma k-derivação simples de $k[x, y]$.*

Exemplo 3.8 *Seja $d = D(x^2 + x, x^2)$, isto é, $d(y) = (x^2 + x)y + x^2$. Sendo grau $(x^2 + x) =$ grau x^2 e $x^2 \neq \alpha(x^2 + x)$, para todo $\alpha \in k^*$, temos, pela Proposição 3.5 (iv), que d é uma k-derivação simples de $k[x, y]$.*

Note que, com a proposição 3.5, sabemos decidir facilmente se a derivação $D(a, b)$ é simples quando *grau* $a \geq$ *grau* b.

A próxima proposição trata do caso em que *grau* $a <$ *grau* b, e juntamente com a proposição 3.5 nos permitirá decidir quando uma derivação do tipo $D(a, b)$ é ou não simples.

Proposição 3.9 *Sejam $a, b \in k[x]$ com $a \neq 0$ e $b = ca + r$, onde $c, r \in k[x]$ e grau $r <$ grau a. Então*

$D(a, b)$ é simples se e somente se $D(a, c' + r)$ é simples.

Prova. Primeiro observe que, escrevendo $c' = ac + (-ac + c')$, temos, pelo Corolário 3.4, que $D(a, -ac + c')$ não é simples. Assim, se $D(a, b)$ não é simples, então, usando a Proposição 3.6 *(i)* temos que $D(a, b - ac + c')$ não é simples. Mas

$$b - ac + c' \overset{b=ca+r}{=} c' + r.$$

Logo, se $D(a, b)$ não é simples então $D(a, c' + r)$ não é simples.

Ainda, escrevendo $(-c)' = a(-c) + (ac - c')$, temos, pelo Corolário 3.4, que $D(a, ac - c')$ não é simples. Assim, se $D(a, c' + r)$ não é simples então, usando a Proposição 3.6 *(i)*, temos que $D(a, c' + r + ac - c') = D(a, ac + r) = D(a, b)$ não é simples. ■

Observação 3.10 *As Proposições 3.5 e 3.9 nos fornecem um algoritmo eficiente para decidir se uma derivação é ou não simples:*

1) se grau $b <$ grau a então $D(a, b)$ é simples se e só se $b \neq 0$ (veja Proposição 3.5 (i) e (iii));

2) se grau $b =$ grau a, $D(a, b)$ é simples se e só se $b \neq \alpha a$, para todo $\alpha \in k^*$;

3) se grau $b >$ grau a, efetua-se a divisão euclidiana de b por a e obtém-se

$$b = u_1 a + r_1 \text{ com grau } r_1 < \text{grau } a.$$

Como grau $b >$ grau a e grau $r_1 <$ grau a, temos

$$\text{grau } b = \text{grau } (u_1 a) = \text{grau } u_1 + \text{grau } a.$$

Logo grau $u_1 \leq$ grau b; daí

$$\text{grau } u_1' < \text{grau } u_1 \leq \text{grau } b.$$

Como grau $r_1 <$ grau $a <$ grau b, temos grau $(u_1' + r_1) <$ grau b.

Se grau $(u_1' + r_1) > grau\ a$, *efetua-se novamente a divisão euclidiana e obtém-se*

$$u_1' + r_1 = u_2 a + r_2 \text{ com } grau\ r_2 < grau\ a;$$

como anteriormente, obtemos

$$grau(u_2' + r_2) < grau(u_1' + r_1) < graub.$$

Desta maneira existirá um natural n *tal que*

$$grau(u_n' + r_n) > grau\ a \text{ e } u_n' + r_n = u_{n+1}a + r_{n+1},$$

com grau $(u_{n+1}' + r_{n+1}) \leq grau\ a$. *Aplicando a Proposição 3.9 sucessiva vezes obtemos*

$D(a,b)$ *é simples* $\Longleftrightarrow D(a, u_1' + r_1)$ *é simples* $\Longleftrightarrow ... \Longleftrightarrow D(a, u_n' + r_n)$ *é simples* $\Longleftrightarrow D(a, u_{n+1}' + r_{n+1})$ *é simples.*

Como grau $(u_{n+1}' + r_{n+1}) \leq grau\ a$, *sabemos decidir por 1) ou 2) se* $D(a, u_{n+1}' + r_{n+1})$ *é ou não simples, portanto sabemos decidir se* $D(a,b)$ *é ou não simples.*

Exemplo 3.11 *Vamos aplicar o algoritmo acima para decidir se* $D(a,b)$ *onde* $a = x^3 + 1$ *e* $b = x^8 + 3x^5 + 1$ *é ou não simples. Efetuando a divisão euclidiana temos:*

$$b = (x^3 + 1)(x^5 + 2x^2) - 2x^2 + 1,$$

de modo que,

$$u_1 = x^5 + 2x^2 \text{ e } r_1 = -2x^2 + 1.$$

Como $u_1' + r_1 = 5x^4 - 2x^2 + 4x + 1$ *tem grau maior que* $a = x^3 + 1$, *efetua-se a divisão euclidiana de* $u_1' + r_1$ *por* a, *encontrando*

$$u_2 = 5x \quad e \quad r_2 = -2x^2 - x + 1.$$

Como $u_2' + r_2 = -2x^2 - x + 6$ *tem grau menor que grau a, o processo pára e temos*

$$D(x^3+1, x^8+3x^5+1) \text{ é simples} \Longleftrightarrow D(x^3+1, -2x^2-x+6) \text{ é simples.}$$

Como grau $(-2x^2-x+6) = 2 <$ *grau* (x^3+1) *e* $-2x^2-x+6 \neq 0$, *concluímos que* $D(x^3+1, -2x^2-x+6)$ *é simples, e portanto* $D(x^3+1, x^8+3x^5+1)$ *é simples.*

Exemplo 3.12 *Apliquemos novamente o algoritmo para decidir se a derivação* $D(x, x^3+1)$ *é ou não simples.*

Aplicando a divisão euclidiana temos

$$x^3 + 1 = xx^2 + 1,$$

de modo que

$$u_1 = x^2 e r_1 = 1.$$

Como $u_1' + r_1 = 2x + 1$ *e grau* $(2x+1) =$ *grau a, o processo pára e temos*

$$D(x, x^3+1) \text{ é simples} \Longleftrightarrow D(x, 2x+1) \text{ é simples.}$$

Pela Proposição 3.5 (iii) $D(x, 2x+1)$ *é simples, pois* $2x+1 \neq \alpha x$, *para todo* $\alpha \in k^*$, *e conseqüentemente* $D(x, x^3+1)$ *é simples.*

A próxima proposição decorre diretamente do algoritmo explicitado na Observação 3.10:

Proposição 3.13 *Seja* $n \in \mathbb{N}$. *A derivação* $D(x, x^n)$ *é simples se e somente se* n *é par.*

Prova. Aplicando a $D(x, x^n)$ o algoritmo descrito na Observação 3.10, obtemos

$$x^n = xx^{n-1} + 0$$
$$(n-1)x^{n-2} = x((n-1)x^{n-3}) + 0$$
$$(n-3)(n-1)x^{n-4} = x((n-3)(n-1)x^{n-5}) + 0$$
$$...$$

Observe que os polinômios que estão à esquerda de cada igualdade terão graus pares, se n for par e terão graus ímpares se n for ímpar.

Pelo algoritmo, devemos efetuar a divisão euclidiana até obter pela primeira vez à esquerda da igualdade, um polinômio $t(x)$ tal que $grau\ (t(x)) \leq grau\ x = 1$. Sabemos que $D(x, x^n)$ é simples se e somente se $D(x, t(x))$ é simples. Daí:

($\Leftarrow$) Se $n = 2p$, a primeira vez que teremos $grau\ (t(x)) \leq 1$ no lado esquerdo da igualdade será na $(p+1)$-ésima igualdade, quando teremos $grau\ (t(x)) = 0$ e

$$t(x) = (2p - (2p-1))...(2p-3)(2p-1)x^{2p-2p} = 1.3.5....(2p-1).$$

Como $1.3.5....(2p-1) \neq 0$, pela Proposição 3.5 *(iii)*, $D(x, 1.3.5....(2p-1))$ é simples. Logo, $D(x, x^n)$ é simples.

($\Rightarrow$) Se $n = 2p+1$ a primeira vez que teremos $t(x)$ tal que $grau\ (t(x)) \leq grau\ x = 1$, no lado esquerdo da igualdade, ocorrerá na $(p+1)$-ésima igualdade, quando teremos $grau\ (t(x)) = 1$ e

$$t(x) = (2p+1-(2p-1))...(2p+1-3)(2p+1-1)x = 2.4.6....(2p)x.$$

Pela Proposição 3.5 *(iv)*, $D(x, 2.4....(2p)x)$ não é simples, logo $D(x, x^n)$ não é simples. ■

Proposição 3.14 *Seja $a \in k[x], a \neq 0$. Então para todo $b \in k[x]$, existe um único $r \in k[x]$ com grau $r <$ grau a e tal que $D(a, b-r)$ não é simples.*

Prova. Se *grau* $b <$ *grau* a então a resposta já está dada pela Proposição 3.5*(iii)*: $D(a, b-r)$ não é simples se e só se $r = b$.

Se *grau* $b =$ *grau* a pela divisão euclidiana temos

$$b = u_1 a + r,$$

com *grau* $r <$ *grau* a e $u_1 \in k^*$. Segue que $b - r = u_1 a$, logo pela Proposição 3.5 *(iv)*, $D(a, b-r)$ não é simples.

Se *grau* $b >$ *grau* a, sendo $a \neq 0$, temos a seguinte seqüência de igualdades, provenientes da divisão euclidiana por a:

$$\begin{cases} b = u_1 a + r_1 \\ u_1' + r_1 = u_2 a + r_2 \\ u_2' + r_2 = u_3 a + r_3 \\ .... \end{cases} \tag{6}$$

Como já foi observado *grau* $b >$ *grau*$(u_1' + r_1) >$ *grau*$(u_2' + r_2) >$ ..., portanto existe $n \in \mathbb{N}^*$ tal que *grau* $(u_n' + r_n) <$ *grau* a, quando então

$$u_n' + r_n = 0.a + r_{n+1}.$$

Somando as $n+1$ igualdades em (6) termo a termo, obtemos

$$b + (u_1 + u_2 + ... + u_n)' + r_1 + r_2 + ... + r_n = a(u_1 + u_2 + ... + u_n) + r_1 + r_2 + ... + r_{n+1},$$

ou ainda, denotandos r_{n+1} por r e $u_1 + u_2 + ... + u_n$ por u,

$$b + u' = au + r,$$

donde

$$b - r = au - u'.$$

Logo, $D(a, b-r) = D(a, au-u')$.

Note agora que $-u \in k[x]$ e

$$\begin{aligned}(-u)' &= b - r - au \\ &= a(-u) + (au - u').\end{aligned}$$

Então $D(a, au-u')$ não é simples, pelo Corolário 3.4. Mas então $D(a, b-r) = D(a, au-u')$ também não é simples.

Mostraremos agora a unicidade do polinômio r. Sejam $s_1, s_2 \in k[x]$ tais que $grau\ s_1 < grau\ a$, $grau\ s_2 < grau\ a$ e que $D(a, b-s_1)$ e $D(a, b-s_2)$ não são simples. Como $D(a, b-s_1)$ não é simples então $D(a, -b+s_1)$ não é simples, pela Proposição 3.6 *(ii)*. Segue da Proposição 3.6*(i)* que $D(a, -b+s_1+b-s_2) = D(a, s_1-s_2)$ não é simples. Mas $grau\ (s_1-s_2) < grau\ a$; deste modo, pela Proposição 3.5*(iii)*, $s_1 - s_2 = 0$, isto é, $s_1 = s_2$. ■

4 POLINÔMIOS DE DARBOUX E SOLUÇÕES ALGÉBRICAS DE EQUAÇÕES DIFERENCIAIS

O objetivo deste capítulo é definir polinômios de Darboux de derivações de $k[x, y]$ e relacioná-los com soluções algébricas de certas equações diferenciais parciais de primeira ordem com coeficientes em $k(x)$.

Definição 4.1 *Um polinômio $f \in k[x_1, ..., x_n]$ é dito um polinômio de Darboux de uma derivação d de $k[x_1, ..., x_n]$ se $f \notin k$ e $d(f) = \lambda f$, para algum $\lambda \in k[x_1, ..., x_n]$.*

Proposição 4.2 *Um polinômio $f \in k[x_1, x_2, ..., x_n]$ é um polinômio de Darboux de uma derivação d de $k[x_1, ..., x_n]$ se e só se $fk[x_1, x_2, ..., x_n]$ é um d-ideal próprio de $k[x_1, ..., x_n]$.*

Prova. Observe que $f \notin k$, se e só se $\{0\} \neq fk[x_1, ..., x_n] \neq k[x_1, ..., x_n]$.

O restante da prova é imediata, a partir da Proposição 2.10 e da definição acima. ■

Corolário 4.3 *Nenhuma derivação simples de $k[x, y]$ admite polinômio de Darboux.*

Antes de analisarmos a recíproca deste corolário, salientamos a seguinte propriedade dos polinômios de Darboux:

Proposição 4.4 *Seja f um polinômio de Darboux de uma derivação d de $k[x, y]$.*

i) Se $f = gh$, com $g, h \in k[x, y]\backslash k$ e $\mathsf{mdc}(g, h) = 1$, então g e h são polinômios de Darboux para d.

ii) Se $f = p_1^{r_1} p_2^{r_2} .... p_t^{r_t}$, *onde* $r_i \in \mathbb{N}^*$ *e* p_i *é irredutível para todo* $i \in \{1, ..., t\}$, *então*

a) cada $p_i^{r_i}$ *é polinômio de Darboux para* d*;*

b) cada p_i *é um polinômio de Darboux para* d*.*

Prova. *i)* Seja $\lambda \in k[x, y]$ tal que $d(f) = \lambda f$. Então

$$\lambda gh = \lambda f = d(f) = d(gh) = d(g)h + gd(h),$$

donde

$$\begin{aligned} d(g)h &= \lambda gh - gd(h) \\ &= g(\lambda h - d(h)). \end{aligned}$$

Daí decorre que g divide $d(g)h$. Como $\mathsf{mdc}(g, h) = 1$, concluímos que g divide $d(g)$, ou seja, $d(g) = \xi g$, com $\xi \in k[x, y]$. Logo g é também um polinômio de Darboux para d.

Analogamente, prova-se que h é um polinômio de Darboux de d.

ii) A parte *(a)* é imediata a partir de *(i);* para a parte *(b),* vemos, a partir de *(a),* que basta considerar o caso $f = h^n$, com $n \in \mathbb{N}^*$ e h irredutível.

Como h^n é polinômio de Darboux para d, existe $\lambda \in k[x, y]$ tal que $d(h^n) = \lambda h^n$; daí,

$$\lambda h^n = d(h^n) = nh^{n-1} d(h)$$

assim temos

$$nd(h) = \lambda h$$

donde

$$d(h) = n^{-1} \lambda h,$$

e portanto h é polinômio de Darboux para d. ■

O lema a seguir é provado em [5] apenas para um corpo algebricamente fechado. No entanto, o resultado vale para qualquer corpo de característica zero. Incluímos aqui então uma outra demonstração para o mesmo, que pode ser encontrada em [4] e que vale também para n variáveis. Aqui trataremos apenas o caso $n = 2$.

Lema 4.5 *Seja $d = \partial_x + \alpha_2\partial_y$ uma derivação de $k[x, y]$, onde $\alpha_2 \in k[x, y]$, e seja $p \in k[x, y]\backslash k[x]$ tal que*

$$\mu d(p) = \eta p,$$

para algum $\mu \in k[x]\backslash\{0\}$ e $\eta \in k[x, y]$. Então, existem $\widetilde{p} \in k[x, y]\backslash k[x]$ e $\lambda \in k[x, y]$ tais que $d(\widetilde{p}) = \lambda\widetilde{p}$.

Prova. Escrevamos p na forma

$$\sum_{i=0}^{N} p_i y^i, \text{ onde } p_i \in k[x], \text{ para todo } i,\ N \geq 1,\ P_N \neq 0$$

Denotando por $\alpha_0 \in k[x]\backslash\{0\}$ o conteúdo[1] de p, podemos escrever

$$p = \alpha_0\widetilde{p},$$

onde $\widetilde{p} \in k[x, y]\backslash k[x]$ é primitivo em $k[x][y]$.

Por hipótese,

$$\mu d(\alpha_0\widetilde{p}) = \mu d(p) = \eta p = \eta\alpha_0\widetilde{p}, \tag{7}$$

[1]Dados um domínio fatorial D e $f(x) \in D[x]$, digamos, $f(x) = \sum_{i=0}^{n} a_i x^i$, denominamos *conteúdo de f* o máximo divisor comum dos coeficientes de f, e o denotamos por $cont(f)$.

Dizemos que $f(x) \in D[x]$ é *primitivo em $D[x]$* se $cont(f)$ é invertível em D.

Lema de Gauss: Sejam D um domínio fatorial . Então

$$cont(fg) = cont(f)cont(g),$$

para quaisquer $f(x), g(x) \in D[x]$.

onde $\mu \in k[x]\backslash\{0\}$. Daí, como também $\alpha_0 \in k[x]$, temos

$$\begin{aligned}\mu cont(d(\alpha_0\widetilde{p})) &= cont(\mu d(\alpha_0\widetilde{p}) = cont(\eta\alpha_0\widetilde{p}) \\ &\overset{\text{Lema de Gauss}}{=} \alpha_0 cont(\eta) cont(\widetilde{p}) \overset{\widetilde{p} \text{ é primitivo}}{=} \alpha_0 cont(\eta).\end{aligned}$$

Logo, μ divide $\eta\alpha_0$, digamos,

$$\eta\alpha_0 = \mu\zeta,$$

para algum $\zeta \in k[x, y]$.

Daí

$$\mu d(\alpha_0\widetilde{p}) \overset{(7)}{=} \eta\alpha_0\widetilde{p} = \mu\zeta\widetilde{p}.$$

Ainda, como $\mu \neq 0$, obtemos

$$d(\alpha_0\widetilde{p}) = \zeta\widetilde{p}.$$

Daí, como d é uma derivação,

$$\zeta\widetilde{p} = d(\alpha_0\widetilde{p}) = \alpha_0 d(\widetilde{p}) + d(\alpha_0)\widetilde{p};$$

pondo $\lambda := \zeta - d(\alpha_0) \in k[x, y]$, obtemos

$$\alpha_0 d(\widetilde{p}) = \lambda\widetilde{p}. \tag{8}$$

Repetimos então o argumento: como $\alpha_0 \in k[x]$ e $\widetilde{p}$ é primitivo, temos

$$\begin{aligned}\alpha_0 cont(d(\widetilde{p})) &= cont(\alpha_0 d(\widetilde{p})) \\ &= cont(\lambda\widetilde{p}) \overset{\text{Lema de Gauss}}{=} cont(\lambda) cont(\widetilde{p}) = cont(\lambda),\end{aligned}$$

e portanto α_0 divide λ em $k[x, y]$, digamos,

$$\lambda = \alpha_0\widetilde{\eta},$$

para algum $\widetilde{\eta} \in k[x,y]$. Daí (8) se reescreve

$$\alpha_0 d(\widetilde{p}) = \alpha_0 \widetilde{\eta}\widetilde{p},$$

e como $\alpha_0 \neq 0$, obtemos

$$d(\widetilde{p}) = \widetilde{\eta}\widetilde{p},$$

o que completa prova. ■

Teorema 4.6 *Seja* $d = \partial_x + \alpha_2 \partial_y$ *uma* k*-derivação de* $k[x,y]$ *onde* $\alpha_2 \in k[x,y]$. *Então*

a) as seguintes condições são equivalentes:

i) d *não é simples;*

ii) d *tem um polinômio de Darboux;*

iii) d *tem um polinômio de Darboux irredutível.*

b) Se d *não é simples então*

i) todo polinômio de Darboux f *de* d *satisfaz* $grau_y\ f \geq 1$;

ii) existe, a menos de multiplicação por um elemento de k^*, *um único polinômio de Darboux irredutível e mônico de* d.

Prova. *a) (i)*$\Longrightarrow$*(ii):* Se $k[x,y]$ não é d-simples então existe I um d-ideal próprio de $k[x,y]$. Seja $p(x,y) = \sum_{i=0}^{N} p_i y^i$, $p \neq 0$ onde $p_i \in k[x]$, um polinômio não nulo pertencente a I e com o menor grau em y.

1^ocaso: $N > 0$. Pela divisão euclidiana (aplicada a $d(p)$ e p considerados como elementos em $k(x)[y]$, temos que existe $g \in k[x]\backslash\{0\}$ tal que

$$gd(p) = hp + r,$$

para certos $h, r \in k[x,y]$ satisfazendo

$$grau_y(r) < grau_y(p) \ \text{ ou } \ r = 0.$$

Sendo I um d-ideal, temos que $r \in I$, mas isto implica, pelo caráter minimal de p, que $r = 0$. Portanto,

$$gd(p) = hp.$$

Como $g \in k[x]$, o Lema 4.5 nos garante que existem $\lambda \in k[x, y]$ e $\widetilde{p} \in k[x, y] \backslash k[x]$ tais que

$$d(\widetilde{p}) = \lambda \widetilde{p}.$$

Assim $\widetilde{p}$ é um polinômio de Darboux de d.

2^ocaso: $N = 0$, ou seja, $p \in I \cap k[x] \backslash \{0\}$. Daí temos

$$\begin{aligned} &p \in I \cap k[x] \text{ e } d(p) \in I \text{ e } d(p) = \partial_x(p) \in k[x] \Rightarrow \\ &p \in I \cap k[x] \text{ e } \partial_x(p) \in I \cap k[x] \Rightarrow \\ &\quad p \text{ gera um } \partial_x\text{-ideal não trivial de } k[x], \end{aligned}$$

absurdo, pois ∂_x é uma derivação simples de $k[x]$.

(ii)$\Longrightarrow$*(iii)* Decorre da proposição 4.4.

(iii)$\Longrightarrow$*(i)* é imediata pelo Corolário 4.3.

b) i) Para cada $f \in k[x]$, digamos,

$$f = \sum_{i=0}^{n} a_i x^i,$$

onde $n \in \mathbb{N}$ e $a_i \in k$, $a_n \neq 0$, temos

$$d(f) = \sum_{i=0}^{n} d(a_i x^i) \overset{d \text{ é } k\text{-derivação}}{=} \sum_{i=1}^{n} a_i i x^{i-1} d(x) \overset{d|_{k[x]} = \partial_x}{=} \sum_{i=1}^{n} a_i i x^{i-1},$$

e portanto $grau_x\ d(f) = n - 1 < n = grau_x\ f$. Assim, não existe $\lambda \in k[x, y]$ tal que $d(f) = \lambda f$, ou seja, nenhum polinômio $f \in k[x]$ pode ser um polinômio de Darboux de d. Em outras palavras, todo polinômio de Darboux f de d satisfaz $grau_y\ f \geq 1$.

Provamos agora o ítem *(ii)* para o caso em que k é um corpo algebricamente fechado (que é o caso em que vamos utilizá-lo), mas a afirmação vale para qualquer corpo de característica zero.

Suponhamos que existam f_1 e $f_2 \in k[x,y]$, polinômios de Darboux de d irredutíveis e tais que $f_1 \neq cf_2$, qualquer que seja $c \in k^*$. Então os ideais $f_1k[x,y]$ e $f_2k[x,y]$ são distintos e, um vez sendo f_1 e f_2 irredutíveis, são também ideais primos de altura 1. Pela Proposição 2.10 o ideal de $k[x,y]$ gerado por f_1 e f_2 é um d-ideal. Seja P um primo mínimo de (f_1, f_2). Pela Proposição 2.22 P é um d-ideal. Como $(f_1) \subset (f_1, f_2) \subseteq P$ e (f_1) é um ideal primo, então P é um ideal máximo de $k[x,y]$. Sendo k algebricamente fechado $P = (x-\alpha, y-\beta)$ com $\alpha, \beta \in k$ (Teorema 32 em [2]). Por outro lado $x - \alpha \in P$ e $d(x-\alpha) = d(x) - d(\alpha) = d(x) = 1 \notin P$, o que contradiz o fato de P ser um d-ideal. Portanto existe um único polinômio irredutível de Darboux, a menos de multiplicação por um fator de k^*. ∎

Nos próximos resultados, dado $r \in \overline{k(x)}$, continuaremos a utilizar a notação r' para a derivada de r com respeito à única extensão da derivação $\partial/\partial x : k(x) \longrightarrow k(x)$ para o fecho algébrico $\overline{k(x)}$ (veja Capítulo 2).

Teorema 4.7 *Seja d uma k-derivação de $k[x,y]$ com $d(x) = p(x,y)$ e $d(y) = q(x,y)$, e seja $f \in k[x,y]$ um polinômio de Darboux para d. Se f é irredutível então existe $r \in \overline{k(x)}$ tal que*

$$p(x,r)r' = q(x,r) \text{ e } f(x,r) = 0,$$

a saber, qualquer raiz em $\overline{k(x)}$ da equação $f(x,y) = 0$ (com coeficientes em $k(x)$).

Prova. Observe inicialmente que se existe um polinômio de Darboux f para d então, pelo Teorema 4.6, d não é simples e $grau_y f \geq 1$. Escrevemos

então

$$f(x,y) = \Sigma_{i=0}^{n} g_i(x) y^i,$$

onde $n \geq 1$ e $g_i(x) \in k[x]$, para todo $i \in \{0, 1, ..., n\}$. Olhando f como um elemento de $k(x)[y]$ e sendo $n = grau_y f \geq 1$, temos que f tem uma raiz em $\overline{k(x)}$, que vamos denotar por r :

$$0 = f(x,r) = \Sigma_{i=0}^{n} g_i(x) r^i.$$

Daí, aplicando a derivação $(\ )'$ à igualdade acima, obtemos

$$\begin{aligned} 0 &= \left(\Sigma_{i=0}^{n} g_i(x) r^i\right)' \\ &= \Sigma_{i=0}^{n} \left(g_i(x) r^i\right)' \\ &= \Sigma_{i=0}^{n} g_i(x)' r^i + \Sigma_{i=0}^{n} i g_i(x) r^{i-1} r' \\ &= \frac{\partial f}{\partial x}(x,r) + r' \frac{\partial f}{\partial y}(x,r), \end{aligned} \tag{9}$$

Por outro lado, pela Proposição 2.7, sabemos que, sendo d uma k-derivação de $k[x,y]$, temos

$$\begin{aligned} d(f) &= d(x)\frac{\partial f}{\partial x} + d(y)\frac{\partial f}{\partial y} \\ &= p(x,y)\frac{\partial f}{\partial x} + q(x,y)\frac{\partial f}{\partial y}. \end{aligned}$$

Agora, como f é um polinômio de Darboux para d, digamos,

$$d(f) = \lambda f,$$

com $\lambda \in k[x,y] \backslash k$, temos

$$p(x,y)\frac{\partial f}{\partial x}(x,y) + q(x,y)\frac{\partial f}{\partial y}(x,y) = d(f) = \lambda(x,y) f(x,y),$$

e, escrevendo esta igualdade para $y = r$, temos (lembrando que $f(x,r) = 0$)

$$p(x,r)\frac{\partial f}{\partial x}(x,r) + q(x,r)\frac{\partial f}{\partial y}(x,r) = 0. \tag{10}$$

Como f é por hipótese irredutível em $k[x,y] = k[x][y]$ e como $f(x,r) = 0$, então f é o polinômio mínimo de r sobre $k(x)$. Ainda, como $grau_y\ f(x,y) \geq 1$ temos $grau_y\ \dfrac{\partial f}{\partial y}(x,y) \geq 0$, e portanto $\dfrac{\partial f}{\partial y}(x,r) \neq 0$. Daí, de (10) obtemos

$$q(x,r) = -\frac{\dfrac{\partial f}{\partial x}(x,r)}{\dfrac{\partial f}{\partial y}(x,r)} p(x,r) \overset{(9)}{=} r'p(x,r). \quad \blacksquare$$

Teorema 4.8 *Seja d uma k-derivação de $k[x,y]$ com $d(x) = p(x,y)$ e $d(y) = q(x,y)$. Se $r \in \overline{k(x)}$ é uma solução da equação diferencial*

$$p(x,r)r' = q(x,r), \tag{11}$$

então seu polinômio minimal primitivo f em $k[x,y]$ é um polinômio de Darboux de d irredutível.

Prova. Como $f(x,y)$ é o polinômio minimal primitivo de r em $k[x,y]$, então $grau_y\ f \geq 1$. Defina $h \in k[x,y]$ por

$$h(x,y) = d(f(x,y)).$$

Afirmamos que $h(x,r) = 0$. De fato,

$$\begin{aligned} h(x,r) &= d(f(x,y))(r) \\ &= p(x,r)\frac{\partial f}{\partial x}(x,r) + q(x,r)\frac{\partial f}{\partial y}(x,r) \overset{(11)}{=} \\ &= p(x,r)\frac{\partial f}{\partial x}(x,r) + p(x,r)r'\frac{\partial f}{\partial y}(x,r) \\ &= p(x,r)\left[\frac{\partial f}{\partial x}(x,r) + r'\frac{\partial f}{\partial y}(x,r)\right] \end{aligned}$$

Mas

$$\frac{\partial f}{\partial x}(x,r) + \frac{\partial f}{\partial y}(x,r).r' = \frac{\partial}{\partial x}\left(f(x,r)\right) = \frac{\partial}{\partial x}(0) = 0,$$

e portanto

$$h(x,r) = p(x,r).0 = 0.$$

Como $f(x,y)$ é um polinômio minimal primitivo para r em $k[x,y]$ e $h(x,r)=0$ concluímos que $h(x,y)$ deve ser um múltiplo de f em $k(x)[y]$:

$$d(f) = h = \Lambda f.$$

para algum $\Lambda = \Lambda(x,y) \in k(x)[y]$. Afirmamos que $\Lambda \in k[x][y]$, e portanto f é um polinômio de Darboux para d.

De fato, escrevendo Λ na forma

$$\Lambda = \frac{l(x)t(x,y)}{g(x)}, \tag{12}$$

onde $l(x), g(x) \in k[x]$ e $t(x,y) \in k[x,y]$, com $t(x,y)$ primitivo como polinômio na variável y, temos

$$l(x)t(x,y)f(x,y) = g(x)\Lambda(x,y)f(x,y) = g(x).d(f).$$

Como $t(x,y)$ e $f(x,y)$ são primitivos como polinômios em y, temos, pelo Lema de Gauss, que $t(x,y)f(x,y)$ também é primitivo e, como $l(x), g(x) \in k[x]$, obtemos

$$\begin{aligned} l(x) &\overset{t(x,y)f(x,y) \text{ é primitivo}}{=} cont[l(x)t(x,y)f(x,y)] \\ &= cont[g(x)d(f)] = g(x)cont(d(f)). \end{aligned}$$

Daí obtemos

$$\frac{l(x)}{g(x)} = cont(d(f)) \in k[x],$$

donde, por (12),

$$\Lambda = \frac{l(x)t(x,y)}{g(x)} \in k[x,y],$$

o que completa a prova. ■

Decorrem dos teoremas 4.7 e 4.8, os seguintes corolários:

Corolário 4.9 *Seja d uma k-derivação de $k[x,y]$ com $d(x) = p(x,y)$ e $d(y) = q(x,y)$, isto é,*

$$d = p(x,y)\partial_x + q(x,y)\partial_y.$$

Então as seguintes condições são equivalentes:

(i) Existe um polinômio de Darboux $f \in k[x,y]$ para d com $grau_y f \geq 1$.

(ii) Existe uma função racional $r \in \overline{k(x)}$ tal que $p(x,r)r' = q(x,r)$.

Para os próximos capítulos, será útil destacarmos o próximo corolário:

Corolário 4.10 *Seja $d = \partial_x + q(x,y)\partial_y$ uma k-derivação de $k[x,y]$, onde $q(x,y) \in k[x,y]$, então*

a) as seguintes condições são equivalentes:

i) d não é simples em $k[x,y]$;

ii) Existe f polinômio irredutível de Darboux de d em $k[x,y]$

iii) Existe $r \in \overline{k(x)}$ tal que $r' = q(x,r)$.

b) Se d não é simples então todo polinômio de Darboux f de d satisfaz $grau_y\ f \geq 1$ e existe um único polinômio de Darboux de d que é irredutível e mônico.

c) As soluções em $\overline{k(x)}$ da equação diferencial $z' = q(x,z)$ são exatamente as soluções (em $\overline{k(x)}$) da equação $f(x,z) = 0$.

Prova. Decorre dos Teoremas 4.6, 4.7 e 4.8. ■

5 SOBRE UMA CLASSE DE EQUAÇÕES DE RICCATI

Neste capítulo, consideramos uma equação diferencial de Riccati da forma

$$t' = t^2 - p(x), \tag{13}$$

onde $p = p(x)$ é um polinômio de $k[x]$. Nosso objetivo é saber decidir sobre a simplicidade das $k-$derivações $\partial_x + (y^2 - p(x))\partial_y$, onde $p(x) \in k[x]$ e que denotaremos por Δ_p :

$$\Delta_p = \partial_x + (y^2 - p(x))\partial_y,$$

ou ainda: para cada $p = p(x) \in k[x]$, Δ_p denotará a k-derivação de $k[x, y]$ induzida por

$$\begin{cases} \Delta_p(x) = 1 \\ \Delta_p(y) = y^2 - p(x) \end{cases}$$

Uma importante simplificação acontece no caso em que k é algebricamente fechado, a saber, as soluções algébricas são na verdade racionais.

Teorema 5.1 ([5], Theorem 5.1) *Se k é algebricamente fechado então, para cada $p(x) \in k[x]$, a equação (13) não admite solução em $\overline{k(x)} \setminus k(x)$. Em outras palavras, as soluções algébricas de (13), se existirem, são todas racionais.*

Prova. Suponha que existe $t \in \overline{k(x)} \setminus k(x)$ que é solução de (13).

Seja $f \in k(x)[y]$ o polinômio minimal para t sobre $k(x)$. Como $t \notin k(x)$, temos $grau_y f \geq 2$.

Seja K um corpo de fatoração de f sobre $k(x)$ e sejam $t_1, ..., t_n$ as n raízes de f em K. Como a característica de k é zero e f é irredutível em $k(x)[y]$,

temos que $t = t_1, ..., t_n$ são todas distintas e

$$f = f(x, y) = y^n - \sigma_1 y^{n-1} + \sigma_2 y^{n-2} - ... + (-1)^n \sigma_n, \tag{14}$$

onde $n \geq 2$ e σ_i denotam os polinômios simétricos em $t_1, ..., t_n$.

Ainda, como a extensão $k(x) \subset K$ é algébrica, a derivação $\frac{d}{dx}$ de $k(x)$ pode ser estendida de maneira única a uma derivação de K (veja Teorema 2.16) que poderíamos continuar denotando por $(\quad)'$ ou por $\partial/\partial x$, mas que aqui, para simplificação de escrita, vamos denotar por d. Assim, a equação (13) se reescreve

$$d(t) = t^2 - p(x) \tag{15}$$

Afirmação 1: Se σ é um $k(x)$-automorfismo de K, então $\sigma d\sigma^{-1}$ é uma derivação de K. De fato, dados $a, b \in K$, é claro que

$$(\sigma d\sigma^{-1})(a + b) = \sigma d\sigma^{-1}(a) + \sigma d\sigma^{-1}(b).$$

Além disso,

$$\begin{aligned}\left(\sigma d\sigma^{-1}\right)(ab) &= (\sigma d)\left(\sigma^{-1}(a)\sigma^{-1}(b)\right) \\ &= \sigma\left[d(\sigma^{-1}(a))\sigma^{-1}(b) + \sigma^{-1}(a)d(\sigma^{-1}(b))\right] \\ &= \left(\sigma d\sigma^{-1}\right)(a)b + a\left(\sigma d\sigma^{-1}\right)(b).\end{aligned}$$

Afirmação 2: Se σ é um $k(x)$-automorfismo de K, então $\sigma d\sigma^{-1}|_{k(x)} = d|_{k(x)} = \partial/\partial x$, e portanto, pela unicidade da extensão de $\partial/\partial x$ a uma extensão algébrica, temos que $\sigma d\sigma^{-1} = d$, ou ainda, $\sigma d = d\sigma$.

De fato, dado $m \in k(x)$, temos, uma vez que σ é um $k(x)$-automorfismo,

$$\sigma d\sigma^{-1}(m) = \sigma d(m) \overset{m \in k(x)}{=} \sigma \frac{\partial}{\partial x}(m) = \frac{\partial}{\partial x}(m).$$

Afirmação 3: Toda raiz t_i de f $(i = 1, ..., n\ )$ é também solução de (15).

De fato, para cada $i \in \{1, ..., n\}$, $t_i = \sigma(t)$ para algum $\sigma \in Aut_{k(x)}(K)$. Daí,

$$d(t_i) = d(\sigma(t)) \overset{\sigma d = d\sigma}{=} \sigma d(t) \overset{(15)}{=}$$
$$= \sigma(t^2 - p(x)) = \sigma(t)^2 - \sigma(p(x)) \overset{\substack{\sigma|_{k(x)}=\text{identidade} \\ \sigma(t)=t_i}}{=} t_i^2 - p(x).$$

Considere agora o discriminante de f, que denotamos por Δ. Como $f(x,y) = \prod_{i=1}^{n}(y - t_i)$, temos

$$\Delta = (-1)^{n(n-1)/2} \prod_{i \neq j} (t_i - t_j) \in k(x)$$

Afirmação 4: $d(\Delta) = (-1)^{n(n-1)/2} \sum_{i \neq j} d(t_i - t_j) \prod_{m \neq k,\ (m,k) \neq (i,j)} (t_m - t_k)$.

A prova desta afirmação é feita por indução sobre n, e encontra-se no Apêndice (veja seção 7.1).

Afirmação 5: O coeficiente σ_1 de f (veja (14)) pode também ser dado por

$$\sigma_1 = \frac{d(\Delta)}{2(n-1)\Delta}.$$

De fato, a partir da Afirmação 4 podemos calcular a *derivada logarítmica* de Δ:

$$\frac{d(\Delta)}{\Delta} \overset{\text{Afirm.4}}{=} \frac{(-1)^{n(n-1)/2} \sum_{i \neq j} d(t_i - t_j) \prod_{m \neq k,\ (m,k) \neq (i,j)} (t_m - t_k)}{(-1)^{n(n-1)/2} \prod_{i \neq j} (t_i - t_j)}$$
$$= \sum_{i \neq j} \frac{d(t_i - t_j)}{t_i - t_j} = \sum_{i \neq j} \frac{d(t_i) - d(t_j)}{t_i - t_j} \overset{\text{Afirm.3}}{=}$$
$$= \sum_{i \neq j} \frac{t_i^2 - p(x) - t_j^2 + p(x)}{t_i - t_j}$$

$$= \sum_{i \neq j} \frac{t_i^2 - t_j^2}{t_i - t_j} = \sum_{i \neq j} \frac{(t_i - t_j)(t_i + t_j)}{t_i - t_j} = \sum_{i \neq j} (t_i + t_j)$$
$$= 2(n-1)(t_1 + t_2 + ... + t_n) \overset{(14)}{=} 2(n-1)\sigma_1,$$

donde se obtém a expressão desejada.

Afirmação 6: Como $\Delta \in k(x)$, podemos escrever $\Delta = \frac{h}{g}$, com $h, g \in k[x]$ e $mdc(h, g) = 1$. Daí segue que

$$\frac{d(\Delta)}{\Delta} = \frac{h'g - hg'}{hg}.$$

De fato,

$$d(\Delta) = \frac{h'g - hg'}{g^2},$$

e conseqüentemente,

$$\frac{d(\Delta)}{\Delta} = \frac{h'g - hg'}{g^2} . \frac{g}{h} = \frac{h'g - hg'}{hg}.$$

Afirmação 7: Sendo k algebricamente fechado, temos

$$h = m \prod_{i=1}^{u} (x - l_i)^{r_i} \quad \text{e} \quad g = b \prod_{i=1}^{v} (x - \xi_i)^{s_i}, \tag{16}$$

onde $m, b \in k^*$, $l_1, ..., l_u, \xi_1, ..., \xi_v \in k$. Afirmamos que

$$\sigma_1 = \sum_{\alpha \in R} \frac{\lambda_\alpha}{x - \alpha}, \tag{17}$$

onde $\lambda_\alpha \in \mathbb{Q}$ e $R = \{l_1, ..., l_u, \xi_1, ..., \xi_v\}$.

De fato, de 16 obtemos

$$h' = m \sum_{i=1}^{u} r_i (x - l_i)^{r_i - 1} \prod_{j \in \{1,...,u\}, j \neq i} (x - l_j)^{r_j}$$

$$
\begin{aligned}
&= m\sum_{i=1}^{u} r_i \frac{\prod_{j=1}^{u}(x-l_j)^{r_j}}{x-l_i} \\
&= m\prod_{j=1}^{u}(x-l_j)^{r_j}\sum_{i=1}^{u} r_i \frac{1}{x-l_i} \\
&= mh\sum_{i=1}^{u} r_i \frac{1}{x-l_i},
\end{aligned}
$$

e portanto

$$\frac{h'}{h} = \sum_{i=1}^{u} \frac{r_i}{x-l_i},$$

com $r_i \in \mathbb{N}^*$. Analogamente temos que

$$\frac{g'}{g} = \sum_{i=1}^{v} \frac{s_i}{(x-\xi_i)},$$

com $s_i \in \mathbb{N}^*$. Como

$$
\begin{aligned}
\frac{d(\Delta)}{\Delta} = \frac{h'g - hg'}{hg} &= \frac{h'}{h} - \frac{g'}{g} \\
&= \sum_{i=1}^{u} \frac{r_i}{(x-l_i)} - \sum_{i=1}^{v} \frac{s_i}{(x-\xi_i)}
\end{aligned}
$$

podemos escrever

$$\frac{d(\Delta)}{\Delta} = \sum_{\alpha \in R} \frac{\gamma_\alpha}{x-\alpha}$$

onde $R = \{l_1, ..., l_u, \xi_1, ..., \xi_v\}$ e $\gamma_\alpha \in \mathbb{Z}^*$.

Logo,

$$\sigma_1 \overset{\text{Afirm.5}}{=} \frac{d(\Delta)}{2(n-1)\Delta} \overset{\text{Afirm.6}}{=} \frac{1}{2(n-1)} \frac{h'g - hg'}{hg} = \sum_{\alpha \in R} \frac{\lambda_\alpha}{x-\alpha},$$

onde $\lambda_\alpha = \gamma_\alpha / 2(n-1) \in \mathbb{Q}^*$, para cada $\alpha \in R$.

Afirmação 8: f é um polinômio de Darboux para a derivação

$$\Delta_p = \frac{\partial}{\partial x} + (y^2 - p)\frac{\partial}{\partial y},$$

olhada como derivação de $k(x)[y]$.

De fato, como $f(x,y) \in k(x)[y]$, existem $m(x), n(x) \in k[x]$ e $f_1(x,y) \in k[x,y]$ primitivo tais que $f(x,y) = \dfrac{n(x)}{m(x)} f_1(x,y)$.

Como f é polinômio mínimo de t sobre $k(x)$, f_1 é polinômio minimal primitivo de t. Logo pela Proposição 4.8, f_1 é polinômio de Darboux de Δ_p, e portanto existe $\lambda \in k[x,y]$ tal que $\Delta_p(f_1) = \lambda f_1$. Decorre daí que

$$\begin{aligned}\Delta_p(f) &= \Delta_p\left(\frac{n}{m} f_1\right) = \Delta_p\left(\frac{n}{m}\right) f_1 + \frac{n}{m}\Delta_p\left(f_1\right) \\ &= \Delta_p\left(\frac{n}{m}\right)\left[\frac{m}{n}\left(\frac{n}{m} f_1\right)\right] + \frac{n}{m}\lambda f_1 \\ &= \left[\Delta_p\left(\frac{n}{m}\right)\frac{m}{n} + \lambda\right]\frac{n}{m} f_1 = \left[\Delta_p\left(\frac{n}{m}\right)\frac{m}{n} + \lambda\right] f.\end{aligned}$$

Logo f é um polinômio de Darboux para a derivação Δ_p.

Afirmação 9: Seja $\beta \in k(x)[y]$ tal que

$$\Delta_p(f) = \beta f. \tag{18}$$

Afirmamos que $grau_y \beta = 1$ e o coeficiente do seu termo em y é n.

De fato, da igualdade

$$\beta f = \Delta_p(f) = \frac{\partial f}{\partial x} + (y^2 - p)\frac{\partial f}{\partial y},$$

e do fato que $grau_y\left(\dfrac{\partial f}{\partial x} + (y^2 - p)\dfrac{\partial f}{\partial y}\right) = 1 + grau_y f$, concluímos que $grau_y \beta = 1$.

Além disso, comparando coeficientes e tendo em vista que $grau_y \dfrac{\partial f}{\partial x} \leq grau_y f$, temos que o coeficiente do termo líder em y de β é n. Portanto

$$\beta = ny + a, \text{ para algum } a \in k(x). \tag{19}$$

Passamos agora a estudar em detalhe o "termo constante" $a \in k(x)$ de (19)

De (14), obtemos

$$\frac{\partial f}{\partial x} \overset{\sigma_0=1}{=} \sum_{i=1}^{n}(-1)^i\sigma_i' y^{n-i} \ ,$$

$$\frac{\partial f}{\partial y} = \sum_{i=0}^{n-1}(-1)^i(n-i)\sigma_i y^{n-i-1} = \sum_{i=1}^{n}(-1)^{i-1}(n-i+1)\sigma_{i-1}y^{n-i},$$

$$y^2\frac{\partial f}{\partial y} = \sum_{i=1}^{n}(-1)^{i-1}(n-i+1)\sigma_{i-1}y^{n-i+2} = \sum_{i=-1}^{n-2}(-1)^{i+1}(n-i-1)\sigma_{i+1}y^{n-i}$$

$$-p\frac{\partial f}{\partial y} = \sum_{i=1}^{n}(-1)^i(n-i+1)p\sigma_{i-1}y^{n-i}$$

e portanto

$$\begin{aligned}\frac{\partial f}{\partial x} + (y^2-p)\frac{\partial f}{\partial y} &= \sum_{i=1}^{n}(-1)^i\sigma_i' y^{n-i} + \sum_{i=-1}^{n-2}(-1)^{i+1}(n-i-1)\sigma_{i+1}y^{n-i} \\ &\quad + \sum_{i=1}^{n}(-1)^i(n-i+1)p\sigma_{i-1}y^{n-i} \\ &= ny^{n+1} - (n-1)\sigma_1 y^n \\ &\quad + \sum_{i=1}^{n-2}(-1)^i\left[\sigma_i' - (n-i-1)\sigma_{i+1} + (n-i+1)p\sigma_{i-1}\right]y^{n-i} \\ &\quad + (-1)^{n-1}(\sigma_{n-1}' + 2p\sigma_{n-2})y + (-1)^n(\sigma_n' + p\sigma_{n-1}) \qquad (20)\end{aligned}$$

Por outro lado,

$$\begin{aligned}\beta f = (ny+a)f &= (ny+a)\sum_{i=0}^{n}(-1)^i\sigma_i y^{n-i} = \\ &= ny^{n+1} + (n(-1)^1\sigma_1 + a(-1)^0\sigma_0)y^n \\ &\quad + \sum_{i=1}^{n-1}\left((-1)^{i+1}n\sigma_{i+1} + (-1)^i a\sigma_i\right)y^{n-i} + (-1)^n a\sigma_n \\ &= ny^{n+1} + (a-n\sigma_1)y^n \\ &\quad + \sum_{i=1}^{n-1}(-1)^i\left(-n\sigma_{i+1} + a\sigma_i\right)y^{n-i} + (-1)^n a\sigma_n. \qquad (21)\end{aligned}$$

Comparando os coeficientes de y^i nas igualdades (20) e (21) deduzimos que

$$-(n-1)\sigma_1 = (a - n\sigma_1),$$

ou seja,

$$\sigma_1 = a;$$

para $1 \leq i \leq n-1$, deduzimos que

$$(-1)^i(\sigma_i' - (n-i-1)\sigma_{i+1} + (n-i+1)p\sigma_{i-1}) = (-1)^i(-n\sigma_{i+1} + a\sigma_i),$$

ou ainda,

$$-(n-i-1-n)\sigma_{i+1} = -\sigma_i' - (n-i+1)p\sigma_{i-1} + a\sigma_i,$$

o que nos leva a

$$(i+1)\sigma_{i+1} = a\sigma_i - \sigma_i' - (n-i+1)p\sigma_{i-1}.$$

Já para $i = n$, obtemos

$$(-1)^n(\sigma_n' + p\sigma_{n-1}) = (-1)^n a\sigma_n,$$

o que nos leva a

$$\sigma_n' + p\sigma_{n-1} = a\sigma_n,$$

e assim obtemos o seguinte sistema de $n+1$ equações:

$$(\Sigma) \begin{cases} \sigma_1 = a \\ 2\sigma_2 = a\sigma_1 - \sigma_1' - np \\ 3\sigma_3 = a\sigma_2 - \sigma_2' - (n-1)p\sigma_1 \\ ... \\ i\sigma_i = a\sigma_{i-1} - \sigma_{i-1}' - (n+2-i)p\sigma_{i-2} \\ ... \\ n\sigma_n = a\sigma_{n-1} - \sigma_{n-1}' - 2p\sigma_{n-2} \\ 0 = a\sigma_n - \sigma_n' - p\sigma_{n-1} \end{cases} \tag{22}$$

Note que os coeficientes σ_i de f podem ser também pensados como uma seqüência de funções racionais $(\sigma_i)_{i\in\mathbb{N}}$, definidas indutivamente por

$$\sigma_0 = 1, \quad \sigma_1 = a$$

e, para $2 \leq i \leq n$,

$$i\sigma_i = a\sigma_{i-1} - \sigma'_{i-1} - (n+2-i)p\sigma_{i-2} \tag{23}$$

e

$$\sigma_i = 0,$$

para $i > n$. Daí, após feitas todas as substituições, a última equação de (Σ) se torna uma equação diferencial para a.

Afirmação 10: Seja α um dos pólos de $a = \sigma_1$ (veja (17)). Como $p(x) \in k[x]$, obviamente α não é pólo de $p(x)$. Afirmamos no entanto que, para todo $i \in \{1, 2, ..., n\}$.

i) α é um pólo de σ_i com ordem no máximo i;

ii) se denotarmos por $\overline{\sigma_i}$ a parte de σ_i que envolve o pólo α de ordem i então

$$i!\overline{\sigma_i} = \frac{\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+i-1)}{(x-\alpha)^i}, \tag{24}$$

A prova desta afirmação é feita por indução sobre i, e encontra-se no Apêndice (veja seção 7.2).

Afirmação 11: Para cada pólo α de σ_1, o racional λ_α definido em (17) satisfaz

$$\lambda_\alpha \in \{-1, -2, ..., -n\},$$

e portanto a fórmula (24) vale também para $i > n$.

De fato, da última equação de (22) temos que

$$\sigma_{n+1} = 0 = a\sigma_n - \sigma'_n - p\sigma_{n-1}.$$

Pela prova da Afirmação 10, α é um pólo de $a\sigma_n = \sigma_1\sigma_n$ e de $-\sigma_n'$ de ordem no máximo $n+1$ e é de ordem no máximo $n-1$ como pólo de σ_{n-1}; daí concluímos que, ainda denotando por $\overline{\sigma_{n+1}}$ a parte de σ_{n+1} que envolve o pólo α de ordem $n+1$, obtemos

$$0 = \overline{\sigma_{n+1}} = \overline{a\sigma_n} - \overline{\sigma_n'}.$$

De (24) obtemos

$$\overline{\sigma_n'} = -\frac{1}{n!}\frac{n\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+n-1)}{(x-\alpha)^{n+1}},$$

e portanto

$$\begin{aligned} 0 &= \overline{a\sigma_n} - \overline{\sigma_n'} \\ &= \frac{\lambda_\alpha}{x-\alpha}\frac{1}{n!}\frac{\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+n-1)}{(x-\alpha)^n} + \frac{1}{n!}\frac{n(\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+n-1)}{(x-\alpha)^{n+1}} \\ &= \frac{1}{n!}\frac{\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+n-1)(\lambda_\alpha+n)}{(x-\alpha)^{n+1}}; \end{aligned}$$

com isso, obtemos a seguinte equação para cada λ_α :

$$\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+n) = 0,$$

o que nos dá $\lambda_\alpha \in \{0,-1,-2,...,-n\}$; ainda, como α é um pólo σ_1 temos $\lambda_\alpha \neq 0$. Isto completa prova da Afirmação 11.

Dividimos agora a prova em dois casos:

1º caso: $p \neq 0$.

Neste caso, *grau* $p \geq 0$. Queremos estimar os graus e certos coeficientes das funções racionais $\sigma_1, ..., \sigma_n$. (Por *grau* de uma função racional queremos significar a diferença

(*grau* do numerador) − (*grau* do denominador).)

Nesta etapa, p está fortemente envolvido, conforme nos mostra a afirmação seguir:

Afirmação 12: Se $\delta = grau(p)$ então, para cada $i \in \mathbb{N}$,

$$\begin{aligned} grau(\sigma_{2i}) &= i\delta \quad \text{enquanto } 2i \leq n \\ grau(\sigma_{2i+1}) &\leq i\delta - 1. \end{aligned}$$

Esta afirmação está provada no Apêndice (veja seção 7.3).

Denotemos por $\widehat{p}$ o coeficiente líder de p e, para cada i, por $\widehat{\sigma_{2i}}$ o coeficiente em σ_{2i} do termo de grau $i\delta$, e por $\widehat{\sigma_{2i+1}}$ o coeficiente em σ_{2i+1} do termo de grau $i\delta - 1$ (que pode ser nulo, pela Afirmação 12). É claro que $\widehat{\sigma_j} = 0$ se $j > n$.

Seja Λ o inteiro não negativo dado por

$$\Lambda = -\sum_{\alpha \in R} \lambda_\alpha.$$

Obtemos então as seguintes relações envolvendo os $\widehat{\sigma_i}$:

$$\widehat{\sigma_1} = -\Lambda, \tag{25}$$

pois $\sigma_1 = \sum_{\alpha \in R} \dfrac{\lambda_\alpha}{x - \alpha}$. Ainda, por (23), obtemos

$$\begin{cases} 2\widehat{\sigma_2} = -n\widehat{p}, \\ 3\widehat{\sigma_3} = \widehat{a\sigma_2} - \widehat{\sigma_2'} - (n-1)\widehat{p\sigma_1}, \\ ... \\ (2i)\widehat{\sigma_{2i}} = -(n+2-2i)\widehat{p\sigma_{2i-2}}, \text{ enquanto } 2i \leq n \\ (2i+1)\widehat{\sigma_{2i+1}} = \widehat{a\sigma_{2i}} - \widehat{\sigma_{2i}'} - (n-2i+1)\widehat{p\sigma_{2i-1}}, \\ \qquad\qquad\qquad\qquad \text{enquanto } 2i+1 \leq n \\ ... \end{cases} \tag{26}$$

Observação: As fórmulas acima valem também para $\widehat{\sigma_{n+1}}$:

$$\begin{cases} (n+1)\widehat{\sigma_{n+1}} = -\widehat{p\sigma_{n-1}}, \text{ se } n \text{ for ímpar} \\ (n+1)\widehat{\sigma_{n+1}} = \widehat{a\sigma_n} - \widehat{\sigma_n'} - \widehat{p\sigma_{n-1}}, \text{ se } n \text{ for par} \end{cases} \tag{27}$$

De fato:

- se n é par, digamos, $n = 2s$, então

$$\widehat{\sigma_{2s+1}} = \widehat{\sigma_{n+1}} = 0 \overset{(22)}{=} \widehat{a\sigma_{2s}} - \widehat{\sigma'_{2s}} - \widehat{p\sigma_{2s-1}},$$

e portanto vale, para $n = 2s$,

$$(n+1)\widehat{\sigma_{n+1}} = \widehat{a\sigma_n} - \widehat{\sigma'_n} - \widehat{p\sigma_{n-1}};$$

- se n é ímpar, digamos, $n = 2s+1$, então

$$\widehat{\sigma_{2s+2}} = \widehat{\sigma_{n+1}} = 0 \overset{(22)}{=} -\widehat{p\sigma_{2s}},$$

e portanto vale também para $n = 2s+1$,

$$(n+1)\widehat{\sigma_{n+1}} = -\widehat{p\sigma_{n-1}}.$$

Afirmação 13: Para todo $s \in \mathbb{N}$ tem-se

$$\widehat{\sigma_{2s}} = (-1)^s \widehat{p}^s M_{2s}, \qquad \text{enquanto } 2s \leq n+1 \tag{28}$$

e

$$\widehat{\sigma_{2s+1}} = (-1)^{s+1} \widehat{p}^s M_{2s+1}, \quad \text{enquanto } 2s+1 \leq n+1, \tag{29}$$

onde M_i são racionais definidos indutivamente por:

$$M_0 = 1, \qquad M_1 = \Lambda \tag{30}$$

e, para $s \geq 1$,

$$M_{2s} = \frac{n+2-2s}{2s} M_{2(s-1)}, \tag{31}$$

e

$$M_{2s+1} = \frac{1}{2s+1}[(\Lambda + s\delta)M_{2s} + (n+1-2s)M_{2s-1}]. \tag{32}$$

(Note que os racionais M_{2s} são não negativos enquanto $2s \leq n+2$ e os M_{2s+1} são não negativos enquanto $2s \leq n+1$).

A prova desta afirmação encontra-se no Apêndice (veja seção 7.4).

Afirmação 14: n é par.

Se n é ímpar, digamos, $n = 2s + 1$, temos:

$$0 = \widehat{\sigma_{n+1}} = \widehat{\sigma_{2s+2}} = \widehat{\sigma_{2(s+1)}} \overset{(28)}{=} (-1)^{s+1}\widehat{p}^{s+1}M_{2(s+1)} = (-1)^{s+1}\widehat{p}^{s+1}M_{n+1},$$

portanto $M_{2(s+1)} = M_{n+1} = 0$. Daí segue que

$$0 = M_{2(s+1)} \overset{(31)}{=} \frac{n + 2 - 2(s + 1)}{2(s + 1)} M_{2s},$$

o que implica

$$M_{2s} = 0,$$

e conseqüentemente,

$$\widehat{\sigma_{2s}} \overset{(28)}{=} (-1)^{s}\widehat{p}^{s}M_{2s} = 0,$$

o que é um aburdo, pois $p \neq 0$ e, pela Afirmação 12, $grau\ \sigma_{2s} = s \times grau(p)$, portanto $\widehat{\sigma_{2s}} \neq 0$.

Escrevamos então $n = 2s$; como $\sigma_{n+1} = 0$, temos, por (29)

$$0 = M_{n+1} = M_{2s+1}.$$

Deste modo,

$$0 = M_{2s+1} \overset{(32)}{=} \frac{1}{2s + 1}[(\Lambda + s\delta)M_{2s} + (n + 1 - 2s)M_{2s-1}],$$

como $n = 2s$

$$(\Lambda + s\delta)M_n + M_{n-1} = 0.$$

Como $M_i \geq 0$, para todo $i \leq n + 1$ e $M_n \neq 0$, temos que $(\Lambda + s\delta)M_n + M_{n-1} = 0$ implica $\Lambda + s\delta = 0$ e $M_{n-1} = 0$.

Mas $\Lambda \geq 0$, $s > 0$ e $\delta \geq 0$, portanto $\Lambda = \delta = 0$.

Concluímos: se a equação diferencial (13) tem solução $t \in \overline{k(x)} \setminus k(x)$ e $p \neq 0$ então devemos ter, por (17),

$$\sigma_1 = \Lambda = 0 \tag{33}$$

e

$$grau\ p = \delta = 0, \tag{34}$$

ou seja, p é um polinômio constante e o coeficiente σ_1 de f é igual a zero. Além disso f teria grau par $n = 2s$.

Afirmação 15: Para todo $i \in \mathbb{N}$,

$$\sigma_{2i+1} = 0 \quad \text{e, enquanto } 2i \leq n, \qquad \sigma_{2i} = (-1)^i \binom{s}{i} p^i;$$

em particular σ_{2i} é constante, pois p é constante.

Esta afirmação está provada no Apêndice (veja seção 7.5).

Logo

$$f = y^{2s} + (-1)^1 \tbinom{s}{1} p^1 y^{2(s-1)} + \ldots + (-1)^{s-1} \tbinom{s}{s-1} p^{s-1} y^2 + (-1)^s \tbinom{s}{s} p^s = (y^2 - p)^s.$$

Como f foi suposto irredutível, devemos ter $s = 1$, ou seja,

$$f = y^2 - p \in k[y].$$

Mas $p \in k$ e k é por hipótese algebricamente fechado, então f não tem grau 2, absurdo.

Portanto, acabamos de provar que a equação diferencial (13), quando o polinômio p é não nulo, não admite solução algébrica que não seja função racional.

2º caso: $p = 0$.

Aqui reescrevemos

$$\sigma_1 = \sum_{\alpha \in R} \frac{\lambda_\alpha}{(x-\alpha)},$$

na forma

$$\sigma_1 = \sum_{i=1}^{m} \frac{-1}{(x-\alpha_i)},$$

levando em conta que o conjunto R é finito e que $\lambda_\alpha \in \{-1, -2, ..., -n\}$, para cada α, onde $m = -\sum_{i \in j} \lambda_{\alpha_i}$ (podendo acontecer $\alpha_i = \alpha_j$ com $i \neq j$).

Afirmação 16: Para cada $j \in \{1, 2, ..., n\}$, tem-se

$$\sigma_j = \sum_{1 \leq i_1 < i_2 < ... < i_j \leq m} \frac{(-1)^j}{(x-\alpha_{i_1})(x-\alpha_{i_2})...(x-\alpha_{i_j})}$$

A prova desta afirmação encontra-se no Apêndice (veja seção 7.6).

Definimos agora

$$g(x, y) = ((x-\alpha_1)...(x-\alpha_m))f(x, y).$$

Como $f = f(x, y) = y^n - \sigma_1 y^{n-1} + \sigma_2 y^{n-2} - ... + (-1)^n \sigma_n$, pela Afirmação 16, é claro que $g(x, y) \in k[x, y]$.

Como $t \in \overline{k(x)} \backslash k(x)$ é tal que $f(x, t) = 0$, temos

$$g(x, t) = (x-\alpha_1)...(x-\alpha_m)f(x, t) = 0$$

Como $g(x, y) \in k[x, y] \subseteq k(y)[x]$ e $g(x, y) \neq 0$, então g tem somente um número finito de raízes em $k(y)$, em particular um número finito em k. Sendo k infinito, existe $\alpha \in k$ tal que $g(\alpha, y) \neq 0$. Por outro lado, $g(x, t) = 0$, implica que $g(\alpha, t) = 0$, logo t é raíz de um polinômio não nulo $g(\alpha, y)$ de $k[y]$, portanto t é algébrico sobre k. Sendo k algebricamente fechado temos que $t \in k$, o que é um absurdo, pois por hipótese $t \in \overline{k(x)} \backslash k(x)$.

Isto completa a prova do teorema. ■

6 SIMPLICIDADE DAS $k-$DERIVAÇÕES $\partial_x + (y^2 - p(x))\partial_y$

Neste capítulo, discutiremos a simplicidade das k-derivações de $k[x, y]$

$$\Delta_p = \partial_x + (y^2 - p(x))\partial_y$$

definidas no capítulo anterior. *Estaremos em todo o capítulo supondo que k é algebricamente fechado, apesar de os resultados serem também válidos para quaisquer corpos de característica zero.*

Nas próximas duas proposições analisamos os polinômios de Darboux de Δ_p que satisfazem $grau_y\ f = 1$. Antes observamos que, como os fatores irredutíveis de um polinômio de Darboux são também polinômios de Darboux (veja Proposição 4.4), podemos supor f irredutível em $k[x, y]$.

Proposição 6.1 *Seja f um polinômio de Darboux irredutível de Δ_p. Suponhamos que $grau_y f = 1$, digamos, $f = uy + v$, onde $u, v \in k[x]$, $u \neq 0$ e $mdc(u, v) = 1$. Seja $\lambda \in k[x, y]$ tal que*

$$\Delta_p(f) = \lambda f,$$

então

a) $\lambda = y + s$ para algum $s \in k[x]$;

b) grau $p = 2$ grau s (talvez ambos iguais a $-\infty$).

Prova. *a)* Desenvolvendo a igualdade $\lambda f = \Delta_p(f)$ temos

$$\begin{aligned}
\lambda.(uy + v) = \Delta_p(uy + v) &= \Delta_p(uy) + \Delta_p(v) \\
&= \Delta_p(u)y + u\Delta_p(y) + \Delta_p(v) \overset{u,v\in k[x]}{=} \\
&= u'y + u(y^2 - p) + v' \\
&= uy^2 + u'y + v' - pu, \qquad (35)
\end{aligned}$$

o que implica, comparando os graus em y, que $\lambda = y+s$ para algum $s \in k[x]$.

b) Observe que sendo $\lambda = y + s$, temos

$$\lambda f = (y + s)(uy + v) = uy^2 + (su + v)y + sv. \tag{36}$$

Comparando coeficientes em y de (35) e (36) obtemos

$$su = u' - v \quad \text{e} \quad sv = v' - pu. \tag{37}$$

Isolando v na primeira igualdade em (37) e substituindo na segunda igualdade, obtemos

$$\begin{aligned} v &= u' - su \Rightarrow \\ 0 &= v' - pu - sv \\ 0 &= (u' - su)' - pu - s(u' - su) \end{aligned}$$

$$0 = u'' - s'u - su' - pu - su' + s^2u. \tag{38}$$

Das igualdades em (37), notamos que $p = 0$ se e só se $s = 0$, e portanto vale, neste caso, da igualdade em (38) obtemos

$$grau\ p = 2\ grau\ s.$$

Agora suponhamos que $p \neq 0$ e $s \neq 0$. Então, de (37)

$$su + v = u' \Rightarrow grau\ v = grau\ s + grau\ u$$

e

$$sv = v' - pu \Rightarrow grau\ s + grau\ v = grau\ p + grau\ u.$$

Das duas implicações acima obtemos

$$grau\ s + grau\ s + grau\ u = grau\ p + grau\ u.$$

Como $u \neq 0$, obtemos

$$grau\ p = 2\ grau\ s,$$

o que completa a prova. ■

Proposição 6.2 *Seja f um polinômio irredutível em $k[x,y]$ tal que $grau_y f = 1$, digamos, $f = uy + v \in k[x,y]$, com u,$v \in k[x]$, $u \neq 0$ e $mdc(u,v) = 1$. Seja $r = -v/u \in k(x)$. Então as seguintes condições são equivalentes:*

(i) f é um polinômio de Darboux para Δ_p;

(ii) $r' = r^2 - p(x)$.

Prova. *(i)⇒(ii)* Decorre do Corolário 4.10.

(ii)⇒(i) É imediato do Teorema 4.8 e da unicidade do polinômio irredutível de Darboux de Δ_p (Teorema 4.6). ■

O teorema a seguir nos auxiliará no principal resultado deste trabalho, que é o teorema 6.4.

Teorema 6.3 *Se a derivação Δ_p não é simples sobre $k[x,y]$, então existe um único polinômio irredutível de Darboux $f \in k[x,y]$ de Δ_p. Além disso $grau_y\ f = 1$.*

Prova. Por hipótese Δ_p não é simples. Pelo Teorema 4.6 existe e é único $f(x,y) \in k[x,y]$ polinômio irredutível de Darboux de Δ_p. Além disso $grau_y\ f \geq 1$. Seja $r \in \overline{k(x)}$ uma raíz de $f(x,y) \in \overline{k(x)}[y]$. Pelo Corolário 4.10 temos

$$r' = r^2 - p.$$

Sendo assim, r é uma solução algébrica da equação diferencial

$$r' = r^2 - p.$$

Pelo Teorema 5.1, esta solução é racional, isto é, $r \in k(x)$.

Como $r \in k(x)$ e é raiz do polinômio irredutível $f(x,y)$, então $grau_y$ $f = 1$. Se $r = 0$ então $p = 0$; daí Δ_p não é simples, pois $f = y$ é polinômio de Darboux de Δ_p. Se $r \neq 0$, existem $u, v \in k[x]$, $u \neq 0$ e $mdc(u,v) = 1$ tais que $r = -\dfrac{v}{u}$, pela Proposição 6.2 temos $f(x,y) = uy + v$ é um polinômio de Darboux de Δ_p. ■

Teorema 6.4 *Se p é um polinômio não nulo e de grau ímpar, então Δ_p é uma derivação simples.*

Prova. Suponhamos que Δ_p não seja simples. Pelo Teorema 6.3, existe um polinômio de Darboux f para Δ_p tal que grau_y $f = 1$.

Pela Proposição 6.1, se λ denota o autovalor de f então

$$\lambda = y + s,$$

para algum $s \in k[x]$ e $grau(p) = 2\, grau(s)$. Então $grau(p)$ é um número par, o que completa a prova. ■

No entanto algumas derivações Δ_p com $grau(p)$ par são também simples:

Proposição 6.5 *Toda derivação $d : k[x,y] \longrightarrow k[x,y]$ da forma*

$$d = \frac{\partial}{\partial x} + (y^2 \pm x^n)\frac{\partial}{\partial y}, \quad n \in \mathbb{N}^*.$$

é simples.

Prova. Se n é ímpar então d é simples, pelo teorema acima.

Suponhamos então que $n = 2m$, com $m \in \mathbb{N}^*$, e que d não é simples. Então pelo Teorema 6.3 existe f um polinômio de Darboux de d da forma

$$f = uy + v,$$

onde $u, v \in k[x]$ e $u \neq 0$. Pela Proposição 6.1 temos que se λ denota o autovalor de f então $\lambda = y + s$ para algum $s \in k[x]$. Além disso, necessariamente $n = 2grau\ s$ e por (38) temos

$$0 = u'' - s'u - 2su' + s^2u - pu = u'' - s'u - 2su' + (s^2 - p)u. \tag{39}$$

Como $p = \pm x^{2m}$, temos que $grau\ s = m$. É fácil ver que $grau\ u''$, $grau\ s'u$, $grau\ 2su'$ são todos estritamente menores do que $grau\ s + grau\ u = m + grau\ u$; concluímos então que os graus maiores ou iguais do que $m + grau\ u$ estão todos envolvidos exclusivamente na parcela $(s^2 - p)u$ e devem então se anular. Ou ainda, como $u \neq 0$, que os coeficientes de grau maior ou igual do que m em $s^2 - p$ devem todos se anular.

Como $s \neq 0$, pois $2\ grau\ s = n \geq 1$, podemos escrever

$$s = s_m x^m + ... + s_1 x + s_0 = \sum_{k=0}^{m} s_k x^k,$$

onde $s_0, ..., s_m \in k$ e $s_m \neq 0$, temos

$$s^2 - p = \left(\sum_{k=0}^{2m} \sum_{i+j=k} s_i s_j x^k \right) \mp x^{2m}.$$

Como os coeficientes dos termos de grau maior ou igual do que m, de $s^2 - p$ são nulos obtemos

$$s_m^2 \mp 1 = 0 \tag{40}$$

e, para $k \in \{m, m+1, ..., 2m-1\}$,

$$\sum_{i+j=k} s_i s_j = 0,$$

Como k é algebricamente fechado, um tal s_m existe e é não nulo. Por indução decrescente vamos obter

$$s_{m-1} = s_{m-2} = ... = s_1 = s_0 = 0.$$

Segue daí que $s = s_m x^m$ e (39) se reescreve neste caso na forma

$$\begin{aligned} 0 &= u'' - m s_m x^{m-1} u - 2 s_m x^m u' + (s_m^2 x^{2m} \mp x^{2m}) u \\ &\overset{(40)}{=} u'' - m s_m x^{m-1} u - 2 s_m x^m u'. \end{aligned} \tag{41}$$

Sejam l coeficiente líder de u e $t =$ grau u. Como $u \neq 0$, temos $t \geq 1$. Se $t = 0$ então $u \in k$ e em (41) temos

$$0 = -m s_m x^{m-1} u,$$

mas m, s_m, u não são nulos, absurdo. Segue então

$$grau\ u'' < grau(m s_m x^{m-1} u) = grau(2 s_m x^m u'),$$

portanto o coeficiente do termo de maior grau em (41) é

$$-m s_m l - 2 s_m l t = -s_m l (m + 2t),$$

que deve então se anular. Como $s_m \neq 0$ e $l \neq 0$, segue que

$$m + 2t = 0,$$

que é uma contradição, pois $t \geq 0$ e $m > 0$.

Portanto, não existe polinômio de Darboux para d, ou seja, d é simples, como queríamos demonstrar. ■

Proposição 6.6 *Toda derivação d de $k[x, y]$ da forma*

$$d = \frac{\partial}{\partial x} + (y^2 - x^{2m} + m x^{m-1}) \frac{\partial}{\partial y}, \quad m \in \mathbb{N}^*.$$

não é simples e seu polinômio irredutível de Darboux é $y - x^m$.

Prova. Note que

$$\begin{aligned} d(y - x^m) &= \frac{\partial}{\partial x}(y - x^m) + (y^2 - x^{2m} + m x^{m-1}) \frac{\partial}{\partial y}(y - x^m) \\ &= -m x^{m-1} + y^2 - x^{2m} + m x^{m-1} \\ &= y^2 - x^{2m} = (y + x^m)(y - x^m), \end{aligned}$$

e portanto $f = y - x^m$ é polinômio de Darboux de d e $y + x^m$ é seu auto valor. ■

Observação 6.7 *Na demonstração acima, chegamos ao polinômio de Darboux $y - x^m$ com o seguinte raciocínio: pelo Teorema 6.3, se d não for simples então existe um polinômio de Darboux de grau 1 em y. Ainda, se isto acontecer, pela Proposição 6.1, temos que se λ denota o autovalor de f então $\lambda = y + s$ para algum $s \in k[x]$.*

Inicialmente supondo que existe um polinômio $f = uy + v$, com $u, v \in k[x]$, $u \neq 0$ tal que $d(f) = \lambda f$. Como na prova da Proposição 6.5, chegaremos a

$$u'' - s'u - 2su' + s^2u - (x^{2m} - mx^{m-1})u = 0. \tag{42}$$

Seguindo com a mesma idéia da prova proposição 6.5, obteremos $m =$ grau s, digamos,

$$s = \sum_{k=0}^{m} s_k x^k,$$

donde

$$s^2 = \sum_{k=0}^{2m} \sum_{i+j=k} s_i s_j x^k,$$

e substituindo na expressão (42), obtemos

$$\begin{aligned} 0 &= u'' - s'u - 2su' + u\sum_{k=0}^{2m} \sum_{i+j=k} s_i s_j x^k - (x^{2m} - mx^{m-1})u \\ &= u'' - s'u - 2su' \\ &+ u\left[(s_m^2 - 1)x^{2m} + \sum_{k=m}^{2m-1} \sum_{i+j=k} s_i s_j x^k + \left(m + \sum_{i+j=m-1} s_i s_j\right) x^{m-1} + \sum_{k=0}^{m-2} \sum_{i+j=k} s_i s_j x^k\right] \end{aligned}$$

Como grau u'', grau $s'u$, grau $2su'$ são todos estritamente menores do que $m +$ grau u, concluímos que os coeficientes dos termos de grau maior ou igual a $m +$ grau u são todos provenientes exclusivamente da expressão entre colchetes.

Assim, obteremos

$$s_m^2 = 1,$$
$$\sum_{i+j=k} s_i s_j = 0, \text{ para } k \in \{m, ..., 2m-1\},$$

o que nos dá

$$s_m = \pm 1,$$

e, por indução decrescente, vamos obter

$$s_{m-1} = s_{m-2} = ... = s_1 = s_0 = 0.$$

Portanto $s = \pm x^m$ *e (42) fica*

$$\begin{aligned} 0 &= u'' - s_m m x^{m-1} u - 2 s_m x^m u' + x^{2m} u - x^{2m} u + m x^{m-1} u \\ &= u'' - s_m m x^{m-1} u - 2 s_m x^m u' + m x^{m-1} u \\ &= u'' + (-s_m m + m) x^{m-1} u - 2 s_m x^m u' \end{aligned}$$

Claramente a expressão acima envolve termos de grau no máximo igual a $m - 1 + grau\ u$ *(lembre que* $u \neq 0$*). Assim, se* l *denota o coeficiente líder de* u *e* $t = grau\ u$ *então, olhando o coeficiente do termo de grau* $m - 1 + grau\ u$*, obtemos*

$$(-s_m m + m) l - 2 s_m t l = 0,$$

e como $l \neq 0$*, chegamos a*

$$-s_m m + m - 2 s_m t = 0. \tag{43}$$

Daí, se $s_m = -1$*, obtemos*

$$m + m + 2t = 0,$$

o que é um absurdo, pois $m > 0$ *e* $t \geq 0$. *Concluímos então que* $s_m = 1$, $s = x^m$ *e, de (43) que*

$$0 = -m + m - 2t = -2t,$$

o que implica $t = 0$ *e conseqüentemente* u *é constante.*

Agora por (37) temos $v = -us$, *portanto,*

$$f = uy + v = uy - ux^m$$

com $u \in k^*$. *Logo, módulo produto por um elemento de* k^*, $y - x^m$ *é o polinômio irredutível de Darboux de* Δ_p *de* $k[x, y]$. *Pela Proposição 6.1 a) seu autovalor é* $\lambda = y + s$, *isto é,* $y + x^m$.

7 APÊNDICE

7.1 Prova da Afirmação 4 do Teorema 5.1:

Se $f(x,y)=\prod_{i=1}^{n}(y-t_i)$ *então seu discriminante*

$$\Delta=(-1)^{n(n-1)/2}\prod_{i\neq j}(t_i-t_j)\in k(x)$$

satisfaz a igualdade

$$d(\Delta)=(-1)^{n(n-1)/2}\sum_{i\neq j}d(t_i-t_j)\prod_{m\neq k,\ (m,k)\neq(i,j)}(t_m-t_k).$$

Prova. Como $d(\Delta)=(-1)^{n(n-1)/2}d\left(\prod_{i\neq j}(t_i-t_j)\right)$, não precisamos nos preocupar com o fator $(-1)^{n(n-1)/2}$. Provaremos por indução sobre n que

$$d\left(\prod_{i\neq j}(t_i-t_j)\right)=\sum_{i\neq j}d(t_i-t_j)\prod_{m\neq k,\ (m,k)\neq(i,j)}(t_m-t_k).$$

Para $n=2$ temos:

$$\begin{aligned}d\left(\prod_{i,j\in\{1,2\},i\neq j}(t_i-t_j)\right)&=d[(t_1-t_2)(t_2-t_1)]\\&=d(t_1-t_2)(t_2-t_1)+(t_1-t_2)d(t_2-t_1)\\&=\sum_{i,j\in\{1,2\},i\neq j}d(t_i-t_j)\prod_{m\neq k,\ (m,k)\neq(i,j)}(t_m-t_k)\end{aligned}$$

Suponhamos que para $n\geq 2$ vale

$$d\left(\prod_{i,j\in\{1,\ldots,n\},i\neq j}(t_i-t_j)\right)=\sum_{i,j\in\{1,\ldots,n\},i\neq j}d(t_i-t_j)\prod_{m,k\in\{1,..,n\},\ m\neq k,\ (m,k)\neq(i,,j)}(t_m-t_k).$$

Daí:

$$
\begin{aligned}
& d\left(\prod_{i,j\in\{1,\ldots,n,n+1\},\ i\neq j}(t_i-t_j)\right)\\
&= d\left(\prod_{i,j\in\{1,\ldots,n\},\ i\neq j}(t_i-t_j)\prod_{r\in\{1,\ldots,n\}}(t_{n+1}-t_r)\prod_{s\in\{1,\ldots,n\}}(t_s-t_{n+1})\right)\\
&= d\left(\prod_{i,j\in\{1,\ldots,n\},\ i\neq j}(t_i-t_j)\right)\prod_{r\in\{1,\ldots,n\}}(t_{n+1}-t_r)\prod_{s\in\{1,\ldots,n\}}(t_s-t_{n+1})\\
&+\prod_{i,j\in\{1,\ldots,n\},\ i\neq j}(t_i-t_j)\ \ d\left(\prod_{r\in\{1,\ldots,n\}}(t_{n+1}-t_r)\right)\prod_{s\in\{1,\ldots,n\}}(t_s-t_{n+1})\\
&+\prod_{i,j\in\{1,\ldots,n\},\ i\neq j}(t_i-t_j)\prod_{r\in\{1,\ldots,n\}}(t_{n+1}-t_r)\ \ d\left(\prod_{s\in\{1,\ldots,n\}}(t_s-t_{n+1})\right)\\
&\overset{HI}{=}\sum_{i,j\in\{1,\ldots,n\},i\neq j}d(t_i-t_j)\prod_{\substack{m,k\in\{1,..,n\},\\ m\neq k,\ (m,k)\neq(i,,j)}}(t_m-t_k)\prod_{r\in\{1,\ldots,n\}}(t_{n+1}-t_r)\prod_{s\in\{1,\ldots,n\}}(t_s-t_{n+1})\\
&+\sum_{r\in\{1,\ldots,n\}}d(t_{n+1}-t_r)\prod_{m\in\{1,\ldots,n\},\ m\neq r}(t_{n+1}-t_m)\prod_{i,j\in\{1,\ldots,n\},\ i\neq j}(t_i-t_j)\prod_{s\in\{1,\ldots,n\}}(t_s-t_{n+1})\\
&+\sum_{s\in\{1,\ldots,n\}}d(t_s-t_{n+1})\prod_{k\in\{1,\ldots,n\},\ k\neq s}(t_k-t_{n+1})\prod_{i,j\in\{1,\ldots,n\},\ i\neq j}(t_i-t_j)\prod_{r\in\{1,\ldots,n\}}(t_{n+1}-t_r)\\
&=\sum_{i,j\in\{1,\ldots,n\},i\neq j}d(t_i-t_j)\prod_{m,k\in\{1,..,n+1\},\ m\neq k,\ (m,k)\neq(i,,j)}(t_m-t_k)\\
&+\sum_{r\in\{1,\ldots,n\}}d(t_{n+1}-t_r)\prod_{m,k\in\{1,..,n+1\},\ m\neq k,\ (m,k)\neq(n+1,r)}(t_m-t_k)\\
&+\sum_{s\in\{1,\ldots,n\}}d(t_s-t_{n+1})\prod_{m,k\in\{1,..,n+1\},\ m\neq k,\ (m,k)\neq(s,n+1)}(t_m-t_k)\\
&=\sum_{i,j\in\{1,\ldots,n+1\},i\neq j}d(t_i-t_j)\prod_{m,k\in\{1,..,n+1\},\ m\neq k,\ (m,k)\neq(i,,j)}(t_m-t_k)
\end{aligned}
$$

■

7.2 Prova da Afirmação 10 do Teorema 5.1:

Seja α um dos pólos de $a = \sigma_1$ (veja (17)). Então, para todo $i \in \{1, 2, ..., n\}$,

i) α é um pólo de σ_i com ordem no máximo i;

ii) se denotarmos por $\overline{\sigma_i}$ a parte de σ_i que envolve o pólo α de ordem i então

$$i!\overline{\sigma_i} = \frac{\lambda_\alpha(\lambda_\alpha + 1)...(\lambda_\alpha + i - 1)}{(x-\alpha)^i}, \tag{44}$$

Prova. A prova é por indução sobre i. Por (17),

$$\sigma_1 = \sum_{\alpha \in R} \frac{\lambda_\alpha}{x - \alpha}, \tag{45}$$

e então é claro que α é um pólo de σ_1 com ordem 1. Além disso,

$$\overline{\sigma_1} = \frac{\lambda_\alpha}{(x-\alpha)},$$

portanto *(44)* é satisfeita para $i = 1$.

Para $i = 2$ temos (veja (22))

$$\sigma_2 = \frac{1}{2}(a\sigma_1 - \sigma_1' - np).$$

Como

$$a\sigma_1 = \sigma_1\sigma_1 = \sum_{\alpha \in R} \frac{\lambda_\alpha^2}{(x-\alpha)^2} + \sum_{\alpha,\beta \in R,\ \beta \neq \alpha} \frac{\lambda_\alpha \lambda_\beta}{(x-\beta)(x-\alpha)}$$

e

$$-\sigma_1' = -(\sum_{\alpha \in R} \frac{\lambda_\alpha}{x-\alpha})' = \sum_{\alpha \in R} \frac{\lambda_\alpha}{(x-\alpha)^2},$$

temos

$$\begin{aligned}\sigma_2 &= \frac{1}{2}\left(\sum_{\alpha \in R} \frac{\lambda_\alpha^2}{(x-\alpha)^2} + \sum_{\alpha,\beta \in R,\ \beta \neq \alpha} \frac{\lambda_\alpha \lambda_\beta}{(x-\beta)(x-\alpha)} + \sum_{\alpha \in R} \frac{\lambda_\alpha}{(x-\alpha)^2} - np\right) \\ &= \frac{1}{2}\left(\sum_{\alpha \in R} \frac{\lambda_\alpha^2 + \lambda_\alpha}{(x-\alpha)^2} + \sum_{\alpha,\beta \in R,\ \beta \neq \alpha} \frac{\lambda_\alpha \lambda_\beta}{(x-\beta)(x-\alpha)} - np\right).\end{aligned}$$

Assim, vemos que α é pólo de σ_2 de ordem no máximo 2.

Além disso,

$$\overline{\sigma_2} = \frac{1}{2}\frac{\lambda_\alpha^2 + \lambda_\alpha}{(x-\alpha)^2},$$

donde

$$2!\overline{\sigma_2} = \frac{\lambda_\alpha(\lambda_\alpha+1)}{(x-\alpha)^2}.$$

Deste modo, *ii)* vale para $i = 2$.

Suponhamos que *i)* e *ii)* valem para $i \in \{2, ..., n-1\}$.

Por (23), temos que

$$\sigma_{i+1} = \frac{1}{i+1}(a\sigma_i - \sigma_i' - (n-i+1))p\sigma_{i-1}).$$

Mas

$$a\sigma_i = \sigma_1\sigma_i \overset{HI\ (ii)}{\underset{(45)}{=}} \sum_{\alpha\in R}\frac{\lambda_\alpha}{x-\alpha}\frac{1}{i!}\frac{\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+i-1)}{(x-\alpha)^i}$$

$$+ \text{ parcelas envolvendo o pólo } \alpha \text{ com ordem } \leq i$$

$$= \sum_{\alpha\in R}\frac{1}{i!}\frac{\lambda_\alpha(\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+i-1))}{(x-\alpha)^{i+1}} + \text{parcelas envolvendo } \alpha \text{ com ordem } \leq i;$$

por outro lado,

$$\sigma_i' \overset{HI\ (ii)}{=} \left(\frac{1}{i!}\frac{\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+i-1)}{(x-\alpha)^i} + \text{parcelas envolvendo } \alpha \text{ com ordem } \leq i-1\right)'$$

$$= -\frac{1}{i!}\frac{i.\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+i-1)}{(x-\alpha)^{i+1}} + \text{parcelas envolvendo } \alpha \text{ com ordem } \leq i;$$

ainda, por hipótese, a ordem do pólo α em σ_{i-1} é no máximo $i-1$. Concluímos então que α é um pólo de σ_{i+1} com ordem no máximo $i+1$. Além disso,

$$\begin{aligned}\overline{\sigma_{i+1}} &= \frac{1}{i+1}\ \frac{1}{i!}\ \frac{\lambda_\alpha(\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+i-1))}{(x-\alpha)^{i+1}} + \\ &+ \frac{1}{i+1}\ \frac{1}{i!}\ \frac{i(\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+i-1)}{(x-\alpha)^{i+1}}) \\ &= \frac{1}{(i+1)!}\ \frac{\lambda_\alpha(\lambda_\alpha+1)...(\lambda_\alpha+i-1)(\lambda_\alpha+i)}{(x-\alpha)^{i+1}},\end{aligned}$$

e portanto, *(ii)* é também satisfeita por σ_{i+1}. ■

7.3 Prova da Afirmação 12 do Teorema 5.1:

Se $\delta = grau(p)$ então, para cada $i \in \mathbb{N}$,

$$grau(\sigma_{2i}) = i\delta \quad enquanto\ 2i \leq n$$
$$grau(\sigma_{2i+1}) \leq i\delta - 1.$$

Prova. A prova é feita por indução sobre i.

Inicialmente observemos que se $f(x), g(x) \in k[x]$ então

$$grau\left(\frac{f}{g}\right)' \leq grau\ f - grau\ g - 1 = grau\left(\frac{f}{g}\right) - 1,$$

uma vez que

$$\left(\frac{f}{g}\right)' = \frac{f\,'g - fg'}{g^2}.$$

Sendo $\sigma_0 = 1$ temos que $grau(\sigma_0) = 0 = 0\delta$, e da Afirmação 5,

$$\sigma_{2\times 0+1} = \sigma_1 = \frac{d(\Delta)}{2(n-1)\Delta},$$

onde $\Delta \in k(x)$; então $grau\ \sigma_1 \leq 0\delta - 1 = -1$.

Seja $k \in \{0, 1, ..., n-1\}$ e suponhamos que

$$grau(\sigma_{2i}) = i\delta \ \text{ e } \ grau(\sigma_{2j+1}) \leq j\delta - 1,$$

enquanto $2i \leq k$ e $2j + 1 \leq k$. Daí:

- se k for ímpar então, como $k + 1 \leq n$ e pondo $k + 1 = 2(i + 1)$, temos

$$\begin{aligned}\sigma_{k+1} = \sigma_{2(i+1)} &\overset{(23)}{=} \frac{1}{2(i+1)}(a\sigma_{2i+2-1} - \sigma'_{2i+2-1} - (n+2-2i-2)p\sigma_{2i+2-2}) \\ &= \frac{1}{2i+2}(a\sigma_{2i+1} - \sigma'_{2i+1} - (n-2i)p\sigma_{2i});\end{aligned}$$

daí, pela hipótese de indução, temos:

$grau\ (a\sigma_{2i+1}) = grau\ (\sigma_1\sigma_{2i+1}) \leq -1 + i\delta - 1 = i\delta - 2,$

$grau\ \sigma'_{2i+1} \leq grau\ \sigma_{2i+1} - 1 \overset{HI}{\leq} i\delta - 1 - 1 = i\delta - 2$

$grau\ p\sigma_{2i} \overset{HI}{=} \delta + i\delta = (i+1)\delta,$

de modo que, neste caso, obtemos

$$grau\ \sigma_{k+1} = grau(\sigma_{2(i+1)}) = (i+1)\delta.$$

- se k for par então, como $k+1 \leq n$ e pondo $k+1 = 2i$, temos

$$\begin{aligned}\sigma_{k+1} = \sigma_{2i+1} &\overset{(23)}{=} \frac{1}{2i+1}(a\sigma_{2i+1-1} - \sigma'_{2i+1-1} - (n+2-2i-1)p\sigma_{2i+1-2}) \\ &= \frac{1}{2i+1}(a\sigma_{2i} - \sigma'_{2i} - (n-2i+1)p\sigma_{2i-1});\end{aligned}$$

daí, pela hipótese de indução, temos:

$grau\ (a\sigma_{2i}) = grau\ (\sigma_1\sigma_{2i}) = -1 + i\delta = i\delta - 1,$
$grau\ \sigma'_{2i} \overset{HI}{\leq} i\delta - 1$
$grau\ p\sigma_{2i-1} = grau\ p\sigma_{2(i-1)+1} \overset{HI}{\leq} \delta + (i-1)\delta - 1 = i\delta - 1,$

de modo que, neste caso, obtemos

$$grau\ \sigma_{k+1} = grau(\sigma_{2i+1}) \leq i\delta - 1.$$

Logo $grau(\sigma_{2i}) = i\delta$ enquanto $2i \leq n$ e $grau(\sigma_{2i+1}) \leq i\delta - 1$ para todo $i \in \mathbb{N}$. ■

7.4 Prova da Afirmação 13 do Teorema 5.1:

Dado $s \in \mathbb{N}$, *tem-se*

$$\widehat{\sigma_{2s}} = (-1)^s \widehat{p}^s M_{2s}, \quad \text{enquanto } 2s \leq n+1$$

e

$$\widehat{\sigma_{2s+1}} = (-1)^{s+1} \widehat{p}^s M_{2s+1}, \quad \text{enquanto } 2s+1 \leq n+1,$$

onde M_i *são racionais definidos indutivamente por:*

$$M_0 = 1, \qquad M_1 = \Lambda$$

e, para $s \geq 1$,

$$M_{2s} = \frac{n+2-2s}{2s} M_{2(s-1)}$$

e

$$M_{2s+1} = \frac{1}{2s+1}[(\Lambda + s\delta)M_{2s} + (n+1-2s)M_{2s-1}].$$

Prova. A prova é por indução sobre s.

Para $s = 0$ temos

$$\widehat{\sigma_0} = 1 = (-1)^0 \widehat{p}^0 M_{2\times 0}$$

e

$$\widehat{\sigma_1} \overset{(25)}{=} -\Lambda \ = (-1)^1 \widehat{p}^0 M_1$$

Suponhamos que, dado $i \in \mathbb{N}$ tal que $2(i+1) \leq n+1$, tenhamos

$$\widehat{\sigma_{2i}} = (-1)^i \widehat{p}^i M_{2i}$$

Daí, como $2(i+1) \leq n+1$, podemos aplicar (26) e (27) e obter

$$\begin{aligned}
&\widehat{\sigma_{2(i+1)}} = \\
&= -\frac{1}{2(i+1)}(n+2-2(i+1))p\widehat{\sigma_{2(i+1)-2}} \\
&= -\frac{1}{2(i+1)}(n-2i)\widehat{p}\widehat{\sigma_{2i}} \overset{HI}{=} \\
&= -\frac{1}{2(i+1)}(n-2i)\widehat{p}(-1)^i\widehat{p}^i M_{2i} \\
&= \frac{(n-2i)}{2(i+1)}(-1)^{i+1}\widehat{p}^{i+1}M_{2i}.
\end{aligned}$$

Note ainda que

$$\begin{aligned}
M_{2(i+1)} &= \frac{(n+2-2(i+1))}{2(i+1)}M_{2i} \\
&= \frac{(n-2i)}{2(i+1)}M_{2i}
\end{aligned}$$

e portanto

$$\widehat{\sigma_{2(i+1)}} = (-1)^{i+1}\widehat{p}^{i+1}M_{2(i+1)}, \tag{46}$$

enquanto $2(i+1) \leq n+1$.

Suponhamos agora que dado $i \in \mathbb{N}$ tal que $2(i+1)+1 \leq n+1$ tenhamos

$$\widehat{\sigma_{2i}} = (-1)^i\widehat{p}^i M_{2i} \quad \text{e} \quad \widehat{\sigma_{2i+1}} = (-1)^{i+1}\widehat{p}^i M_{2i+1}.$$

Então vale (46). Ainda, como $\sigma'_{2(i+1)}$ tem grau $\leq (i+1)\delta - 1$, temos, por (46),

$$\widehat{\sigma'_{2(i+1)}} = (i+1)\delta(-1)^{i+1}\widehat{p}^{i+1}M_{2(i+1)}, \tag{47}$$

de modo que, como $2(i+1)+1 \leq n+1$, podemos aplicar (26) e (27) e obter

$$
\begin{aligned}
&\widehat{\sigma_{2(i+1)+1}} = \\
&= \frac{1}{2(i+1)+1}\left[\widehat{a\sigma_{2(i+1)}} - \widehat{\sigma'_{2(i+1)}} - (n-2(i+1)+1)\widehat{p\sigma_{2(i+1)-1}}\right] \overset{(47),(25)}{\underset{(46)}{=}} \\
&= \frac{1}{2(i+1)+1}\left[-\Lambda(-1)^{i+1}\widehat{p}^{i+1}M_{2(i+1)} - (i+1)\delta(-1)^{i+1}\widehat{p}^{i+1}M_{2(i+1)} - (n-2i-1)\widehat{p\sigma_{2i+1}}\right] = \\
&= \frac{1}{2(i+1)+1}\left[\Lambda(-1)^{i}\widehat{p}^{i+1}M_{2(i+1)} + (i+1)\delta(-1)^{i}\widehat{p}^{i+1}M_{2(i+1)} - (n-2i-1)\widehat{p\sigma_{2i+1}}\right] \overset{HI}{=} \\
&= \frac{1}{2(i+1)+1}\left[\Lambda(-1)^{i}\widehat{p}^{i+1}M_{2(i+1)} + (i+1)\delta(-1)^{i}\widehat{p}^{i+1}M_{2(i+1)} - (n-2i-1)\widehat{p}(-1)^{i+1}\widehat{p}^{i}M_{2i+1}\right] \\
&= \frac{1}{2(i+1)+1}\left[\Lambda(-1)^{i}\widehat{p}^{i+1}M_{2(i+1)} + (i+1)\delta(-1)^{i}\widehat{p}^{i+1}M_{2(i+1)} + (n-2i-1)(-1)^{i}\widehat{p}^{i+1}M_{2i+1}\right] \\
&= \frac{1}{2(i+1)+1}(-1)^{i}\widehat{p}^{i+1}\left[M_{2(i+1)}(\Lambda + (i+1)\delta) + (n-2i-1)M_{2i+1}\right].
\end{aligned}
$$

Por outro lado,

$$
\begin{aligned}
M_{2(i+1)+1} &= \frac{1}{2(i+1)+1}\left[(\Lambda + (i+1)\delta)M_{2(i+1)} + (n+1-2(i+1))M_{2(i+1)-1}\right] \\
&= \frac{1}{2(i+1)+1}[M_{2(i+1)}(\Lambda + (i+1)\delta) + (n-2i-1)M_{2i+1}],
\end{aligned}
$$

e portanto

$$
\widehat{\sigma_{2(i+1)+1}} = (-1)^{i}\widehat{p}^{i+1}M_{2(i+1)+1} = (-1)^{i+2}\widehat{p}^{i+1}M_{2(i+1)+1},
$$

enquanto $2(i+1)+1 \leq n$. ∎

7.5 Prova da Afirmação 15 do Teorema 5.1:

Para todo $i \in \mathbb{N}$,

$$\sigma_{2i+1} = 0$$

e, enquanto $2i \leq n$,

$$\sigma_{2i} = (-1)^i \binom{s}{i} p^i.$$

Prova. A prova é por indução sobre i.

Inicialmente observamos $p \neq 0$ e p constante implica que $\widehat{p} = p$.

Daí, para $i = 0$ temos

$$\sigma_0 = 1 = (-1)^0 \binom{s}{0} p^0 \quad \text{e} \quad \sigma_1 \overset{(33)}{=} 0.$$

Seja $i \geq 0$ e suponhamos que, por indução, tenhamos

$$\sigma_{2i+1} = 0 \qquad \text{e,} \;\; \sigma_{2i} = (-1)^i \binom{s}{i} p^i \text{ se } 2i < n.$$

Então se $2(i+1) \leq n$ temos

$$\begin{aligned}
\sigma_{2(i+1)} &\overset{(22)}{=} \frac{1}{2(i+1)} \left[a\sigma_{2(i+1)-1} - \sigma'_{2(i+1)-1} - (n+2-2(i+1))p\sigma_{2(i+1)-2} \right] \\
&= \frac{1}{2(i+1)} \left[a\sigma_{2i+1} - \sigma'_{2i+1} - (n-2i)p\sigma_{2i} \right] \overset{HI: \sigma_{2i+1}=0, \text{ portanto } \sigma'_{2i+1}=0}{=} \\
&= -\frac{n-2i}{2(i+1)} p\sigma_{2i} \overset{HI}{=} \\
&= -\frac{n-2i}{2(i+1)} p(-1)^i \binom{s}{i} p^i \overset{n=2s}{=} \\
&= (-1)^{i+1} p^{i+1} \frac{2(s-i)}{2(i+1)} \frac{s!}{i!(s-i)!} \\
&= (-1)^{i+1} p^{i+1} \frac{s!}{(i+1)!(s-i-1)!} \\
&= (-1)^{i+1} \binom{s}{i+1} p^{i+1}
\end{aligned}$$

Também se $2(i+1)+1 \leq n$, temos

$$\sigma_{2(i+1)+1} \overset{(22)}{=} \frac{1}{2(i+1)+1}\left[a\sigma_{2(i+1)+1-1} - \sigma'_{2(i+1)+1-1} - (n+2-(2(i+1)+1))p\sigma_{2(i+1)+1-2}\right]$$

$$= \frac{1}{2i+3}[a\sigma_{2(i+1)} - \sigma'_{2(i+1)} - (n-2i-\ 1)p\sigma_{2i+1}] \underset{HI:\ \sigma_{2i+1}=0,\ \text{portanto}\ \sigma'_{2i+1}=0}{\overset{a=0}{=}} 0,$$

o que completa a prova. ■

7.6 Prova da Afirmação 16 do Teorema 5.1:

Para cada $j \in \{1, 2, ..., n\}$, *tem-se*

$$\sigma_j = \sum_{1 \leq i_1 < i_2 < ... < i_j \leq m}^{l} \frac{(-1)^j}{(x - \alpha_{i_1})(x - \alpha_{i_2})...(x - \alpha_{i_j})}.$$

Prova. A prova é por indução sobre j. Relembremos que reescrevemos

$$\sigma_1 = \sum_{\alpha \in R} \frac{\lambda_\alpha}{(x - \alpha)}$$

na forma

$$\sigma_1 = \sum_{i=1}^{m} \frac{-1}{(x - \alpha_i)},$$

levando em conta que o conjunto R é finito e que $\lambda_\alpha \in \{-1, -2, ..., -n\}$, onde $m = -\sum_{\alpha \in R} \lambda_\alpha$

Lembrando que $a = \sigma_1$, temos

$$a\sigma_1 = \sigma_1^2 = \sum_{i=1}^{m} \frac{+1}{(x - \alpha_i)^2} + \sum_{1 \leq i_1 < i_2 \leq m} \frac{2}{(x - \alpha_{i_1})(x - \alpha_{i_2})}$$

e

$$\sigma_1' = \sum_{i=1}^{m} \frac{1}{(x - \alpha_i)^2};$$

daí, lembrando que $p = 0$, segue que

$$\sigma_2 \overset{(22)}{=} \frac{a\sigma_1 - \sigma_1'}{2} = \sum_{1 \leq i_1 < i_2 \leq m} \frac{1}{(x - \alpha_{i_1})(x - \alpha_{i_2})},$$

e portanto a afirmação vale para $j = 2$.

Suponhamos que para $j \in \{2, ..., n - 1\}$ vale

$$\sigma_j = \sum_{1 \leq i_1 < i_2 < ... < i_j \leq m} \frac{(-1)^j}{(x - \alpha_{i_1})(x - \alpha_{i_2})...(x - \alpha_{i_j})}.$$

Por (22) obtemos

$$\sigma_{j+1} = \frac{a\sigma_j - \sigma_j'}{j + 1}$$

Mas

$$
\begin{aligned}
&a\sigma_j \overset{HI}{=} \\
&= \left(\sum_{i=1}^{m} \frac{-1}{(x-\alpha_i)}\right)\left(\sum_{1\le i_1<i_2<\ldots<i_j\le m} \frac{(-1)^j}{(x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})}\right) \\
&= \sum_{i=1}^{m}\sum_{1\le i_1<i_2<\ldots<i_j\le m} \frac{(-1)^{j+1}}{(x-\alpha_i)(x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})} \\
&= \sum_{1\le i_1<i_2<\ldots<i_j\le m} \frac{(-1)^{j+1}}{(x-\alpha_{i_1})^2(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})} \\
&+ \sum_{1\le i_1<i_2<\ldots<i_j\le m} \frac{(-1)^{j+1}}{(x-\alpha_{i_1})(x-\alpha_{i_2})^2\ldots(x-\alpha_{i_j})} \\
&+ \ldots \\
&+ \sum_{1\le i_1<i_2<\ldots<i_j\le m} \frac{(-1)^{j+1}}{(x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})^2} \\
&+ \sum_{1\le i_1<i_2<\ldots<i_j\le m}\ \sum_{i\in\{1,\ldots,m\}\setminus\{i_1,\ldots,i_j\}} \frac{(-1)^{j+1}}{(x-\alpha_i)(x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})}
\end{aligned}
$$

e

$$
\begin{aligned}
\sigma_j' &= \left(\sum_{1\le i_1<i_2<\ldots<i_j\le m} \frac{(-1)^j}{(x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})}\right)' \\
&= \sum_{1\le i_1<i_2<\ldots<i_j\le m} \frac{-((x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j}))'(-1)^j}{((x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j}))^2} \\
&= \sum_{1\le i_1<i_2<\ldots<i_j\le m} \frac{(-1)^{j+1}}{(x-\alpha_{i_1})^2(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})} \\
&+ \sum_{1\le i_1<i_2<\ldots<i_j\le m} \frac{(-1)^{j+1}}{(x-\alpha_{i_1})(x-\alpha_{i_2})^2\ldots(x-\alpha_{i_j})} \\
&\ldots \\
&+ \sum_{1\le i_1<i_2<\ldots<i_j\le m} \frac{(-1)^{j+1}}{(x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})^2};
\end{aligned}
$$

então, depois dos cancelamentos obtemos

$$\begin{aligned}\sigma_{j+1} &= \frac{1}{j+1}\sum_{1\leq i_1<i_2<\ldots<i_j\leq m}\ \sum_{i\in\{1,\ldots,m\}\setminus\{i_1,\ldots,i_j\}}\frac{(-1)^{j+1}}{(x-\alpha_i)(x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})}\\ &= \frac{1}{j+1}\sum_{1\leq i_1<i_2<\ldots<i_j<i_{j+1}\leq m}\frac{(j+1)(-1)^{j+1}}{(x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})(x-\alpha_{i_{j+1}})}\\ &= \sum_{1\leq i_1<i_2<\ldots<i_j<i_{j+1}\leq m}\frac{(-1)^{j+1}}{(x-\alpha_{i_1})(x-\alpha_{i_2})\ldots(x-\alpha_{i_j})(x-\alpha_{i_{j+1}})}.\end{aligned}$$

■

Referências

[1] A.M.S. Doering - Y. Lequain - C.C. Ripoll, *Differential simplicity and cyclic maximal idelas of the Weyl algebra* $A_2(K)$, Glasgow Math. J. 48 (2006), 269-274.

[2] I. Kaplansky, *Commutative Rings*, TheUniversity of Chicago Press, 1974.

[3] Lequain, Y. *Simple Shamsuddin derivations of* $K[X_1, ..., X_n]$ *and cyclic maximal left ideals of the Weyl algebra* $\mathbb{A}_n[K]$, preprint.

[4] Y.Lequain, D.Levcovitz, J.C.Souza Jr., *$d-$simple rings and principal maximal ideals of the Weyl algebra,* Glasgow Math. J. 47 (2005), 269-285.

[5] A.Maciejewski, J.Moulin-Ollagnier, A.Nowicki, *Simple quadratic derivations in two variables,* Comm. Algebra 29 (2001), 5095-5113.

[6] A.Nowicki, *Polynomial derivations and their rings of constants*, Nicholas Copernicus University Press, Torun, 1994.

[7] Werle, E., *Derivações de Shamsuddin simples de* $K[X_1, ..., X_n]$ *e ideais maximais cíclicos à esquerda da Álgebra de Weyl* $\mathbb{A}_n(K)$. Dissertação de Mestrado - Universidade Federal do Rio Grande do Sul - Porto Alegre, 2005.