INSTITUTO DE MATEMÁTICA

Universidade Federal do Rio de Janeiro

UFRJ

Sobre isotropia de derivações simples

Gabriel Barruci da Silva

Rio de Janeiro, Brasil

10 de março de 2020

Sobre isotropia de derivações simples

Gabriel Barruci da Silva

Dissertação de mestrado apresentada ao Programa de Pós-graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática

Universidade Federal do Rio de Janeiro

Instituto de Matemática

Programa de Pós-Graduação em Matemática

Orientador: Severino Collier Coutinho

Rio de Janeiro, Brasil

10 de março de 2020

Gabriel Barruci da Silva

Sobre isotropia de derivações simples

Dissertação de mestrado apresentada ao Programa de Pós-graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática

Trabalho aprovado por

Severino Collier Coutinho
Orientador

Luciane Quoos Conte

Daniel Levcovitz

Rio de Janeiro, Brasil
10 de março de 2020

Agradecimentos

Agradeço imensamente meu orientador, Severino Collier Coutinho, por toda a sua gentileza, compreensão e paciência durante o desenvolvimento da dissertação. Poucos foram os professores em que vi presente essas características todas juntas.

Agradeço também ao professor Ivan Pan que, com sua cordialidade e dedicação, me ajudou quando houveram problemas no presente texto.

Agradeço cada um de meus amigos da salinha pelas várias risadas e histórias que surgiram nesses dois anos de mestrado.

Agradeço do fundo do coração a minha família pelo apoio e motivação. Nossa família é e sempre será nosso suporte em todos os momentos da vida.

De maneira geral, agradeço a cada um que passou pela minha vida e deixou sua marca nessa jornada até aqui.

Agradeço a Capes pelo apoio financeiro. Fundamental para o desenvolvimento do projeto.

Resumo

O principal objetivo dessa dissertação é apresentar um teorema que relaciona a simplicidade de derivações definidas no anel $\mathbb{K}[x, y]$ com seu grupo de isotropia. Para isso, começaremos apresentando alguns conceitos fundamentais da álgebra diferencial e automorfismos polinomiais. Resultados que serão necessários para o desenvolvimento posterior.

Em seguida, faremos uma exposição sobre soluções para derivações, provaremos o resultado principal e apresentaremos algumas aplicações deste importante resultado como uma caracterização da derivação de Shamsuddin através de seu grupo de isotropia.

No último capítulo, apresentaremos um exemplo que mostra que a recíproca do teorema principal não é valida.

Palavras-chave:Álgebra diferencial, Derivações simples, Automorfismos polinomiais.

Abstract

The main aim of this work is to present a theorem that combines the simplicity of derivations defined in the $\mathbb{K}$-algebra of polynomials in two variables $\mathbb{K}[x, y]$ with its isotropy group. For this purpose, we begin by showing some fundamental concepts of differential algebra and polynomial automorphisms.

Later we expose some results about solutions for derivations, we prove the main theorem of this dissertation and give some applications of this result like a characterization of Shamsuddin derivations by means of its isotropy group.

In the last chapter, we give an example that shows that the converse of main theorem does not hold.

Keywords: Differential algebra, Simple derivations, Polynomial automorphisms.

Sumário

1 Introdução

O estudo da simplicidade de derivações tem cada vez mais recebido atenção dos pesquisadores da área. Isso se deve muito ao fato de que derivações simples dão origem a anéis não comutativos cuja estrutura ainda é pouco conhecida como a extensão de Ore [GW04]. Derivações simples também estão ligadas com a geometria dos anéis em que estão definidas como mostra o fundamental resultado demonstrado por A. Seidenberg [Sei67] que diz que se um domínio finitamente gerado R admite uma derivação simples, então R é regular.

Mais recentemente, inúmeros resultados foram obtidos com respeito à simplicidade de derivações de carater geral e de de tipos específicos, como as chamadas derivações de Shamsuddin [Leq08]. Em especial, devemos citar o resultado provado por R. Baltazar [Bal16] que diz se uma derivação de Shamsuddin d definida em $\mathbb{K}[x, y]$ é simples, então a identidade é o único automorfismo que comuta com d. Essa dissertação se baseia principalmente no artigo [Men17] em que I. Pan e L. Mendes provam o fato mais geral que diz que se uma derivação d em duas variáveis é simples, então seu grupo de isotropia é trivial.

No capítulo 2, fazemos uma exposição sobre derivações e automorfismos. Conceitos básicos para o entendimento dos capítulos subsequentes. Abordaremos os teoremas de extensão de derivações em anéis polinomiais e faremos uma exposição dos principais subgrupos presentes no estudo de automorfismos polinomiais.

No capítulo 3, definiremos formalmente o conceito de simplicidade e trataremos de derivações simples dando primeiramente uma visão mais geral, em seguida, falando das derivações do tipo Shamsuddin e passando brevemente pelo caso de anéis locais.

O capítulo 4 é voltado para o estudo do grupo de isotropia e para o resultado principal da dissertação que diz que se uma derivação é simples, então possui grupo de isotropia trivial.

Por fim, no capítulo 5, apresentamos meios práticos de se determinar o grupo de isotropia de uma derivação de Shamsuddin e damos uma caracterização da simplicidade de derivações de Shamsuddin via esse grupo. Devido a um equívoco encontrado no artigo [Men17], alguns resultados desse capítulo possuem demonstrações ligeiramente diferentes daquelas presentes naquele texto. Além disso, através de um exemplo, conseguimos mostrar que a recíproca do resultado principal da dissertação não vale.

Ao longo de toda a dissertação, salvo menção contrária, todos os corpos serão admitidos de característica zero. Denotaremos por $\mathbb{K}$ um corpo de característica zero e por

R um anel comutativo com unidade. Denotaremos por $S^{[n]}$ a S-álgebra de polinômios em n variáveis $S[x_1, ..., x_n]$ e $S^{[[n]]}$ o anel de séries formais em n variáveis $S[[x_1, ..., x_n]]$ com S sendo, por vezes, R ou $\mathbb{K}$.

2 Preliminares

Para um melhor entendimento dos conceitos apresentados neste capítulo ver [Van12], [Abh06], [Now94], [Fre06], [BS13], [BFL14], [KS95] e [Wri13].

2.1 Derivações

Definição 2.1.1. *Seja R um anel. Uma derivação d é uma aplicação aditiva $d : R \to R$ que satisfaz*

$$d(ab) = d(a)b + ad(b),$$

para $a, b \in R$. No caso de R ser uma $\mathbb{K}$-álgebra, uma $\mathbb{K}$-derivação é uma derivação que também satisfaz $d(\alpha b) = \alpha d(b)$ para todo $b \in R$ e todo $\alpha \in \mathbb{K}$.

Chamaremos de $\mathrm{Der}(R)$ o conjunto das derivações de R e $\mathrm{Der}_{\mathbb{K}}(R)$ o conjunto das $\mathbb{K}$-derivações definidas no anel R. A primeira coisa a notar é que a soma de derivações é uma derivação e a multiplicação de uma derivação por uma constante ainda é uma derivação. Em verdade, se R é um anel, então $\mathrm{Der}(R)$ é um R-módulo. Em segundo lugar, note que

$$d(1) = d(1 \cdot 1) = d(1) \cdot 1 + 1 \cdot d(1) = 2d(1).$$

Logo, $d(1) = 0$, donde se segue que $d(\mathbb{K}) = 0$, para toda $d \in \mathrm{Der}_{\mathbb{K}}(R)$.

Além disso, observe que, num anel polinomial $R^{[n]}$, uma derivação fica unicamente determinada pela sua ação nas variáveis.

A derivada parcial $\partial_x : R[x] \to R[x]$ é um dos primeiros exemplos de derivação, pois satisfaz claramente a Definição 2.1.1.

Proposição 2.1.2 (Extensão na localização)**.** *Sejam R um anel, $S \subset R$ um conjunto multiplicativo e $d \in \mathrm{Der}(R)$. Então existe uma única derivação $d_S : S^{-1}R \to S^{-1}R$ com $d_S(a/1) = d(a)$.*

Demonstração. Com efeito, definamos d_S por

$$d_S\left(\frac{a}{b}\right) = \frac{d(a)b - ad(b)}{b^2},$$

para todo $a \in R$ e para todo $b \in S$. Note que, desde que d é uma derivação, segue-se que d_S também é uma derivação. Além disso,

$$d_S\left(\frac{a}{1}\right) = \frac{d(a)1 - ad(1)}{1^2} = d(a).$$

Por fim, suponhamos que d_S e $\tilde{d}_S$ sejam duas derivações satisfazendo as condições do enunciado e tomemos $b \in S$. Logo,

$$\tilde{d}_S(b^{-1}) = \tilde{d}_S\left(\frac{1}{b}\right) = \frac{\tilde{d}_S(1)b - 1\tilde{d}_S(b)}{b^2} = \frac{\tilde{d}_S(b)}{b^2} = \frac{d_S(b)}{b^2} = d_S(b^{-1}).$$

Portanto, para qualquer $a/b \in S^{-1}R$, temos

$$d_S\left(\frac{a}{b}\right) = d_S(a)b^{-1} + ad_S(b^{-1}) = \tilde{d}_S(a)b^{-1} + a\tilde{d}_S(b^{-1}) = \tilde{d}_S\left(\frac{a}{b}\right).$$

Donde segue que $d_S = \tilde{d}_S$. □

Dado um polinômio $g \in R[x]$ com $g(x) = a_0 + a_1x + \cdots + a_nx^n$ e uma derivação $d \in \mathrm{Der}(R[x])$, podemos definir um novo polinômio da seguinte forma $g^d(x) = d(a_0) + d(a_1)x + \cdots + d(a_n)x^n$.

Proposição 2.1.3 (Extensão no anel de polinômios)**.** *Seja d uma derivação definida no anel R e $p(x) \in R[x]$. Então existe uma única derivação $\overline{d}$ definida no anel $R[x]$ tal que $\overline{d}|_R = d$ e $\overline{d}(x) = p(x)$.*

Demonstração. Definamos $\overline{d}$ da seguinte forma

$$\overline{d}(f) = f^d + \partial_x(f)p(x),$$

para todo $f \in R[x]$. Observe que

$$\overline{d}(x) = d(1) + \partial_x(x)p(x) = p(x),$$

e que $\overline{d}(c) = d(c)$ para todo $c \in R$. Sejam $f, g \in R[x]$ tais que $f = \sum_{i=0}^{n} a_ix^i$ e $g = \sum_{j=0}^{m} b_jx^j$ e notemos que

$$fg = \left(\sum_{i+j=k} a_ib_j\right)x^k.$$

Portanto,

$$\begin{aligned}
(fg)^d &= \left(\sum_{i+j=k} d(a_ib_j)\right)x^k \\
&= \left(\sum_{i+j=k} d(a_i)b_j + a_id(b_j)\right)x^k \\
&= \left(\sum_{i+j=k} d(a_i)b_j\right)x^k + \left(\sum_{i+j=k} a_id(b_j)\right)x^k \\
&= f^dg + fg^d.
\end{aligned}$$

Assim,

$$\begin{aligned}\overline{d}(fg) &= (fg)^d + \partial_x(fg)p(x)\\ &= f^d g + fg^d + \partial_x(f)gp(x) + f\partial_x(g)p(x)\\ &= \overline{d}(f)g + f\overline{d}(g).\end{aligned}$$

Como d é linear, temos que $\overline{d}$ é linear. Isso mostra que, de fato, $\overline{d}$ é derivação de $R[x]$. Por fim, desde que $\overline{d}$ está definida na variável x, a unicidade fica estabelecida. □

Com base na demonstração acima e no fato que $R^{[n]} = R^{[n-1]}[x_n]$, o resultado acima pode ser estendido para o anel $R^{[n]}$.

Corolário 2.1.4. *Sejam d uma derivação definida no anel R e $f_1, \ldots, f_n \in R^{[n]}$. Então existe uma única derivação $\overline{d}$ definida no anel $R^{[n]}$ tal que $\overline{d}|_R = d$ e $\overline{d}(x_i) = f_i$ para cada $i = 1, \ldots, n$.*

Exemplo 2.1.5. Dadas duas derivações $d_1, d_2 \in \mathrm{Der}(R)$ podemos definir uma nova derivação através do *Colchete de Lie* dado por $[d_1, d_2] = d_1d_2 - d_2d_1$. Com efeito, se $a, b \in R$, então

$$\begin{aligned}[d_1, d_2](a+b) &= d_1d_2(a+b) - d_2d_1(a+b)\\ &= d_1(d_2(a) + d_2(b)) - d_2(d_1(a) + d_1(b))\\ &= d_1d_2(a) + d_1d_2(b) - d_2d_1(a) - d_2d_1(b)\\ &= [d_1, d_2](a) + [d_1, d_2](b)\end{aligned}$$

e

$$\begin{aligned}[d_1, d_2](ab) &= d_1d_2(ab) - d_2d_1(ab)\\ &= d_1(d_2(a)b + ad_2(b)) - d_2(d_1(a)b + ad_1(b))\\ &= [d_1d_2(a)b + d_2(a)d_1(b)] + [d_1(a)d_2(b) + ad_1d_2(b)]\\ &\quad - [d_2d_1(a)b + d_1(a)d_2(b)] - [d_2(a)d_1(b) + ad_2d_1(b)]\\ &= [d_1, d_2](a)b - a[d_1, d_2](b).\end{aligned}$$

Esse exemplo elucida o método trabalhoso de se verificar se uma aplicação é uma derivação. Porém, em anéis polinomiais, temos resultados que facilitam esse processo.

Teorema 2.1.6. *Sempre vale:*

i) Dados $f_1, \ldots, f_n \in \mathbb{K}^{[n]}$, existe única $\mathbb{K}$-derivação $d : \mathbb{K}^{[n]} \to \mathbb{K}^{[n]}$ com $d(x_i) = f_i$. Essa derivação se escreve $d = f_1\partial_{x_1} + ... + f_n\partial_{x_n}$.

ii) $\mathrm{Der}_{\mathbb{K}}(\mathbb{K}^{[n]})$ é um $\mathbb{K}^{[n]}$-módulo livre de base $\{\partial_{x_1}, ..., \partial_{x_n}\}$.

iii) Para quaisquer $i, j = 1, ..., n$ vale $\partial_{x_i}\partial_{x_j} = \partial_{x_j}\partial_{x_i}$.

iv) Para quaisquer $d \in \mathrm{Der}_{\mathbb{K}}(\mathbb{K}^{[n]})$ e $f \in \mathbb{K}^{[n]}$ vale $d(f) = \sum_{k=1}^{n} \frac{\partial f}{\partial x_k} d(x_k)$.

Demonstração. *i*) Segue da Proposição 2.1.3.

ii) Sejam $f_1, \ldots, f_n \in \mathbb{K}^{[n]}$ e suponhamos que $\sum_{i=1}^{n} f_i \partial_{x_i} = 0$. Pelo item *i*) seguficomie-se que existe única derivação d tal que $d = \sum_{i=1}^{n} f_i \partial_{x_i}$ com $d(x_i) = f_i$ e $i = 1, \ldots, n$. Disso, temos que $f_i = 0$, para $i = 1, \ldots, n$.

iii) Como cada ∂_{x_i} é uma $\mathbb{K}$-derivação do anel $\mathbb{K}^{[n]}$, temos que $[\partial_{x_i}, \partial_{x_j}] \in \mathrm{Der}_{\mathbb{K}}(\mathbb{K}^{[n]})$ para $i, j = 1, \ldots, n$. Desde que $[\partial_{x_i}, \partial_{x_j}](x_k) = 0$, para $k = 1, \ldots, n$ e uma derivação em $\mathbb{K}^{[n]}$ é unicamente determinada pelos valores em x_i, segue-se que $[\partial_{x_i}, \partial_{x_j}] = 0$ para $i, j = 1, \ldots, n$. Portanto, $\partial_{x_i} \partial_{x_j} = \partial_{x_j} \partial_{x_i}$.

iv) Imediato de *i*). □

Exemplo 2.1.7. O Teorema 2.1.6 nos permite criar uma série de exemplos de derivações em $\mathbb{K}^{[n]}$. Em duas variáveis, por exemplo, tomando a, b polinômios em $\mathbb{K}[x]$, formamos a classe de derivações de *Shamsuddin* definidas como $d = \partial_x + (ay + b)\partial_y$. Se considerarmos os polinômios $\{1, y^2 + ay + b\}$ tais que $a, b \in \mathbb{K}[x]$, podemos construir a derivação $d = \partial_x + (y^2 + ay + b)\partial_y$ que faz parte da classe das chamadas *derivações quadráticas*. Mais ainda, $f_1, \ldots, f_n \in \mathbb{K}^{[n]}$ são polinômios homogêneos, então $d = f_1 \partial_{x_1} + \cdots + f_n \partial_{x_n}$ é uma derivação que pertence à classe das derivações *homogêneas*.

Da mesma forma como apresentado na Proposição 2.1.3, se $d \in \mathrm{Der}_{\mathbb{K}}(R)$, podemos definir uma derivação no anel de séries formais $R^{[[n]]}$ da seguinte forma $\widehat{d} = \sum_{n=0}^{\infty} d(a_i) t^i$. Segue-se de d ser derivação que $\widehat{d}$ satisfaz a definição 2.1.1.

Proposição 2.1.8 (Extensão em séries formais)**.** *Sejam R um anel e $d : R \to R$ uma derivação. Se $f_1, \ldots, f_n \in R^{[[n]]}$, então existe uma única derivação $\widehat{d} : R^{[[n]]} \to R^{[[n]]}$ tal que $\widehat{d}(x_i) = f_i$, para $i = 1, \ldots, n$.*

Demonstração. Veja [Bou59, p. A.V -130]. □

Proposição 2.1.9. *i) Se $f_1, \ldots, f_n \in \mathbb{K}^{[[n]]}$, então existe única $\mathbb{K}$-derivação d de $\mathbb{K}^{[[n]]}$ tal que $d(x_1) = f_1, \ldots, d(x_n) = f_n$.*

ii) $\mathrm{Der}(\mathbb{K}^{[[n]]})$ é um $\mathbb{K}^{[[n]]}$-módulo livre de base $\{\partial_{x_1}, \ldots, \partial_{x_n}\}$.

iii) Para quaisquer $i, j \in 1, \ldots, n$ vale $\partial_{x_i} \partial_{x_j} = \partial_{x_j} \partial_{x_i}$.

iv) Para quaisquer $d \in \mathrm{Der}_{\mathbb{K}}(\mathbb{K}^{[[n]]})$ e $f \in \mathbb{K}^{[[n]]}$ vale $d(f) = \sum_{k=1}^{n} \frac{\partial f}{\partial x_k} d(x_k)$.

Os próximos dois resultados dizem respeito ao comportamento de derivações com relação a ideais.

Proposição 2.1.10. *Sejam R um anel, $d \in \mathrm{Der}(R)$ e $\mathfrak{a} \subset R$ um ideal. Então $d(\mathfrak{a}^n) \subset \mathfrak{a}^{n-1}$ para todo natural n.*

Demonstração. Se $b \in \mathfrak{a}^n$, então $b = \sum_{i=1}^{k} b_{i_1} \cdots b_{i_n}$ em que $b_{i_j} \in \mathfrak{a}$ para cada $j = 1, \ldots, n$ e $k \in \mathbb{N}$. Mas,

$$d(b_{i_1} \cdots b_{i_n}) = \sum_{i=1}^{n} b_{i_1} \cdots d(b_{i_j}) \cdots b_{i_n} \in \mathfrak{a}^{n-1}.$$

□

Proposição 2.1.11. *Seja $d \in \mathrm{Der}(R)$, $\mathfrak{a} \subset R$ um ideal com $d(\mathfrak{a}) \subset \mathfrak{a}$ e considere a projeção $\pi : R \to R/\mathfrak{a}$. Então d induz uma derivação d^* definida em $R/\mathfrak{a}$ tal que $d^* \circ \pi = \pi \circ d$.*

Demonstração. Sejam $x \in R/\mathfrak{a}$, $r \in R$ tais que $\pi(r) = x$ e definamos então $d^*(x) = \pi(d(r))$. Se $r, s \in R$ são tais que $x = \pi(s) = \pi(r)$, então $r - s \in \mathfrak{a}$. Como $d(\mathfrak{a}) \subset \mathfrak{a}$, temos que $d(r - s) \in \mathfrak{a}$, donde se segue que $\pi(d(r)) = \pi(d(s))$. Isso mostra que d^* está bem definida e, da própria definição de d^*, temos $d^* \circ \pi = \pi \circ d$. Por fim, vamos mostrar que d^* é derivação. De fato, se $x, y \in R/\mathfrak{a}$, então

$$d^*(x + y) = \pi(d(r + s)) = \pi(d(r)) + \pi(d(s)) = d^*(x) + d^*(y)$$

e

$$d^*(xy) = \pi(d(rs)) = \pi(d(r)s + rd(s)) = \pi(d(r))\pi(s) + \pi(r)\pi(d(s)) = d^*(x)y + xd^*(y).$$

□

2.2 Automorfismos

Definição 2.2.1. *Definimos um $\mathbb{K}$-endomorfismo de $\mathbb{K}^{[n]}$ como sendo uma aplicação $\rho : \mathbb{K}^{[n]} \to \mathbb{K}^{[n]}$ que satisfaz*

i) $\rho(af) = a\rho(f),\ a \in \mathbb{K},\ f \in \mathbb{K}^{[n]}$.

ii) $\rho(f + g) = \rho(f) + \rho(g),\ f, g \in \mathbb{K}^{[n]}$.

iii) $\rho(fg) = \rho(f)\rho(g),\ f, g \in \mathbb{K}^{[n]}$.

Caso ρ seja bijetivo, dizemos que ρ é um automorfismo.

Denotaremos o conjunto de automorfismos de $\mathbb{K}^{[n]}$ por $\mathrm{Aut}(\mathbb{K}^{[n]})$ e, da mesma como para derivações, $\mathrm{Aut}_{\mathbb{K}}(\mathbb{K}^{[n]})$ o conjunto dos $\mathbb{K}$-automorfismos de $\mathbb{K}^{[n]}$, isto é, que satisfazem $\rho(\alpha f) = \alpha\rho(f)$, para $\alpha \in \mathbb{K}$ e $f \in \mathbb{K}^{[n]}$.

Decorre da definição 2.2.1, que endomorfismos são unicamente determinados pelos seus valores nas variáveis, isto é, se $f \in \mathbb{K}^{[n]}$, então

$$\rho(f) = f(\rho(x_1), \ldots, \rho(x_n)).$$

Nesse sentido, para cada endomorfismo ρ, existem polinômios $\rho(x_1), \ldots, \rho(x_n)$ a ele associados.

Definição 2.2.2. *Sejam $f_1, \ldots, f_n$ polinômios em $\mathbb{K}^{[n]}$. Chamaremos de função polinomial a aplicação $\varphi : \mathbb{K}^n \to \mathbb{K}^n$ definida por*

$$\varphi(a_1, \ldots, a_n) = (f_1(a_1, \ldots, a_n), \ldots, f_n(a_1, \ldots, a_n)).$$

Dado um conjunto de polinômios $\{f_1, \ldots, f_n\} \subset \mathbb{K}^{[n]}$, representaremos uma função polinomial φ como $\varphi = (f_1, \ldots, f_n)$. Dizemos que uma função polinomial é inversível se existe uma função polinomial $\psi : \mathbb{K}^n \to \mathbb{K}^n$ tal que $\varphi(\psi(x)) = x$ para $x = (x_1, \ldots, x_n) \in \mathbb{K}^n$.

Proposição 2.2.3. *Seja $\varphi : \mathbb{K}^n \to \mathbb{K}^n$ uma função polinomial injetiva. Então φ é bijetiva e sua inversa é uma função polinomial.*

Demonstração. Ver [Bia62, p. 203]. □

Proposição 2.2.4. *Seja $\varphi : \mathbb{K}^n \to \mathbb{K}^n$ função polinomial inversível. Então* $\det J(\varphi) \in \mathbb{K}^*$.

Demonstração. Como φ é inversível, existe uma função polinomial ψ tal que $(\psi \circ \varphi)(x) = x$ para todo $x = (x_1, \ldots, x_n)$. Tomando o operador Jacobiano de ambos os lados da última igualdade, temos $J(\varphi(\psi(x))J(\psi(x)) = I$, em que I é a matriz identidade $n \times n$ com entradas em $\mathbb{K}$. Aplicando o determinante, obtemos

$$\det J(\psi(\varphi(x)) \det J(\varphi(x)) = 1,$$

para todo $x \in \mathbb{K}^n$. Como os únicos polinômios inversíveis são as constantes, segue-se que $\det J(\varphi(x)) \in \mathbb{K}^*$, para todo $x \in \mathbb{K}^n$. □

Com base nas definições 2.2.1 e 2.2.2, a próxima proposição mostra que estudar automorfismos é equivalente a estudar funções polinomiais.

Proposição 2.2.5. *Seja $\varphi = (f_1, \ldots, f_n) : \mathbb{K}^n \to \mathbb{K}^n$ uma função polinomial. São equivalentes:*

i) $f_1, \ldots, f_n$ geram $\mathbb{K}^{[n]}$.

ii) φ é inversível.

iii) O endomorfismo ρ determinado por $f_1, \ldots, f_n$ é um automorfismo.

Demonstração. Ver [FM09, p. 61]. □

Sabemos, desde os cursos de álgebra para a graduação, que a composição de dois automorfismos é ainda um automorfismo; isto é, o conjunto $\mathrm{Aut}(\mathbb{K}^{[n]})$ forma um grupo com respeito à composição.

Nesse sentido, faremos, então, uma pequena exposição de alguns subconjuntos de $\mathrm{Aut}(\mathbb{K}^{[n]})$ que frequentemente aparecem no decorrer do estudo de automorfismos polinomiais. Dentre estes, começamos com os mais básicos em estrutura e, por esse motivo, chamados de automorfismos elementares. Um automorfismo $\rho \in \mathrm{Aut}(\mathbb{K}^{[n]})$ é dito *elementar* se é da forma

$$\rho : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{i-1}, ax_i + f, x_{i+1}, \ldots, x_n),$$

em que $f \in \mathbb{K}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ e $a \in \mathbb{K}^*$. Denotaremos o conjunto de automorfismos elementares por $E_n(\mathbb{K})$. Em $\mathbb{K}[x]$, todo automorfismo é da forma $\rho(x) = ax + b$ com $a \in \mathbb{K}^*$, $b \in \mathbb{K}$ e, portanto, em uma variável, todo automorfismo é elementar.

Decorre da Proposição 2.2.5, que as operações naturais de matrizes podem ser vistas como composições finitas de automorfismos elementares como, por exemplo, a multiplicação de uma linha por uma constante não nula e a soma de um múltiplo de uma linha por outra. Como exemplo, a sequência de automorfismos elementares abaixo explicita a troca de linhas em $\mathbb{K}^2$.

$$(x, y) \overset{\rho_1}{\mapsto} (-x + y, y) \overset{\rho_2}{\mapsto} (-x + y, x) \overset{\rho_3}{\mapsto} (y, x)$$

em que $\rho_1 : (x, y) \mapsto (-x + y, y)$, $\rho_2 : (x, y) \mapsto (x, y - x)$ e $\rho_3 : (x, y) \mapsto (x + y, y)$.

Se M é uma matriz inversível $n \times n$ e $x = (x_1, \ldots, x_n)$, a aplicação $\rho(x) = Mx$ define um automorfismo chamado de automorfismo *linear*. Estes automorfismos formam um subgrupo de $\mathrm{Aut}(\mathbb{K}^{[n]})$, o bem conhecido grupo *linear geral* $\mathrm{GL}_n(\mathbb{K})$. Se além disso, $c \in \mathbb{K}^n$, a aplicação afim $\rho(x) = Mx + c$ define um automorfismo cujo inverso, dado por $\rho^{-1}(x) = M^{-1}x - M^{-1}c$, também é afim. O grupo formado por esses automorfismos é chamado do subgrupo *afim* e denotado por

$$\mathrm{Aff}_n(\mathbb{K}) = \{\rho = (\rho_1, \ldots, \rho_n) \in \mathrm{Aut}(\mathbb{K}^{[n]});\ \mathrm{gr}(\rho_i) = 1,\ i = 1, ..., n\}.$$

Observe que se $\sigma, \rho \in \mathrm{Aff}_n(\mathbb{K})$ com $\rho(x) = M_1x + c_1$ e $\sigma = M_2x + c_2$, então

$$\rho\sigma(x) = M_2M_1x + M_2c_1 + c_2.$$

Portanto, $\mathrm{Aff}_n(\mathbb{K}^{[n]}) = \mathrm{GL}_n(\mathbb{K}) \ltimes \mathrm{T}_n$, em que T_n são as translações em $\mathbb{K}^n$, isto é, todo automorfismo afim é obtido por uma transformação linear inversível e uma translação.

Toda composição finita de automorfismos elementares com um automorfismos afim gera um novo automorfismo chamado de automorfismo *triangular*. Esses formam o

chamado grupo de *de Jonquière* ou *Triangular*.

$$J_n(\mathbb{K}) = \{\rho \in \mathrm{Aut}(\mathbb{K}^{[n]});\ \rho_i = a_i x_i + f_i,\ f_i \in \mathbb{K}[x_{i+1}, \ldots, x_n] \text{ e } f_n \in \mathbb{K}\}. \tag{2.1}$$

Se definirmos $a_i = 1$ em (2.1) para todo $i = 1, \ldots, n$, então temos o subgrupo *unitriangular* que denotamos por $U_n(\mathbb{K})$. Pode-se mostrar [BNS12, p. 3] que $J_n(\mathbb{K}) = D_n(\mathbb{K}) \ltimes U_n(\mathbb{K})$ em que $D_n(\mathbb{K})$ é o chamado grupo *diagonal*, que é composto por automorfimos da forma $\rho : x_i \to \alpha_i x_i$ com $\alpha_i \in \mathbb{K}^*$. Observe que $D_n(\mathbb{K}) \subset \mathrm{GL}_n(\mathbb{K})$.

Usando composições finitas de automorfismos afins e triangulares podemos gerar um novo subgrupo de $\mathrm{Aut}(\mathbb{K}^{[n]})$ chamado de grupo dos automorfismos *mansos*,

$$T_n(\mathbb{K}) = \langle \mathrm{Aff}_n(\mathbb{K}), J_n(\mathbb{K}) \rangle.$$

Nesse sentido, os autormorfismos que não mansos, são chamados de *selvagens*. A interseção $\mathrm{Aff}_n(\mathbb{K}) \cap J_n(\mathbb{K})$ forma um subgrupo chamado grupo de *Borel* e que denotamos por $B_n(\mathbb{K})$.

Antes de enunciar um dos teoremas mais importantes dessa seção, devemos fazer algumas considerações sobre o processo de construir o produto amalgamado de grupos. Sejam G um grupo e A, B dois subgrupos com $G = \langle A, B \rangle$. Consideremos primeiramente o grupo livre $A * B$; isto é, para cada $g \in A * B$, temos que

$$g = a_1 b_1 \cdots a_n b_n \tag{2.2}$$

com $a_i \in A \setminus B$, $b_i \in B \setminus A$, $a_i, b_i \notin A \cap B$ para $i = 1, \ldots, n$ e em que (2.2) nunca é a identidade. Tomemos os morfismos de inclusão $i_A : A \cap B \to A * B$ e $i_B : A \cap B \to A * B$ e consideremos o homomorfismo sobrejetor $\varphi : A \cap B \to G$ dado por $\varphi(h) = i_A(h) i_B^{-1}(h)$. Definimos, então, o produto amalgamado de A e B sobre $A \cap B$ como $A *_{A \cap B} B \cong (A * B)/\ker \varphi$.

O grupo $\mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x, y])$ é um exemplo de produto amalgamado e, em particular, o que nos interessa aqui.

Teorema 2.2.6 (Jung, Van Der Kulk)**.** $\mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x, y]) = \mathrm{Aff}_2(\mathbb{K}) *_{B_2(\mathbb{K})} J_2(\mathbb{K})$.

Demonstração. Uma demonstração pode ser encontrada em [Van12, p. 89]. □

Um pergunta que é de bastante interesse no estudo de automorfismos polinomiais, é saber o tamanho do conjunto de automorfismos selvagens presentes em $\mathrm{Aut}(\mathbb{K}^{[n]})$. Nesse sentido, o resultado acima nos diz que não há automorfismos selvagens em duas variáveis. Em três variáveis, o caso já é diferente. Sheskatov e Umirbaev [SU04] mostraram que o chamado automorfismo de Nagata [Nag72],

$$\begin{aligned} \rho(x) &= x - 2y(xz + y^2) - z(xz + y^2) \\ \rho(y) &= y + z(xz + y^2) \\ \rho(z) &= z, \end{aligned}$$

é um automorfismo selvagem de $\mathbb{K}[x, y, z]$.

O teorema de Van der Kulk é um resultado estrutural, isto é, qualquer elemento $\rho \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x, y])$ é escrito da forma

$$\rho = \alpha_1 \circ \gamma_1 \circ \cdots \circ \alpha_n \circ \gamma_n, \tag{2.3}$$

em que $\alpha_i \in \mathrm{Aff}_2(\mathbb{K}) \setminus J_2(\mathbb{K})$, $\gamma_i \in J_2(\mathbb{K}) \setminus \mathrm{Aff}_2(\mathbb{K})$, $\alpha_i, \gamma_i \notin \mathrm{Aff}_2(\mathbb{K}) \cap_2 (\mathbb{K})$ para $i = 1, ..., n$ e (2.3) nunca é a identidade. Mais ainda, essa representação é única módulo composições de elementos de $B_2(\mathbb{K})$. O número natural n em (2.3) é chamado de *comprimento* de ρ, que representamos aqui por $\ell(\rho)$.

Lema 2.2.7. *Seja $G \subset \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}^{[n]})$ um subgrupo tal que $G = L \ltimes M$ em que $L \subset \mathrm{GL}_n(\mathbb{K})$ e M subgrupo tal que $\frac{1}{r}\sum_{i=1}^{r} m_i \in M$ para qualquer sequência $m_1, \ldots, m_r \in M$. Então, todo $g \in G$ é conjugado ao subgrupo L por um elemento de M.*

Demonstração. [BFL14, p. 200 - Lema 5.1] □

Corolário 2.2.8. *Todo automorfismo de $\mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x, y])$ de ordem finita é conjugado a um automorfismo linear.*

Demonstração. Seja $\rho \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x, y])$. A demonstração é feita por indução no comprimento de ρ. Por 2.2.6 podemos escrever

$$\rho = \alpha_1 \circ \gamma_1 \circ \cdots \circ \alpha_k \circ \gamma_k, \tag{2.4}$$

em que $\alpha_i \in \mathrm{Aff}_2(\mathbb{K}) \setminus J_2(\mathbb{K})$ e $\gamma_i \in J_2(\mathbb{K}) \setminus \mathrm{Aff}_2(\mathbb{K})$ para $i = 1, ..., k$ e (2.4) nunca é a identidade. Como ρ tem ordem finita, deve haver algum cancelamento no produto

$$\rho^2 = \alpha_1 \circ \gamma_1 \circ \cdots \circ \alpha_k \circ \gamma_k \circ \alpha_1 \circ \gamma_1 \circ \cdots \circ \alpha_k \circ \gamma_k.$$

Então, note que, ou $\alpha_k \circ \gamma_k \circ \alpha_1 \in B_2(\mathbb{K})$ ou $\gamma_k \circ \alpha_1 \circ \gamma_1 \in B_2(\mathbb{K})$. Suponha que estejamos no primeiro caso e observe que

$$\begin{aligned} \alpha_1^{-1} \circ \rho \circ \alpha_1 &= \alpha_1^{-1} \circ \alpha_1 \circ \gamma_1 \circ \cdots \circ \gamma_{k-1}\alpha_k \circ \gamma_k \circ \alpha_1 \\ &= \gamma_1 \circ \alpha_2 \circ \cdots \circ \alpha_{k-1} \circ \gamma_{k-1}. \end{aligned}$$

Segue-se que $\ell(\alpha_1^{-1} \circ \rho \circ \alpha_1) = k-1$. Assim, por indução, temos que existe um automorfismo $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x, y])$ tal que $\sigma^{-1} \circ \rho \circ \sigma = \beta$ em que β é elemento de $\mathrm{Aff}_2(\mathbb{K}) \setminus J_2(\mathbb{K})$ ou $J_2(\mathbb{K}) \setminus \mathrm{Aff}_2(\mathbb{K})$. Como $\mathrm{Aff}_2(\mathbb{K}) = \mathrm{GL}_2(\mathbb{K}) \ltimes \mathrm{T}_2$ e $J_2(\mathbb{K}) = D_2(\mathbb{K}) \ltimes U_2(\mathbb{K})$, o resultado segue de 2.2.7. □

O estudo dos automorfismos passa pelo conhecimento de suas propriedades invariantes. O próximo resultado, devido a D. R. Lane [Lan75, p. 728], mostra que, em duas variáveis, todo automorfismo preserva, pelo menos, um ideal não trivial.

Teorema 2.2.9. *Seja $\rho \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x,y])$, então existe pelo menos um ideal não trivial $\mathfrak{a} \subset \mathbb{K}[x,y]$ tal que $\rho(\mathfrak{a}) \subset \mathfrak{a}$.*

Em vista do último resultado, temos ainda que $\rho(\mathfrak{a}) \subset \mathfrak{a}$ se, e somente se, $\rho(\mathfrak{a}) = \mathfrak{a}$. Com efeito, desde que $\mathbb{K}[x,y]$ é anel Noetheriano deve existir algum $n \in \mathbb{N}$ tal que a sequência

$$\mathfrak{a} \subset \rho^{-1}(\mathfrak{a}) \subset \cdots \subset \rho^{-k}(\mathfrak{a}) \subset \cdots$$

para de modo que $\rho^{-n}(\mathfrak{a}) = \rho^{-n-1}(\mathfrak{a})$. Dessa forma, segue-se que $\rho(\mathfrak{a}) = \mathfrak{a}$.

Proposição 2.2.10. *Seja $\mathfrak{a} \subset \mathbb{K}^{[n]}$ um ideal. Se $\rho(\mathfrak{a}) \subset \mathfrak{a}$,então $\rho(\sqrt{\mathfrak{a}}) \subset \sqrt{\mathfrak{a}}$.*

Demonstração. Suponhamos, por absurdo, que $\rho(\sqrt{\mathfrak{a}}) \not\subset \sqrt{\mathfrak{a}}$. Isto é, existe $y \in \rho(\sqrt{\mathfrak{a}})$, de modo que $y \notin \sqrt{\mathfrak{a}}$. Dessa forma, existe $x \in \sqrt{\mathfrak{a}}$ tal que $\rho(x) = y$. Por definição, existe $m \in \mathbb{N}$ tal que $x^m \in \mathfrak{a}$. Agora,

$$y^m = (\rho(x))^m = \rho(x^m) \in \rho(\mathfrak{a}) \subset \mathfrak{a}.$$

Da definição de radical de um ideal, $y \in \sqrt{\mathfrak{a}}$, o que é um absurdo. □

Consideremos um ideal $\mathfrak{a} \subset \mathbb{K}^{[n]}$ e suponha que $\rho(\mathfrak{a}) \subset \mathfrak{a}$ para algum automorfismo $\rho \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}^{[n]})$. Como $\mathbb{K}^{[n]}$ é Noetheriano, o conjunto dos primos minimais do ideal $\mathfrak{a}$ é finito. Denotemos por $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ tais primos minimais. Da proposição 2.2.10 e do fato de que $\sqrt{\mathfrak{a}} = \cap_{i=1}^{k} \mathfrak{p}_i$, segue-se que

$$\bigcap_{i=1}^{k} \rho(\mathfrak{p}_i) \subset \sqrt{\mathfrak{a}}.$$

Logo, para cada primo minimal $\mathfrak{p}_j$, existe $l \in \{1, \ldots, k\}$ tal que $\rho(\mathfrak{p}_l) = \mathfrak{p}_j$, ou seja, os primos minimais são permutados pela ação do automorfismo ρ. Como o conjunto dos primos minimais é finito, cada orbita referente a um primo minimal é finita. Portanto, decorre da proposição anterior, que uma potência de ρ fixa os primos minimais de $\mathfrak{a}$.

Terminamos essa seção comentando sobre o comportamento de automorfismos polinomiais com respeito a curvas.

Definição 2.2.11. *Seja γ a curva definida pela equação $F(x,y) = 0$ em que $F(x,y) \in \mathbb{K}[x,y]$. Dizemos que γ é geometricamente irredutível se $F(x,y)$ é irredutível em $\overline{\mathbb{K}}[x,y]$.*

Teorema 2.2.12. *Seja γ uma curva geometricamente irredutível em $\mathbb{K}[x,y]$. Então, existe $\rho \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x,y])$ tal que $\rho(\gamma)$ tem como equação:*

i) $x = 0$ ou

ii) $x^b = \lambda y^a$ com $a, b > 1$ inteiros coprimos e $\lambda \in \mathbb{K}^*$ ou

iii) $x^b y^a = \lambda$ com $a, b \geq 1$ inteiros coprimos e $\lambda \in \mathbb{K}^*$.

Demonstração. Ver [BS13, p.194].

□

3 Derivações Simples

Derivações simples aparecem frequentemente na álgebra não comutativa como na criação de exemplos da chamada Extensões de Ore. Como referências para esse capítulo, sugerimos [Now94] e [BP15].

3.1 Caso geral

Definição 3.1.1. *Sejam R um anel e $d \in \mathrm{Der}(R)$, diremos que um ideal $I \subset R$ é d-estável (ou um d-ideal) se $d(I) \subset I$. Dizemos que d é simples se somente 0 e R são d-estáveis. Diremos também que R é d-simples se existe derivação simples $d \in \mathrm{Der}(R)$.*

Observe que se $d \in \mathrm{Der}_{\mathbb{K}}(R)$, então a simplicidade é preservada pela multiplicação por uma constante não-nula. De fato, seja d simples, $\alpha \in \mathbb{K}^*$ e suponha, por absurdo, que αd não seja simples. Então existe $\mathfrak{a} \subset R$ ideal não trivial tal que $\alpha d(\mathfrak{a}) \subset \mathfrak{a}$. Porém,

$$d(\mathfrak{a}) = \alpha^{-1}\mathfrak{a} \subset \mathfrak{a}.$$

Exemplo 3.1.2. Um exemplo de derivação que não é simples é a derivação homogênea em $\mathbb{K}[x, y]$ definida por $d = x\partial_x + y\partial_y$. De fato, observe que (x) e (y) são ideais d-estáveis.

Lema 3.1.3. *Sejam $\mathbb{K} \subset M \subset F \subset L$ corpos e considere a $\mathbb{K}$-derivação $d : M \to L$. Então d pode ser extendida a uma $\mathbb{K}$-derivação $\tilde{d} : F \to L$. Além disso se F/M é algébrica, então a extensão d é unica e se $\alpha \in F$ é tal que $\min(\alpha) = p(x) \in M[x]$, então $\tilde{d}(\alpha) \in L$ é o único elemento satisfazendo $p^d(\alpha) + \tilde{d}(\alpha)p'(\alpha) = 0$.*

Demonstração. Ver [ZS75, p. 122]. □

O próximo teorema nos dá uma primeira caracterização de derivações simples

Teorema 3.1.4. *Seja $\mathbb{K}$ um corpo com $\mathrm{char}(\mathbb{K}) = 0$ e $\overline{\mathbb{K}}$ seu fecho algébrico. Seja $d \in \mathrm{Der}(\mathbb{K}[x])$ com $d(\mathbb{K}) \subset \mathbb{K}$ e suponha que $d(x) = f(x)$ para algum $f \in \mathbb{K}[x]$. Então $\mathbb{K}[x]$ não é d-simples se, e somente se, $d(\alpha) = f(\alpha)$ para algum $\alpha \in \overline{\mathbb{K}}$.*

Demonstração. Sejam $d \in \mathrm{Der}(\mathbb{K}[x])$, $\alpha \in \overline{\mathbb{K}}$ e consideremos seu polinômio minimal $\min(\alpha) = q(x)$. Pelo que foi visto em 2.1.6 existe uma única derivação – que também chamaremos de d – tal que

$$d(g) = g^d + fg',$$

para todo $g(x) \in \mathbb{K}[x]$. Como $\mathbb{K}[x]$ é domínio de ideais principais, $q(x)$ gera um d-ideal de $\mathbb{K}[x]$ se, e somente se,

$$d(q(x)) = q(x)^d + f(x)g'(x) = p(x)q(x),$$

para algum $p(x) \in \mathbb{K}[x]$. Em particular

$$q(\alpha)^d + f(\alpha)g'(\alpha) = 0.$$

Segue-se do Lema 3.1.3, que isso acontece se, e somente se, $d(\alpha) = f(\alpha)$. □

O resultado acima nos mostra que toda derivação simples de $\mathbb{K}[x]$ é da forma $d = c\partial_x$ para $c \in \mathbb{K}^*$. De fato, pelo Teorema 2.1.6, $d = f\partial_x$ para algum $f \in \mathbb{K}[x]$. Logo, se $\mathbb{K}[x]$ é d-simples, devemos ter

$$0 = f(\alpha)\partial_x(\alpha) \neq f(\alpha),$$

para todo $\alpha \in \overline{\mathbb{K}}$. Isso acontece se, e somente se, $f \in \mathbb{K}^*$.

Seja R um domínio de integridade contendo $\mathbb{Q}$ e denote por $k = S^{-1}R$ o corpo total de frações de R, isto é, $S = R \setminus \{0\}$. Pela Proposição 2.1.2, uma derivação $d \in \mathrm{Der}(R[x])$ pode ser estendida a uma única derivação em $\mathrm{Der}(k[x])$.

Lema 3.1.5. *Sejam R um anel, $d \in \mathrm{Der}(R)$ uma derivação simples e k o corpo total de frações de R. Então os d-ideais primos de $R[x]$ correspondem, biunivocamente, aos d-ideais primos de $k[x]$.*

Demonstração. Seja $\mathfrak{p}$ ideal primo próprio de $R[x]$ com $d(\mathfrak{p}) \subset \mathfrak{p}$ e seja $\mathfrak{a} = \mathfrak{p} \cap R$. Então $\mathfrak{a} \neq R$, $d(\mathfrak{a}) \subset \mathfrak{a}$ e, como R é d-simples, segue-se que $\mathfrak{a} = 0$. Portanto, existe $\mathfrak{q}$ ideal primo de $k[x]$ tal que $\mathfrak{q}^r = \mathfrak{p}$ em que r é o homomorfismo de restrição. Note então que

$$d(\mathfrak{q}) = d(\mathfrak{p}^e) \subset \mathfrak{p}^e = \mathfrak{q},$$

em que e é o homomorfismo de extensão. Logo os homomorfismos de restrição e de extensão garantem a bijeção de d-ideais. □

Observe que o lema acima nos diz, então, que $R[x]$ é d-simples se, e somente se, $k[x]$ é d-simples. Usando o Teorema 3.1.4, temos um resultado mais forte.

Teorema 3.1.6. *Sejam R um domínio de integridade, $d \in \mathrm{Der}(R[x])$ com $d(x) = f(x)$ e $d(R) \subset R$ e suponha que R é d-simples. Então $R[x]$ não é d-simples se, e somente se $d(\alpha) = f(\alpha)$ para todo $\alpha \in \overline{k}$.*

Definição 3.1.7. *Sejam $(R, \mathfrak{m}, k)$ com $k = R/\mathfrak{m}$ um anel local e completo e $S \subset R$ um subanel. Dizemos que um elemento $a \in R$ é analiticamente independente sobre S se a aplicação $\varphi : S[[t]] \to R$ definida por $\varphi|_S = id$ e $\varphi(t) = a$ é injetiva.*

Dada uma derivação $d \in \mathrm{Der}(R)$, iremos considerar a aplicação $\theta : R^{[[t]]} \to R^{[[t]]}$ definida por

$$\theta(a) = \sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!} d^n(a),$$

para cada $a \in R$ e em que $d^n = d^{n-1} \circ d$ e $d^0 = id$. A primeira coisa a notar é que θ é linear. De fato, isso se segue do fato de d^n ser linear para todo $n \geq 0$. Em segundo lugar, se definimos $d(x) = 1$ para algum $x \in R$, então e $d^n(x) = 0$ para $n > 0$. Portanto,

$$\theta(x) = d^0(x) - d^1(x)x = 0.$$

Por fim, note que essa aplicação é também um automorfismo. Com efeito, sejam $a, b \in R$ e observemos que

$$d^n(ab) = \sum_{i+j=n} \binom{n}{i} d^i(a) d^j(b) = \sum_{i+j=n} n! \frac{d^i(a)}{i!} \frac{d^j(b)}{j!}.$$

Portanto,

$$\begin{aligned} \theta(ab) = \sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!} d^n(ab) &= \sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!} \left(\sum_{i+j=n} n! \frac{d^i(a)}{i!} \frac{d^j(b)}{j!} \right) \\ &= \left(\sum_{i=0}^{\infty} (-1)^i \frac{x^i}{i!} d^i(a) \right) \left(\sum_{j=0}^{\infty} (-1)^j \frac{x^j}{j!} d^j(b) \right) = \theta(a)\theta(b). \end{aligned}$$

Teorema 3.1.8 (Zariski)**.** *Seja $(R, \mathfrak{m}, k)$ um anel local completo. Suponha que existam uma derivação $d \in \mathrm{Der}(R)$ e um elemento $x \in \mathfrak{m}$ tais que $d(x) \in R^\times$. Então existe um subanel $B \subset R$ tal que:*

(i) $d|_B = 0$.

(ii) x *é analiticamente independente sobre* B.

(iii) $R = B[[x]]$.

Demonstração. Observe, primeiramente, que desde que $d(x) \in R^\times$ podemos assumir que $d(x) = 1$.

(i) Vamos mostrar que $B = \theta(R)$ satisfaz (i). Com efeito, se $b \in B$, então existe $a \in R$ com

$$b = \sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!} d^n(a).$$

Da definição de derivação, temos

$$d(b) = \sum_{n=0}^{\infty} (-1)^{n+1} \frac{(n+1)x^n}{(n+1)!} d^{n+1}(a) + \sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!} d^{n+1}(a) = 0$$

Isso prova (i).

(ii)

Afirmação 1: $\ker(\theta) = (x)$.

Se $a \in \ker(\theta)$, então

$$0 = \sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!} d^n(a)$$

isto é,

$$a = x(\sum_{n=1}^{\infty} (-1)^n \frac{x^{n-1}}{n!} d^n(a)).$$

Logo, $a \in (x)$. Por outro lado, note que $\theta(x) = 0$ e, portanto, $\theta(ax) = 0$ para todo $a \in R$ o que prova a afirmação.

Afirmação 2: $(x) \cap B = 0$.

Com efeito, se $c \in B$, então $\theta(c) = c$, pois $\theta(x) = 0$. Se ainda $c \in (x) = \ker(\theta)$ temos $c = 0$.

Suponhamos, então, $\sum_{n=0}^{\infty} a_n x^n = 0$, em que $a_n \in B$ para todo $n \geq 0$. Vamos mostrar que $a_n = 0$ para todo $n \geq 0$. Da linearidade de θ, temos

$$0 = \theta(\sum_{n=0}^{\infty} a_n x^n) = \theta(a_0) + \theta(x\beta)$$

em que $\beta = \sum_{n=1}^{\infty} a_n x^{n-1}$. Como $\ker(\theta) \cap B = 0$, segue-se que $\theta(x\beta) = 0$ e desde que $d(B) = 0$, temos que $\theta(a_0) = a_0 = 0$. Agindo da mesma forma para cada $n \in \mathbb{N}$, isso prova (ii).

(iii) Primeiramente, desde que $\theta(a) \in B$, temos, por (i), que $d^n(\theta(a)) = 0$ para todo $n > 0$ e todo $a \in R$. Logo, $\theta^2 = \theta$ e, portanto,

$$\theta(a - \theta(a)) = \theta(a) - \theta^2(a) = \theta(a) - \theta(a) = 0.$$

Logo, $a - \theta(a) \in \ker(\theta) = (x)$ e portanto, existe $a_1 \in R$ tal que $a = b_0 + a_1 x$, em que $b_0 = \theta(a)$. Agindo da mesma forma com a_1, obtemos $a_2 \in R$ e $b_1 = \theta(a_1) \in B$ tal que $a = b_0 + b_1 x + a x^2$. Por indução, segue-se que $a \in B[[x]]$, para todo $a \in R$. Da independencia analitica de x sobre B, segue-se que essa expressão é única. Isso prova (iii). □

Sabemos que todo ideal em $\mathbb{K}[[x]]$ é da forma (x^a) para algum $a \in \mathbb{N}$. Portanto, de 2.1.10, temos

$$\partial_x((x^a)) \subset (x^{a-1}) \not\subset (x^a),$$

para todo $a \in \mathbb{N}$. Isso mostra que $\mathbb{K}[[x]]$ é ∂_x-simples.

Corolário 3.1.9. *Se $n \geq 2$, então $R = \mathbb{K}^{[[n]]}$ não é d-simples para toda derivação $d \in \mathrm{Der}_{\mathbb{K}}(R)$.*

Demonstração. Seja $\mathfrak{m}$ ideal maximal do anel completo local R e suponhamos que exista derivação d com R d-simples. Isto é, $d(\mathfrak{m}) \not\subset \mathfrak{m}$ e portanto, existe $x \in \mathfrak{m}$ tal que $d(x) \in R^{\times}$.

Pelo Teorema 3.1.8, existe $B \subset R$ subanel tal que $R = B[[x]]$ e $d(B) = 0$. Note que qualquer ideal gerado por elementos de B são d-deais, o que é um absurdo. □

Lema 3.1.10. *Seja R um anel Noetheriano e $d \in \mathrm{Der}(R)$. Se $\mathfrak{a} \subset R$ é d-ideal, então todo ideal primo minimal de $\mathfrak{a}$ é d-ideal.*

Demonstração. Como R é Noetheriano, $\mathfrak{a}$ possui uma quantidade finita de primos minimais $\{p_1, \ldots, p_n\}$. Como $p_1 \cdots p_n \subset \sqrt{\mathfrak{a}}$, segue, da Proposição 2.1.10, que

$$\sum_{i=1}^{n} p_1, \cdots d(p_i) \cdots p_n \subset d(\sqrt{\mathfrak{a}}) \subset \sqrt{\mathfrak{a}} \subset p_1 \cap \cdots \cap p_n$$

Assim,

$$p_1 \cdots d(p_i) \cdots p_n \subset p_j$$

para $j = 1, \ldots, n$. Desde que $p_i \neq p_j$ para $i \neq j$, temos que $d(p_j) \subset p_j$, para cada $j = 1, \ldots, n$. □

Proposição 3.1.11. *Se R é d-simples para alguma derivação $d \in \mathrm{Der}(R)$, então R é domínio.*

Demonstração. Pelo Lema 3.1.10, todo ideal primo minimal de R fica estável por d. Como R é d-simples, então apenas 0 é ideal primo minimal de R. Logo, R é domínio. □

3.2 Derivações de Shamsuddin

Ainda é um problema em aberto descrever completamente as derivações simples de um anel. Porém, Shamsuddin, em sua tese de doutorado [Sha77], conseguiu apresentar uma classe de derivações em que a simplicidade é bastante conhecida.

Teorema 3.2.1 (Shamsuddin)**.** *Seja R uma anel com $\mathrm{char}(R) = 0$, d uma derivação simples em R e $\bar{d}$ definida por $\bar{d}(t) = at + b$ com $a, b \in R$ extensão de d no anel $R[t]$. São equivalentes:*

i) $\bar{d}$ é simples.

ii) Não existe $r \in R$ de modo que $d(r) = ar + b$.

Demonstração. *i)* $\Rightarrow$ *ii)* Suponhamos por absurdo que exista $r \in R$ tal que $d(r) = ar + b$

e tomemos y pertencente ao ideal $(t-r)$, ou seja, $y = c(t-r)$ para algum $c \in R[t]$. Assim

$$\begin{aligned}\bar{d}(y) &= \bar{d}(c(t-r)) \\ &= \bar{d}(c)(t-r) + c\bar{d}(t-r) \\ &= \bar{d}(c)(t-r) + c(\bar{d}(t) - \bar{d}(r)) \\ &= \bar{d}(c)(t-r) + c(at+b-ar-b) \\ &= \bar{d}(c)(t-r) + ca(t-r) \\ &= (\bar{d}(c) + ca)(t-r)\end{aligned}$$

Isso prova que $\bar{d}$ estabiliza o ideal $(t-r)$, o que é um absurdo.

$ii) \Rightarrow i)$ Suponhamos, por absurdo, que $\bar{d}$ não seja simples, isto é, que exista um ideal não trivial $\mathfrak{a} \in R[t]$ com $\bar{d}(\mathfrak{a}) \subset \mathfrak{a}$. Como $\bar{d}|_R = d$, segue-se que $\mathfrak{a} \cap R$ é d-ideal e portanto, da simplicidade de d, temos que $\mathfrak{a} \cap R = 0$. Agora, seja $n = \min\{\mathrm{gr}(f), f \in \mathfrak{a}, f \neq 0\}$ em que gr é a função grau e consideremos o seguinte conjunto:

$$\sigma(\mathfrak{a}) = \{0\} \cup \{r \in R; \exists f \in \mathfrak{a}, \mathrm{gr}(f) = n \text{ e } c_f = r\}$$

em que c_f é o coeficiente líder de f. Observemos que $n \geq 1$, isto é, não existem constantes em $\mathfrak{a}$, pois $\mathfrak{a} \cap R = 0$. Afirmamos que $\sigma(\mathfrak{a})$ é ideal de R. Com efeito, sejam $r_1, r_2 \in \sigma(\mathfrak{a})$ e polinômios $f_1, f_2 \in \mathfrak{a}$ satisfazendo $\mathrm{gr}(f_1) = \mathrm{gr}(f_2) = n$ com respectivos coeficientes líderes $c_{f_1} = r_1$ e $c_{f_2} = r_2$. Note que $r_1 + r_2 \in \sigma(\mathfrak{a})$, pois $\mathrm{gr}(f_1 + f_2) = n$ ou $\mathrm{gr}(f_1 + f_2) = 0$ e $c_{f_1+f_2} = c_{f_1} + c_{f_2}$. Além disso, sejam $\alpha \in R$, $r \in \sigma(\mathfrak{a})$ e f polinômio com $\mathrm{gr}(f) = n$ e $c_f = r$. Então $\alpha r \in \sigma(\mathfrak{a})$, pois $\mathrm{gr}(\alpha f) = n$ e $c_{\alpha f} = \alpha r$ Agora, note que $\sigma(\mathfrak{a})$ é d-estável. De fato, se $r \in \sigma(\mathfrak{a})$, então existe um polinômio $f(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + rt^n$ em que $a_i \in R$ e definamos o polinômio $g(t) = \bar{d}(f) - naf$. Observe que

$$\bar{d}(rt^n) = d(r)t^n + rnt^{n-1}\bar{d}(t) = d(r)t^n + rnt^{n-1}(at+b);$$

isto é, $\mathrm{gr}(g) = n$ e $c_g = d(r)$. Logo, $d(r) \in \sigma(\mathfrak{a})$ e portanto, $\sigma(\mathfrak{a}) = R$, pois d é simples e $\sigma(\mathfrak{a}) \neq 0$. Assim, $1 \in \sigma(\mathfrak{a})$, donde se segue que existe um polinômio $h(t) = b_0 + b_1 t + \cdots + b_{n-1}t^{n-1} + t^n$ com $b_i \in R$. Considere g como acima e note que

$$g = st^{n-1} + s_{n-2}t^{n-2} + \cdots + s_0;$$

em que $s_0, \ldots, s_{n-2} \in R$ e $s = nb + d(b_{n-1}) - ab_{n-1}$. Porém, note que $g \in \mathfrak{a}$, o que contraria a minimalidade de n, donde se segue que $s = 0$. Isto nos diz que $d(r) = ar + b$, com $r = -\dfrac{b_{n-1}}{n}$, o que é um absurdo. □

Sejam $a, b \in \mathbb{K}[x]$. Para simplicar a notação, nos referiremos como $d_{a,b}$ à família de derivações de Shamsuddin de $\mathbb{K}[x,y]$ tais que $d_{a,b}(x) = 1$ e $d_{a,b}(y) = ay + b$.

Corolário 3.2.2. *Sejam $a, b \in \mathbb{K}[x]$. Então $d_{a,b}$ não é simples se, e somente se, existe $f \in \mathbb{K}[x]$ tal que $f' = af + b$.*

Demonstração. Tome $d = \partial_x$, $R = \mathbb{K}[x]$ e $t = y$ e aplique 3.2.1. □

Proposição 3.2.3. *Sejam $a, b \in \mathbb{K}[x]$. Vale:*

i) $d_{a,0}$ não é simples.

ii) $d_{0,b}$ não é simples.

iii) Se $a, b \neq 0$ e $\mathrm{gr}(a) > \mathrm{gr}(b)$, então $d_{a,b}$ é simples.

iv) Se $a, b \neq 0$, $\mathrm{gr}(a) = \mathrm{gr}(b)$ e $d_{a,b}$ não é simples, então existe $\sigma \in \mathbb{K}^*$ tal que $b = \sigma a$.

v) Se $d_{a,b}$ e $d_{a,c}$ não são simples, então $d_{a,b+\alpha c}$ não é simples para todo $\alpha \in \mathbb{K}^*$.

Demonstração. i) (y) é um $d_{a,0}$-ideal.

ii) Tome $f \in \mathbb{K}[x]$ tal que $f' = b$ e use o Corolário 3.2.2.

iii) Suponha, por absurdo, que $d_{a,b}$ não seja simples. Pelo Colorário 3.2.2, existe $f \in \mathbb{K}[x]$ com $f' = af + b$ e, desde que $b \neq 0$, segue-se que $f \neq 0$. Porém, como $\mathrm{gr}(a) > \mathrm{gr}(b)$, temos

$$\mathrm{gr}(f) - 1 = \mathrm{gr}(f') = \max\{\mathrm{gr}(af), \mathrm{gr}(b)\} = \mathrm{gr}(a) + \mathrm{gr}(f) \geq \mathrm{gr}(f),$$

o que é uma contradição.

iv) Como $d_{a,b}$ não é simples, existe $f \in \mathbb{K}[x]$ tal que $f' = af + b$. Agora, em primeiro lugar, se $f = 0$, então $b = 0$ e, sendo $\mathrm{gr}(a) = \mathrm{gr}(b)$, temos que $a = 0$, donde $b = 1a$. Em segundo lugar, se $f = -\alpha \in \mathbb{K}^*$, então $0 = a(-\alpha) + b$, donde $b = \alpha a$. Por fim, se $\mathrm{gr}(f) \geq 1$, então, novamente, temos $\mathrm{gr}(f) > \mathrm{gr}(f)$, o que é um absurdo.

v) Desde que $d_{a,b}$ e $d_{a,c}$ não são simples, existem $f, g \in \mathbb{K}[x]$ em que $f' = af + b$ e $g' = ag + c$. Então, se $\alpha \in \mathbb{K}^*$, temos $(f + \alpha g)' = a(f + \alpha g) + (b + \alpha c)$, isto é, $d_{a,(b+\alpha c)}$ não é simples. □

Proposição 3.2.4. *Sejam $a, b, c, r \in \mathbb{K}[x]$, com $a \neq 0$ e suponhamos que $b = ac + r$ tal que $\mathrm{gr}(r) < \mathrm{gr}(a)$. Então $d_{a,b}$ não é simples se, e somente se, $d_{a,c'+r}$ não é simples.*

Demonstração. Comecemos notando que

$$c' = c' + ac - ac = ac + (c' - ac).$$

Logo, sendo $f = c$ e $b = c' - ac$, por 3.2.2, $d_{a,c'-ac}$ não é simples.

$(\Rightarrow)$ Do que foi dito acima e do fato de $d_{a,b}$ não ser simples, segue-se de 3.2.3 item (v) que $d_{a,b+c'-ac}$ não é simples. Como $b = ac + r$, temos que $d_{a,c'+r}$ não é simples.

$(\Leftarrow)$ Como $d_{a,c'+r}$ e $d_{a,c'-ac}$ não são derivações simples, de 3.2.3 item (v) segue-se que $d_{a,c'+r-c'+ac} = d_{a,b}$ não é simples. □

3.3 Caso local

Dado um campo de vetores analítico d definido em $\mathbb{C}^n$ e um ponto $p = (p_1, \ldots, p_n) \in \mathbb{C}^n$ com $d(p) \neq 0$, a teoria clássica de equações diferenciais nos diz que existe um aberto $D \subset \mathbb{C}$ e uma única aplicação analítica $\gamma : D \to \mathbb{C}^n$ tal que $\gamma'(t) = d(\gamma(t))$ para todo $t \in D$ e $\gamma(0) = p$.

Consideremos agora o anel de germes de funções analíticas $\mathcal{O}_{n,p}$, em que $p \in \mathbb{C}^n$, isto é, o anel de séries formais sobre $\mathbb{C}$ com raio de convergência positivo. Note que se d é uma derivação em $\mathcal{O}_{n,p}$, então, por 2.1.9, $d = \sum_{i=1}^{n} f_i \partial_{z_i}$ em que $f_i \in \mathcal{O}_{n,p}$ para cada $i = 1, \ldots, n$. Assim, o conceito de solução significa encontrar n funções analíticas numa vizinhança de zero $z_1(t), \ldots, z_n(t)$ tais que

$$\begin{cases} z_i'(t) = f_i(z_1(t), \ldots, z_n(t)) \\ z_i(0) = p_i \end{cases}$$

para cada $i = 1, \ldots, n$. Cada elemento de $\mathcal{O}_{n,p}$ pode ser representado como uma série formal em $z_1 - p_1, \ldots, z_n - p_n$. Então, podemos construir um $\mathbb{C}$-homomorfismo $\varphi : \mathcal{O}_{n,p} \to \mathcal{O}_{n,0}$ tal que $\varphi(z_i) = z_i(t)$. Dessa forma, $\varphi(f)(0) = 0$ se, e somente se, $f(p) = 0$.

Ao longo dessa seção, necessitamos que $\mathbb{K}$ seja algebricamente fechado e que R seja uma $\mathbb{K}$-álgebra.

Definição 3.3.1. *Sejam d uma derivação, $\mathfrak{p} \in \operatorname{Spec}(R)$ e $k(\mathfrak{p})$ o corpo residual de $\mathfrak{p}$. Definimos a solução de d passando por $\mathfrak{p}$ como o $\mathbb{K}$-homomorfismo $\varphi : R \to k(\mathfrak{p})[[t]]$ que satisfaz $\varphi \circ d = \partial_t \circ \varphi$ e $\varphi^{-1}((t)) = \mathfrak{p}$. Dizemos ainda que φ é não-trivial se $\varphi(R) \not\subset k(\mathfrak{p})$.*

Decorre do primeiro teorema do isomorfismo que uma solução é não trivial se, e somente se, existe um homomorfismo injetivo $R/\ker\varphi \to k(\mathfrak{p})$. Semelhante à aplicação usada no Teorema de Zariski, lançaremos mão do que aqui, chamaremos de R-automorfismo *exponencial* $e^{td} : R[[t]] \to R[[t]]$ dado por

$$f \longmapsto \sum_{n=0}^{\infty} \frac{t^n}{n!} d^n(f).$$

A restrição $e^{td}|_R$ é um $\mathbb{K}$-homomorfismo.

Dado um ideal primo $\mathfrak{p} \in R$ definamos $\sigma_{\mathfrak{p}} : R \to k(\mathfrak{p})$ o homomorfismo canônico e consideremos a extensão natural de séries formais $\sigma_{\mathfrak{p}} \otimes 1 : R[[t]] \to k(\mathfrak{p})[[t]]$ em que $1 = id|_{k(\mathfrak{p})[[t]]}$. A próxima proposição nos dá o primeiro de exemplo de solução de uma derivação.

Proposição 3.3.2. *A aplicação $(\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td} : R \to k(\mathfrak{p})[[t]]$ define uma solução de d passando por $\mathfrak{p}$. Além disso, essa solução é trivial se, e somente se, $\sigma_{\mathfrak{p}} \circ d = 0$.*

Demonstração. Seja $x \in R$. Então,

$$\begin{aligned}((\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td} \circ d(x)) &= (\sigma_{\mathfrak{p}} \otimes 1)(e^{td}(d(x)) \\ &= (\sigma_{\mathfrak{p}} \otimes 1)\left(\sum_{n=0}^{\infty} \frac{t^n}{n!} d^{n+1}(x)\right).\end{aligned}$$

Como a soma acima pertence a $R[[t]]$, segue-se que

$$\begin{aligned}((\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td} \circ d(x)) &= (\sigma_{\mathfrak{p}} \otimes 1)\left(\sum_{n=0}^{\infty} \frac{t^n}{n!} d^{n+1}(x)\right) \\ &= \sum_{n=0}^{\infty} \frac{t^n}{n!} \sigma_{\mathfrak{p}}(d^{n+1}(x)) \\ &= \partial_t \left(\sum_{n=-1}^{\infty} \frac{t^{n+1}}{(n+1)!} \sigma_{\mathfrak{p}}(d^{n+1}(x))\right),\end{aligned}$$

fazendo $k = n + 1$,

$$\begin{aligned}((\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td} \circ d(x)) &= \partial_t \left(\sum_{k=0}^{\infty} \frac{t^k}{k!} \sigma_{\mathfrak{p}}(d^k(x))\right) \\ &= \partial_t \circ (\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td}(x).\end{aligned}$$

Agora, note que

$$((\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td})(x) \in (t) \Leftrightarrow \sum_{n=0}^{\infty} \frac{t^n}{n!} \sigma_{\mathfrak{p}}(d^n(x)) = t \cdot \sum_{n=0}^{\infty} a_n t^n,$$

para alguma série $\sum_{n=0}^{\infty} a_n t^n \in R[[t]]$. Mas, isso acontece se, e somente se, $\sigma_{\mathfrak{p}}(x) = 0$, isto é, $x \in \mathfrak{p}$. Isso mostra que $((\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td})^{-1}((t)) = \mathfrak{p}$ e, portanto, segue-se que $((\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td})$ é solução de d passando por $\mathfrak{p}$.

Vamos provar que essa solução é trivial se, e somente se, $\sigma_{\mathfrak{p}} \circ d = 0$. Com efeito, suponha $((\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td})(R) \subset k(\mathfrak{p})$. Então, se $x \in R$, segue-se que

$$\sum_{n=0}^{\infty} \frac{t^n}{n!} \sigma_{\mathfrak{p}}(d^n(x)) \in k(\mathfrak{p}).$$

Ou seja, $\sigma_{\mathfrak{p}}(d^n(x)) = 0$ para todo $n \geq 1$. Em particular, $(\sigma_{\mathfrak{p}} \circ d)(x) = 0$ para todo $x \in R$.

Por outro lado, se $(\sigma_{\mathfrak{p}} \circ d)(x) = 0$, então, por indução, $(\sigma_{\mathfrak{p}} \circ d^n)(x) = 0$ para todo $n \geq 1$. Da arbitrariedade de $x \in R$, isso mostra que $((\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td})(R) \subset k(\mathfrak{p})$. □

Da mesma forma que no cálculo em uma variável, toda série $f \in \mathbb{K}^{[[n]]}$ possui uma expansão em série de Taylor

$$f(x) = \sum_{\substack{|\alpha|=k \\ k=0}} \frac{1}{\alpha!} \partial^{\alpha} f(p)(x-p)^{\alpha}, \tag{3.1}$$

em que $\alpha = (\alpha_1, \ldots, \alpha_n)$ é uma n-tupla de números naturais com $|\alpha| = \alpha_1 + \cdots + \alpha_n$, $\alpha! = \alpha_1! \cdots \alpha_n!$, $x^\alpha = x^{\alpha_1} \cdots x^{\alpha_n}$ e $\partial^\alpha = \partial_{x_1}^{\alpha_1} \cdots \partial_{x_n}^{\alpha_n}$.

Seja $R \to S$ um homomorfismo de anéis. Dizemos que S é uma R-álgebra de tipo finito se existe um $n \in \mathbb{N}$ e um homomorfismo sobrejetor $R[x_1, ..., x_n] \to S$.

Analogamente ao que ocorre na teoria de equações diferenciais, temos um teorema de existência e unicidade de soluções.

Teorema 3.3.3. *Suponhamos que R Noetheriana de tipo finito ou da forma $R = \mathbb{K}^{[[n]]}/I$ com I ideal em $\mathbb{K}^{[[n]]}$, $\mathfrak{p} \in \mathrm{Spec}(R)$ e $d \in \mathrm{Der}(R)$. Se $\mathfrak{p}$ é maximal, então d admite uma única solução passando por $\mathfrak{p}$.*

Demonstração. Note que, de 3.3.2, necessitamos apenas mostrar a unicidade. Consideremos $R = \mathbb{K}^{[[n]]}/I$ e d derivação de $\mathbb{K}^{[[n]]}/I$. O caso em que R é de tipo finito é análogo. Pelo Lema 2.1.11, d é proveniente de $d_1 \in \mathrm{Der}(\mathbb{K}^{[[n]]})$ com $d_1(I) \subset I$. Por 2.1.9,

$$d_1 = \sum_{k=1}^{n} f_k \partial_{x_k},$$

em que $f_k \in \mathbb{K}^{[[n]]}$ para $i = 1, ..., n$. Agora, seja $\varphi : \mathbb{K}^{[[n]]} \to \mathbb{K}[[t]]$ solução de d_1 passando pelo ideal maximal M com $M/I = \mathfrak{m}$ e ponha $\varphi(x_i) = x_i(t)$, $i = 1, ..., n$ com $x(t) = (x_1(t), ..., x_n(t))$. Observe que, dessa forma, $(x_1 - p_1, ..., x_n - p_n) = M$ em que $p_i = x_i(0)$ com $i = 1, ..., n$. Note também que $f_i(x(t)) = \partial_t(x_i(t))$, para cada $i = 1, ..., n$. De fato, desde que $\varphi \circ d_1 = \partial_t \circ \varphi$, temos

$$\partial_t(x_i(t)) = \partial_t(\varphi(x_i)) = \varphi(d_1(x_i)) = \varphi(f_i(x_i)) = f_i(x(t)).$$

Portanto, tomando o desenvolvimento de Taylor de f_i para cada $i = 1, ..., n$ e truncando a série no grau $r \in \mathbb{N}$, temos que

$$\partial_t(x_i(t)) = f_i(x(t)) \equiv \sum_{|\alpha|=0}^{r} \frac{1}{\alpha!} \partial^\alpha f_i(p)(x(t) - p)^\alpha \mod (t^{r+1})$$

Observe, então, que o coeficiente de grau r de cada $\partial_t(x_i(t))$ é unicamente determinado por um número finito de coeficientes de $f_i's$ e dos coeficientes de $(x_i(t) - p_i)$. Isso nos diz que φ é unicamente determinada pelos $f_i's$ e pelo ponto p. Por fim, como $d_1(I) \subset I$, então da Proposição 2.1.11 segue-se que φ gera uma única solução em $\mathbb{K}^{[[n]]}/I$ passando por $\mathfrak{m}$. □

Lema 3.3.4. *Seja R uma $\mathbb{K}$-álgebra Noetheriana, $d \in \mathrm{Der}_{\mathbb{K}}(R)$ e um ideal primo $\mathfrak{p} \subset R$. Então existe um único ideal primo $\mathfrak{q} \subset \mathfrak{p}$ que é maximal entre todos os ideais $\mathfrak{a}$ de R tais que $d(\mathfrak{a}) \subset \mathfrak{a}$.*

Demonstração. [Bal14, p. 12]. □

O próximo teorema mostra a ligação forte que existe entre o conceito de solução de uma derivação e a simplicidade de um anel localizado.

Teorema 3.3.5. *Seja R uma $\mathbb{K}$-álgebra, $d \in \mathrm{Der}_{\mathbb{K}}(R)$, $\mathfrak{p} \in \mathrm{Spec}(R)$ e suponha que exista uma solução não-trivial $\varphi : R \to k(\mathfrak{p})[[t]]$ de d passando por $\mathfrak{p}$. São equivalentes:*

i) $R_{\mathfrak{p}}$ é d-simples.

ii) $\varphi|_{R_{\mathfrak{p}}}$ é injetiva.

Demonstração. ($\Rightarrow$) Primeiramente, como φ é não trivial, $\varphi_{\mathfrak{p}}$ também é não-trivial e $\ker(\varphi_{\mathfrak{p}}) \not\subset \mathfrak{p}R_{\mathfrak{p}}$, pois localização preserva inclusão. Seja $x \in \ker(\varphi_{\mathfrak{p}})$, então

$$d(\varphi_{\mathfrak{p}}(x)) = \partial_t(\varphi_{\mathfrak{p}}(x)) = 0.$$

Logo, $d(\ker(\varphi_{\mathfrak{p}})) \subset \ker(\varphi_{\mathfrak{p}})$. Como $R_{\mathfrak{p}}$ é d-simples, então $\ker(\varphi_{\mathfrak{p}}) = 0$.

($\Leftarrow$) Como $R_{\mathfrak{p}}$ é Noetheriano, do Lema 3.3.4 existe ideal $\mathfrak{a} \subset \mathfrak{p}R_{\mathfrak{p}}$ maximal entre todos os ideais tais que $d(\mathfrak{a}) \subset \mathfrak{a}$. Como $\varphi_{\mathfrak{p}}$ é solução de d passando por $\mathfrak{p}R_{\mathfrak{p}}$, $\partial_t(\varphi_{\mathfrak{p}}(\mathfrak{a})) \subset \varphi_{\mathfrak{p}}(\mathfrak{a})$ e $\varphi_{\mathfrak{p}}(\mathfrak{a}) \subset (t)$. Como ∂_t é simples, segue-se que $\mathfrak{a} \subset \ker \varphi_{\mathfrak{p}}$. Do fato de $\varphi_{\mathfrak{p}}$ ser injetiva e da maximalidade de $\mathfrak{a}$, temos que $R_{\mathfrak{p}}$ é d-simples. □

Terminamos essa seção apresentando dois exemplos de soluções.

Exemplo 3.3.6. Consideremos o anel $R = \mathbb{K}[x, y, z]$ o ideal primo $\mathfrak{p} = (x, y)$ e a derivação $d = \partial_x + \partial_y + \partial_z$. Note que, nesse caso, $k(\mathfrak{p}) = \mathbb{K}(z)$. Se $\varphi : R \to k(\mathfrak{p})[[t]]$ é uma solução de d passando por $\mathfrak{p}$, então, necessariamente, $\varphi \circ d = \partial_t \circ \varphi$. Escrevendo, $\varphi(x) = x(t)$, $\varphi(y) = y(t)$ e $\varphi(z) = z(t)$, esta equação nos dá,

$$x(t) = t + c_1,\ y(t) = t + c_2 \text{ e } z(t) = t + c_3,$$

com $c_i \in k(\mathfrak{p})$ para $i = 1, 2, 3$. Além disso, como $\varphi^{-1}((t)) = \mathfrak{p}$, então $x(t)$ e $y(t)$ pertecem ao ideal, pois $x, y \in \mathfrak{p}$. Isso acontece se, e somente se $c_1 = 0$ e $c_2 = 0$. Agora, note que $\varphi(z) \notin (t)$ e, desde que $k(\mathfrak{p})[[t]]$ é um anel local com ideal maximal (t), segue-se que $\varphi(z) \in k(\mathfrak{p})[[t]]^{\times}$. Ou seja, $z(t) = t + f(t)$ em que $f \in \mathbb{K}(z)$. Explicitamente, temos o homomorfismo

$$\varphi(x, y, z) = (t, t, t + f(t)).$$

Seja $p = (a, b, c) \in \mathbb{K}^3$ e vamos encontrar, agora, a solução de d passando pelo o ideal maximal $\mathfrak{m}_p = (x - a, y - b, z - c)$ de R. Notemos que $k(\mathfrak{p}) = \mathbb{K}$. Agora, se φ_p é solução de d passando por $\mathfrak{m}_p$, então, por 3.3.3, segue-se que φ_p é unica. Portanto, necessariamente devemos ter $c_1 = a$, $c_2 = b$ e $c_3 = c$, o que nos dá

$$\varphi_p(x, y, z) = (t + a, t + b, t + c).$$

Exemplo 3.3.7. Sejam R e $\mathfrak{p}$ como no exemplo anterior e consideremos a derivação $d = y\partial_x + xz\partial_y$. Pimeiramente, seja φ a solução dada na Proposição 3.3.2. Observermos que

$$\varphi(x) = ((\sigma_{\mathfrak{p}} \otimes 1) \circ e^{td})(x) = \sum_{n=0}^{\infty} \frac{t^n}{n!}\sigma_{\mathfrak{p}}(d^n(x)).$$

Note que $(\sigma_{\mathfrak{p}} \circ d)(x) = 0$ e, portanto, em vista da demonstração da Proposição 3.3.2, segue-se que $\sigma_{\mathfrak{p}}(d^n(x)) = 0$. Logo, $\varphi(x) = 0$ e um argumento análogo nos dá $\varphi(y) = 0$. Por fim, como $d^0(z) = z$ e $d^n(z) = 0$ para todo $n \geq 1$, segue-se que essa solução pode ser expressa como

$$\varphi(x, y, z) = (0, 0, z).$$

Agora, vamos considerar $\mathfrak{m}_p$ também como no exemplo anterior e denotar por φ_p a solução dada em 3.3.2 de d passando por $\mathfrak{m}_p$. Como $\varphi_p \circ d = \partial_t \circ \varphi_p$, se $\varphi_p(x) = x(t),\ \varphi_p(y) = y(t)$ e $\varphi_p(z) = z(t)$, temos

$$x'(t) = \varphi_p(y),\ \ y'(t) = \varphi_p(x)\varphi_p(z) \text{ e } z'(t) = 0 \tag{3.2}$$

Primeiramente note que se $\mathfrak{p} \subset \mathfrak{m}_p$, então $p = (0, 0, c)$ e $x(t) = 0, y(t) = 0$ e $z(t) = c$ satisfaz (3.2). Agora, suponhamos $\mathfrak{p} \not\subset \mathfrak{m}_p$, ou seja, $a \neq 0$ e $b \neq 0$ e notemos que $d^{2n+1}(y) = xz^{n+1}$, $d^{2n}(y) = yz^n$, $d^{2n+1}(x) = yz^n$ e $d^{2n}(x) = xz^n$. Vamos analisar o caso $\varphi_p(x)$,

$$\begin{aligned}
(\partial_t \circ \varphi)(x) &= (\varphi \circ d)(x)\\
x'(t) &= \varphi(y)\\
x'(t) &= \sum_{n=0}^{\infty} \frac{t^n}{n!}\sigma_{\mathfrak{m}_p}(d^{n+1}(y))\\
x(t) &= \sum_{n=1}^{\infty} \frac{t^n}{n!}\sigma_{\mathfrak{m}_p}(d^n(y)) + C\\
x(t) &= \sum_{n=1}^{\infty} \frac{t^{2n}}{(2n)!}\sigma_{\mathfrak{m}_p}(yz^n) + \sum_{n=1}^{\infty} \frac{t^{2n+1}}{(2n+1)!}\sigma_{\mathfrak{m}_p}(xz^{n+1}) + C\\
x(t) &= \sum_{n=1}^{\infty} \frac{t^{2n}}{(2n)!}bc^n + \sum_{n=1}^{\infty} \frac{t^{2n+1}}{(2n+1)!}ac^{n+1}
\end{aligned}$$

em que $C = 0$, pois $x(0) = 0$. Agindo da mesma forma para a variável y temos que

$$y(t) = \sum_{n=0}^{\infty} \frac{t^{2n}}{(2n)!}bc^n + \sum_{n=0}^{\infty} \frac{t^{2n+1}}{(2n+1)!}ac^n$$

Por fim, de 3.2, segue-se que $z(t) = c$.

4 Simplicidade e Isotropia

Este é o capítulo central da dissertação. É aqui que vamos finalmente provar e entender um teorema que deixa claro a relação forte que existe entre uma derivação simples e seu grupo de isotropia.

Ao longo dessa e da próxima seção, salvo menção contrária, nos restringiremos apenas ao estudo de derivações sobre o anel $\mathbb{K}[x,y]$ em que $\text{char}(\mathbb{K}) = 0$ e $\mathbb{K}$ algebricamente fechado. Esse capítulo é baseado integralmente em [Men17], [PB19] e [BL20].

4.1 O grupo de Isotropia

Definição 4.1.1. *Definimos o grupo de isotropia de uma derivação d como*

$$\text{Aut}(d) = \{\rho \in \text{Aut}_{\mathbb{K}}(\mathbb{K}[x,y]); d = \rho d \rho^{-1}\}.$$

Observe que esse conjunto, de fato, é um grupo, pois é o estabilizador da ação

$$\begin{gathered}\text{Aut}_{\mathbb{K}}(\mathbb{K}[x,y]) \times \text{Der}_{\mathbb{K}}(\mathbb{K}[x,y]) \to \text{Der}_{\mathbb{K}}(\mathbb{K}[x,y]). \\ (\rho, d) \longmapsto \rho d \rho^{-1}\end{gathered}$$

A primeira coisa que notamos é que essa conjugação preserva simplicidade, isto é, d é simples se, e somente se, $\rho d \rho^{-1}$ é simples para qualquer $\rho \in \text{Aut}_{\mathbb{K}}(\mathbb{K}[x,y])$. De fato, se $\rho d \rho^{-1}$ não é simples, então existe um ideal não trivial $\mathfrak{a} \subset \mathbb{K}[x,y]$ tal que $\rho d \rho^{-1}(\mathfrak{a}) \subset \mathfrak{a}$ e, portanto, $d(\rho^{-1}(\mathfrak{a})) \subset \rho^{-1}(\mathfrak{a})$. Reciprocamente, se d não é simples, então existe ideal não trivial $\mathfrak{a} \subset \mathbb{K}[x,y]$ com $d(\mathfrak{a}) \subset \mathfrak{a}$. Como ρ é automorfismo, existe ideal $\mathfrak{a}_0$ de $\mathbb{K}[x,y]$ tal que $\rho^{-1}(\mathfrak{a}_0) = \mathfrak{a}$. Logo, $d(\rho^{-1}(\mathfrak{a}_0)) \subset \mathfrak{a}$ donde $\rho d \rho^{-1}(\mathfrak{a}_0) \subset \mathfrak{a}_0$.

Além disso, devemos observar que $\text{Aut}(d)$ se comporta bem com relação a essa ação no seguinte sentido, se $d' = \rho d \rho^{-1}$, então $\text{Aut}(d') = \rho(\text{Aut}(d))\rho^{-1}$, ou seja, os grupos de isotropia são conjugados.

O próximo resultado mostra que se d é uma derivação simples, então o único automorfismo de $\text{Aut}(d)$ que fixa um ideal maximal é a identidade. Nesse sentido, essa proposição nos dá uma pista de como deve ser o conjunto $\text{Aut}(d)$ quando d é simples.

Proposição 4.1.2. *Seja $d \in \text{Der}(\mathbb{K}^{[n]})$ derivação simples e $\rho \in \text{Aut}(d)$. Se $\rho(\mathfrak{m}) = \mathfrak{m}$ para algum ideal maximal $\mathfrak{m} \in \mathbb{K}^{[n]}$, então $\rho = id$.*

Demonstração. Em vista de 3.3.3, tomemos $\varphi : \mathbb{K}^{[n]} \to \mathbb{K}[[t]]$ a única solução de d passando pelo ideal maximal $\mathfrak{m}$, então

$$\partial_t \circ \varphi \circ \rho = \varphi \circ d \circ \rho = \varphi \circ \rho \circ d.$$

Mais ainda,

$$\varphi^{-1}((t)) = \mathfrak{m} = \rho(\mathfrak{m}),$$

isto é, $(\varphi \circ \rho)^{-1}(t) = \mathfrak{m}$. Da unicidade da solução, temos que $\varphi \circ \rho = \varphi$. Dessa forma, $\varphi(\rho(g) - g) = 0$ para $g \in \mathbb{K}^{[n]}$, donde se segue que $\rho(g) - g \in \ker \varphi$. Como $\mathbb{K}^{[n]}$ é d-simples e $d(\ker \varphi) \subset \ker \varphi$, segue-se que $\ker \varphi = 0$ e, portanto, $\rho = id$. □

Terminamos essa seção mostrando que o cálculo do grupo de isotropia de uma derivação pode ser trabalhoso mesmo nos casos mais simples.

Exemplo 4.1.3. Seja $d = \partial_x \in \mathrm{Der}_{\mathbb{K}}(\mathbb{K}[x, y])$ e $\rho \in \mathrm{Aut}(d)$. Para encontrar ρ explicitamente devemos resolver o sistema

$$\begin{cases} d(\rho(x)) = \rho(d(x)) & (4.1) \\ d(\rho(y)) = \rho(d(y)) & (4.2) \end{cases}$$

Definindo $\rho(x) = \sum_{i=1}^{n} f_i y^i$ e $\rho(y) = \sum_{j=1}^{m} g_j y^j$ com $f_i, g_j \in \mathbb{K}[x]$, de (4.1), temos que

$$\begin{aligned} d(f_0 + f_1 y + \cdots + f_{n-1} y^{n-1} + f_n y^n) &= 1 \\ d(f_0) + d(f_1) y + \cdots + d(f_{n-1}) y^{n-1} + d(f_n) y^n &= 1, \end{aligned}$$

donde se segue que $d(f_0) = 1$ e $d(f_i) = 0$ para $i = 1, \ldots, n$. Ou, seja

$$\rho(x) = x + c_0 + c_1 y + \cdots + c_n y^n = x + P(y),$$

em que $P(y) \in \mathbb{K}[y]$. De (4.2), temos

$$\begin{aligned} d(g_0 + g_1 y + \cdots + g_{m-1} y^{m-1} + g_m y^m) &= 0, \\ d(g_0) + d(g_1) y + \cdots + d(g_{m-1}) y^{m-1} + d(g_m) y^m &= 0, \end{aligned}$$

o que implica que $d(g_j) = 0$ para $j = 1, \ldots, m$, de modo que

$$\rho(y) = e_0 + \cdots + e_m y^m$$

em que $e_j \in \mathbb{K}$ com $j = 1, \ldots, m$. Pela Proposição 2.2.4, temos que

$$\det J(\rho) = \det \begin{pmatrix} \partial_x \rho(x) & \partial_y \rho(x) \\ \partial_x \rho(y) & \partial_y \rho(y) \end{pmatrix} \in \mathbb{K}^*, \tag{4.3}$$

isto é, $\mathrm{gr}(\rho(y)) = 1$. Logo,

$$\mathrm{Aut}(d) = \{\rho : \rho(x) = x + P(y),\ \rho(y) = e + \beta y,\ P \in \mathbb{K}[y], e \in \mathbb{K} \text{ e } \beta \in \mathbb{K}^*\}.$$

Podemos dizer mais ainda sobre a estrutura de $\mathrm{Aut}(d)$. Se $\rho_1, \rho_2 \in \mathrm{Aut}(d)$, então $\rho_i(x) = x + P_i(y)$ e $\rho_i(y) = e_i + \beta_i y$ com $P_i \in \mathbb{K}[y], e_i \in \mathbb{K}$ e $\beta_i \in \mathbb{K}^*$ para $i = 1, 2$. Logo,

$$\begin{aligned}\rho_1\rho_2(x) &= \rho_1(x + P_2(y)) \\ &= \rho_1(x) + \rho_1(P_2(y)) \\ &= x + P_3(y),\end{aligned}$$

em que $P_3(y) = P_1(y) + P_2(e_1 + \beta_1 y) \in \mathbb{K}[y]$. Além disso,

$$\begin{aligned}\rho_1\rho_2(y) &= \rho_1(e_2 + \beta_2 y) \\ &= \rho_1(e_2) + \rho_1(\beta_2)\rho_1(y) \\ &= e_2 + \beta_2(e_1 + \beta_1 y) \\ &= e_2 + \beta_2 e_1 + \beta_2\beta_1 y.\end{aligned}$$

Por fim, temos que $\mathrm{Aut}(d) = J_2(\mathbb{K}) \rtimes (\mathbb{K} \ltimes \mathbb{K}^*)$ através do isomorfismo

$$\begin{aligned}\psi : \mathrm{Aut}(d) &\to J_2(\mathbb{K}) \rtimes (\mathbb{K} \ltimes \mathbb{K}^*) \\ (\rho(x), \rho(y)) &\mapsto (x + P_3(y), (e_2 + \beta_2 e_1, \beta_1\beta_2 y)).\end{aligned}$$

4.2 Um critério para simplicidade

Proposição 4.2.1. *Seja d uma derivação e $\rho \in \mathrm{Aut}(d)$. Suponhamos que $\rho(\mathfrak{m}) = \mathfrak{m}$ para algum ideal maximal $\mathfrak{m}$ com $d(\mathfrak{m}) \nsubseteq \mathfrak{m}$. Então existe um ideal principal $\mathfrak{a} \subset \mathfrak{m}$ tal que:*

- *(i) $\mathfrak{a}$ é estável por d e fixo por ρ;*
- *(ii) ρ induz a aplicação identidade em $\mathbb{K}[x, y]/\mathfrak{a}$.*

Demonstração. (i) Comecemos considerando a única solução de d passando por $\mathfrak{m}$, $\varphi : \mathbb{K}[x, y] \to \mathbb{K}[[t]]$. Afirmamos que $\ker(\varphi)$ satisfaz as condições acima. Com efeito, se $g \in \ker(\varphi)$ então $\varphi(g) = 0$. Mas, $\varphi(d(g)) = \partial_t(\varphi(g)) = 0$ e isso mostra que $d(\ker\varphi) \subset \ker\varphi$. Agora, das propriedades de φ, temos que

$$\partial_t \circ \varphi \circ \rho = \varphi \circ d \circ \rho = \varphi \circ \rho \circ d.$$

Além disso $(\varphi \circ \rho)^{-1}(t) = \mathfrak{m}$. Dessa forma, $\varphi \circ \rho$ é uma solução de d passando por $\mathfrak{m}$. Pela unicidade de φ temos que $\varphi \circ \rho = \varphi$. Portanto, se $g \in \ker(\varphi)$, então $\varphi(\rho(g)) = \varphi(g) = 0$. Logo, temos $\rho(\ker(\varphi)) \subset \ker(\varphi)$. Como ρ é automorfismo, segue-se que $\rho(\ker(\varphi)) = \ker(\varphi)$.

(ii) Seja $g \in \mathbb{K}[x, y] \setminus \ker(\varphi)$, então, do que foi visto em (i), temos $\varphi(\rho(g) - g) = \varphi(\rho(g)) - \varphi(g) = \varphi(g) - \varphi(g) = 0$. Portanto, $\rho(g) - g \in \ker(\varphi)$, ou seja, $\rho(g) = g + \ker(\varphi)$.

Para completar o resultado, devemos mostrar que $\ker(\varphi)$ é ideal principal. De fato, como $\ker(\varphi)$ é um ideal primo estritamente contido em $\mathfrak{m}$, segue-se que a altura de $\ker(\varphi)$ é no máximo 1. Se a altura de $\ker(\varphi)$ for zero, não há nada a provar. O resultado segue do fato que num domínio de fatoração única, todo ideal primo de altura 1 é principal. □

Observe que o ideal $\mathfrak{a}$ pode ser trivial. De fato, se d é simples então os únicos ideais estáveis por d são 0 e $\mathbb{K}[x,y]$. Note também que se ρ é a identidade, então a parte (ii) do lema acima não traz informações novas.

Devido à estrutura bem conhecida do anel $\mathbb{K}[x,y]$ podemos provar algo, em certo sentido, mais forte do que foi provado em 4.1.2.

Proposição 4.2.2. *Seja d uma derivação simples e $\rho \in \mathrm{Aut}(d)$. Se $\rho \neq id$, então não existe $n \in \mathbb{N}$ tal que ρ^n fixa um ideal maximal. Em particular, ou $\rho = id$ ou ρ tem ordem infinita.*

Demonstração. Comecemos supondo, por absurdo, que existam um ideal maximal $\mathfrak{m}$ de $\mathbb{K}[x,y]$ e $n \in \mathbb{N}$ tais que $\rho^n(\mathfrak{m}) = \mathfrak{m}$. Como $\mathrm{Aut}(d)$ é grupo, temos que $\rho^n \in \mathrm{Aut}(d)$. Além disso, $d(\mathfrak{m}) \not\subset \mathfrak{m}$, pois d é simples. Portanto, pela Proposição 4.2.1 (i), existe ideal principal $\mathfrak{a} \subset \mathfrak{m}$, de modo que $d(\mathfrak{a}) \subset \mathfrak{a}$ e $\rho^n(\mathfrak{a}) = \mathfrak{a}$. Como d é simples, segue-se que $\mathfrak{a} = 0$ e assim, do item (ii) de 4.2.1, temos que $\rho^n = id$. Agora, pelo teorema de Van Der Kulk, existe um automorfismo linear α e $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x,y])$ com $\sigma^{-1}\rho\sigma = \alpha$. Como α é linear, α fixa o ideal maximal $\mathfrak{m}_0 = (x,y)$, donde se segue que, ρ fixa o ideal maximal $\sigma(\mathfrak{m}_0)$. Fazendo uso novamente de 4.2.1, segue-se que $\rho = id$. □

Devido ao seu carater técnico, dividiremos o próximo resultado numa série de afirmações.

Lema 4.2.3. *Seja d uma derivação simples e $\rho \in \mathrm{Aut}(d)$. Se ρ estabiliza o ideal gerado por $x \in \mathbb{K}[x,y]$, então $\rho = id$.*

Demonstração. Primeiramente, note que se ρ tem ordem finita então, pela Proposição 4.2.2, teremos necessariamente $\rho = id$. Suponhamos então, por absurdo, que ρ tem ordem infinita.

Afirmação 1: Podemos escrever $\rho(x) = \alpha x$ e $\rho(y) = g(x) + y$, com $\alpha \in \mathbb{K}^*$, e $0 \neq g \in \mathbb{K}[x]$.

Como $\rho(x) \in (x)$, existe $\alpha \in \mathbb{K}[x,y]$ tal que $\rho(x) = \alpha x$, mas todo polinômio invertível é uma constante não nula, logo $\alpha \in \mathbb{K}^*$. Escrevendo $\rho(y) = \sum_{j=0}^{n} g_j y^j$ em que $g_j \in \mathbb{K}[x]$ e usando o fato de que $\det J(\rho) \in \mathbb{K}^*$, temos que $g_1 = \beta$, para algum $\beta \in \mathbb{K}^*$ e $g_j = 0$ para $j = 2, \ldots, n$. Ou seja, $\rho(y) = g(x) + \beta y$, em que $g(x) = g_0(x)$. Usando a Proposição 4.2.2, temos que $g(0) \neq 0$, pois, do contrário, ρ fixaria o ideal maximal (x,y). Agora, seja $p = (c_1, c_2) \in \mathbb{K}^2$ e considere o ideal maximal $\mathfrak{m} = (x - c_1, y - c_2)$. Note que ρ fixa o ideal maximal $\mathfrak{m}$ se, e somente se,

$$\rho(x - c_1) = \alpha x - c_1 \quad \text{e} \quad \rho(y - c_2) = g(x) + \beta y - c_2$$

pertencem a $\mathfrak{m}$. No primeiro caso, temos que $\alpha = 1$ ou $c_1 = 0$. Se $\alpha \neq 1$, então $c_1 = 0$ e, supondo $\beta \neq 1$, temos que

$$\rho\left(y - \frac{g(0)}{(1-\beta)}\right) \equiv \beta\left(y - \frac{g(0)}{(1-\beta)}\right) \mod x,$$

isto é, ρ estabiliza o ideal

$$\left(x, y - \frac{g(0)}{(1-\beta)}\right),$$

o que contradiz 4.2.2. Portanto, segue-se de $\alpha \neq 1$ que $\beta = 1$. Por outro lado, se $c_1 \neq 0$, então $\alpha = 1$ e, portanto, $\rho(x - c_1) = x - c_1$. Novamente, se $\beta \neq 1$, então

$$\rho\left(y - \frac{g(c_1)}{(1-\beta)}\right) \equiv \beta\left(y - \frac{g(c_1)}{(1-\beta)}\right) \mod (x - c_1),$$

o que implica que o ideal maximal

$$\left(x - c_1, y - \frac{g(c_1)}{(1-\beta)}\right)$$

fica estável por ρ. Novamente, 4.2.2 nos diz que $\beta = 1$ completando a afirmação.

Afirmação 2: α é uma raiz da unidade.

Com efeito, do Teorema 2.1.6, existem $a, b \in \mathbb{K}[x, y]$ tais que $d = a\partial_x + b\partial_y$. Como $\rho(d(x)) = d(\rho(x))$, segue-se que $a(\alpha x, g(x) + y) = \alpha a(x, y)$. Escrevendo $a(x, y) = \sum_{i=0}^{m} a_i y^i$ com $a_i \in \mathbb{K}[x]$ para $i = 0, ..., m$, e $a_m \neq 0$, obtemos

$$\sum_{i=0}^{m} a_i(\alpha x)(g(x) + y)^i = \sum_{i=0}^{m} \alpha a_i(x) y^i \tag{4.4}$$

Em particular, temos que $a_m(\alpha x) = \alpha a_m(x)$, para todo $x \in \mathbb{K}$. Suponhamos que α não seja raiz da unidade e escrevamos $a_m(x) = e_0 + e_1 x + \cdots + e_l x^l$ com $e_l \neq 0$. Dessa forma,

$$a_m(\alpha x) - \alpha a_m(x) = e_0(1 - \alpha) + e_2(\alpha^2 - \alpha)x^2 + \cdots + e_l(\alpha^l - \alpha)x^l = 0,$$

implica que $a_m(x) = A_m x$, com $e_1 = A_m \in \mathbb{K}^*$. Agora, se $m > 0$, segue-se, de (4.4), que

$$a_{m-1}(\alpha x) + m a_m(\alpha x) g(x) = \alpha a_{m-1}(x), \tag{4.5}$$

$$a_{m-1}(\alpha x) + m\alpha A_m x g(x) = \alpha a_{m-1}(x). \tag{4.6}$$

Notemos que, de (4.6), temos que $a_{m-1}(0) = \alpha a_{m-1}(0)$ e, portanto, a_{m-1} não possui termo constante, pois α não é uma raiz da unidade. Ainda de (4.6), temos que $\mathrm{gr}(a_{m-1}) = \mathrm{gr}(g)+1$.

Façamos $a_{m-1}(x) = c_1 x + \cdots + c_{t+1} x^{t+1}$ e $g(x) = d_0 + d_1 x + \cdots + d_t x^t$. Substituindo em (4.6), obtemos

$$m\alpha A_m x g(x) = \alpha a_{m-1}(x) - a_{m-1}(\alpha x)$$

$$\sum_{k=0}^{t} m\alpha A_m d_k x^{k+1} = \sum_{k=2}^{t+1} c_k(\alpha - \alpha^k)x^k,$$

o que implica $m\alpha A_m d_0 = 0$. Dessa forma, se $m > 0$, temos que $d_0 = 0$ e, portanto, $g(0) = 0$, o que é um absurdo. Logo, podemos escrever $a(x, y) = A_0 x$ para algum $A_0 \in \mathbb{K}^*$. Neste caso, d fixaria o ideal (x), o que contradiz a simplicidade de d. Segue-se que α é uma raiz da unidade e isso completa a afirmação.

Como $\mathrm{Aut}(d)$ é um grupo podemos, sem perda de generalidade, substituir ρ por alguma de suas potências e denotar $\rho(x) = x$, $\rho(y) = g(x) + y$ com $g(0) \neq 0$. Note também que para alguma potência de ρ, temos

$$a_{m-1}(x) + m a_m(x) g(x) = a_{m-1}(x),$$

o que implica em $m = 0$. Logo, $a(x, y) = a_0(x)$.

Afirmação 3: $a_0(x) = a \in \mathbb{K}^*$.

Com efeito, se $a_0 = 0$, temos $d = b\partial_y$. Logo, $d(x) = 0 \in (x)$, o que não acontece, pois d é simples. Da mesma forma, se $\mathrm{gr}(a_0) \geq 1$, então

$$d(a_0(x)) = a\partial_x(a_0(x)) + b\partial_y(a_0(x)) = a_0(x)a_0'(x) \in (a(x)),$$

o que contradiz a simplicidade de d. Logo, $a_0 = a \in \mathbb{K}^*$. Isso prova a afirmação.

Definamos $b(x, y) = \sum_{j=0}^{n} b_j y^j$ em que $b_j \in \mathbb{K}[x]$ e $b_n \neq 0$.

Afirmação 4: $b(x, y) = b_0(x)$.

Como $\rho \in \mathrm{Aut}(d)$, então $\rho(d(y)) = d(\rho(y))$. Isto é,

$$\begin{aligned} b(x, g(x) + y) &= ag'(x) + b(x, y) \\ \sum_{j=0}^{n} b_j(x)(g(x) + y)^j &= ag'(x) + \sum_{j=0}^{n} b_j(x) y^j. \end{aligned} \tag{4.7}$$

Suponhamos $n > 1$. Igualando os coeficientes de grau $n - 1$ na variável y em (4.7), temos

$$\binom{n-1}{n-1} b_{n-1} + \binom{n}{n-1} b_n g = b_{n-1}$$

donde se segue que $b_n = 0$, pois $g \neq 0$. Logo, ainda de (4.7), $b(x, y) = b_0(x) + b_1(x)y$ com $ag'(x) = b_1(x)g(x)$. Mas, isso implica que

$$\mathrm{gr}(b_1) + \mathrm{gr}(g) = \mathrm{gr}(g) - 1.$$

Portanto, $b_1 = 0$ e $b(x, y) = b(x)$. Note que $b \neq 0$, pois d é simples.

Por fim, como d é simples e $a \in \mathbb{K}^*$, $(1/a)d = \partial_x + (1/a)b(x)\partial_y$ é simples. Porém, note que $f = \int b$ satisfaz $f' = 0f + b$, o que contradiz 3.2.2. Isso força ρ a ter ordem finita, o que completa a demonstração. □

Teorema 4.2.4. *Se uma derivação d é simples, então* $\mathrm{Aut}(d) = \{id\}$.

Demonstração. Suponhamos, por absurdo, que exista um automorfismo $\rho \in \mathrm{Aut}(d) \setminus \{id\}$. Pelo teorema 2.2.9, existe um ideal não trivial $\mathfrak{a}$ que fica estável por ρ e assim, do Lema 2.2.10, segue-se que existe $n \in \mathbb{N}$ tal que ρ^n estabiliza um primo minimal associado $\mathfrak{p}$ de $\mathfrak{a}$. Observe que o Lema 4.2.2 nos diz que $\mathfrak{p}$ não pode ser maximal.

Como $\mathrm{Aut}(d)$ é grupo, podemos fazer um abuso de notação e denotar ρ^n por ρ. Agora, como $\mathfrak{a}$ é não trivial e $\dim \mathbb{K}[x,y] = 2$, isso nos diz que $\mathfrak{p}$ necessariamente tem altura um. Logo, como $\mathbb{K}[x,y]$ é Noetheriano e domínio de fatoração única, segue-se que $\rho(h) = \mu h$ para algum polinômio irredutível $h \in \mathbb{K}[x,y]$ e $\mu \in \mathbb{K}^*$. Desde que $\mathbb{K}$ é algébricamente fechado, segue-se que h é geometricamente irredutível.

Notemos que a curva $h = 0$ não possui singularidades. De fato, suponha que $p \in \mathbb{K}^2$ é singularidade de h. Por Nullstellensatz, tal ponto corresponde a um ideal maximal $\mathfrak{m}$. Note que p é singularidade de h se, e somente se, $(h) \subset \mathfrak{m}^2$. Como ρ estabiliza o ideal (h), segue-se que

$$(h) \subset \rho(\mathfrak{m}^2) = \rho(\mathfrak{m})^2.$$

Isso acontece se, e somente se, o ponto correpondente ao ideal $\rho(\mathfrak{m})$ também é singularidade de h. Agindo por indução, temos que $\rho^k(\mathfrak{m})$ corresponde a um k-ésimo ponto singular de h. Pelo teorema de Bezout, segue-se que h possui finitos pontos singulares. Logo, existe algum k_0 tal que $\rho^{k_0}(\mathfrak{m}) = \mathfrak{m}$. Porém, novamente pelo Lema 4.2.2, isso não ocorre.

Agora do Teorema 2.2.12, existe um automorfismo $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x,y])$ tal que $\sigma(h) = 0$ nos dá três possibilidades de curvas em $\mathbb{K}[x,y]$. Observe que $ii)$ não ocorre, pois $\sigma(h)$ estabilizaria o ideal maximal (x,y). Dessa forma, ficamos com os casos $\sigma(h) = x$ ou $\sigma(h) = x^b y^a - \lambda$, em que $a, b \geq 1$ são inteiros coprimos e $\lambda \in \mathbb{K}^*$. Note que, a menos de uma constante, $\sigma\rho\sigma^{-1}(x) = x$ ou $\sigma\rho\sigma^{-1}(x^b y^a - \lambda) = x^b y^a - \lambda$. Além disso, d é simples se, e somente se, $\sigma d \sigma^{-1}$ é simples, de modo que podemos considerar $h(x,y) = x$ ou $h(x,y) = x^b y^a - \lambda$. Se fosse $h(x,y) = x$, então teríamos que ρ fixa o ideal gerado por x, o que contradiz o Lema 4.2.3. Logo, temos que $h(x,y) = x^b y^a - \lambda$ e, portanto, $\rho(x^b y^a - \lambda) = \mu(x^b y^a - \lambda)$. Denotando $\rho(x) = \sum_{i=0}^{n} f_i y^i$ e $\rho(y) = \sum_{j=0}^{m} g_j y^j$ com $f_i, g_j \in \mathbb{K}[x]$, em que $i = 0, \ldots, n$ e $j = 0, \ldots, m$, temos

$$\begin{aligned} \rho(x)^b \rho(y)^a - \lambda &= \mu x^b y^a - \mu\lambda \\ \left(\sum_{i=0}^{n} f_i y^i\right)^b \left(\sum_{j=0}^{m} g_j y^j\right)^a - \lambda &= \mu x^b y^a - \mu\lambda. \end{aligned} \tag{4.8}$$

Em particular, com respeito o termo de maior grau em y, temos

$$f_n^b g_m^a y^{bn+am} = \mu x^b y^a. \tag{4.9}$$

Dessa forma, temos necessariamente que $n = 0$ e $m = 1$, isto é, $\rho(x) = f_0(x)$ e $\rho(y) = g_0(x) + g_1(x)y$. Agora,

$$\det J(\rho) = \det \begin{pmatrix} f_0' & 0 \\ g_0' + g_1' y & g_1 \end{pmatrix} = f_0' g_1 \in \mathbb{K}^*. \tag{4.10}$$

Portanto,

$$\deg f_0' + \deg g_1 = 0,$$

donde se segue que $f_0(x) = \alpha x + c$ e $g_1 = \beta$ com $\alpha, \beta \in \mathbb{K}^*$ e $c \in \mathbb{K}$. Ainda de (4.9), temos que $c = 0$ e podemos escrever $\rho(x) = \alpha x$ e $\rho(y) = g_0 + \beta y$, para $\alpha, \beta \in \mathbb{K}^*$. Por fim, de (4.8), segue-se que

$$(\alpha x)^b (g_0 + \beta y)^a = \mu x^b y^a + \lambda(1 - \mu),$$

o que implica $g_0 = 0$. Portanto, ρ fixa o ideal maximal (x, y), o que é um absurdo completando a demonstração. □

5 Isotropia da derivação de Shamsuddin e automorfismos

O Teorema 4.2.4 nos ajuda entender a simplicidade de uma derivação através do cálculo de sua isotropia. Isto é, se $\mathrm{Aut}(d)$ não é um grupo trivial, então d não é simples.

5.1 Uma caracterização das derivações de Shamsuddin

Sejam a derivação de Shamsuddin $d = \partial_x + (ay + b)\partial_y$ com $a, b \in \mathbb{K}[x]$, $a \neq 0$ e $\rho \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x, y])$ com $\rho(x) = f$ e $\rho(y) = g$. Observemos que $\rho \in \mathrm{Aut}(d)$ se, e somente se, $\rho d \rho^{-1} = d$, o que equivale ao sistema

$$\begin{cases} \partial_x(f) + (ay + b)\partial_y(f) = 1, \\ \partial_x(g) + (ay + b)\partial_y(g) = \rho(a)g + \rho(b). \end{cases} \tag{5.1}$$

Neste caso, se $f(x, y) = \sum_{i=0}^{n} f_i y^i$ e $g(x, y) = \sum_{j=0}^{m} g_j y^j$ com $f_i, g_j \in \mathbb{K}[x]$ em que $i \in \{0, \ldots, n\}$ e $j \in \{0, \ldots, m\}$, o sistema acima pode ser reescrito como

$$\begin{cases} f_0' + bf_1 + \sum_{i=1}^{n-1}(f_i' + iaf_i + (i+1)bf_{i+1})y^i + (f_n' + naf_n)y^n = 1, \\ g_0' + bg_1 + \sum_{j=1}^{m-1}(g_j' + jag_j + (j+1)bg_{j+1})y^j + (g_m' + mag_m)y^m = \rho(a)g + \rho(b). \end{cases} \tag{5.2}$$

Analisando o sistema (5.2), temos que $n > 0$ contradiz a equação $f_n' + naf_n = 0$, donde se segue que $f_i = 0$ para $i = 1, \ldots, n$. Então, devemos ter $f_0'(x) = 1$ e, portanto, $f(x, y) = x + c$. Além disso, como $\det J(\rho) \in \mathbb{K}^*$, temos que, $g_j = 0$, para $j = 2, \ldots, m$ e $g_1 = \beta \in \mathbb{K}^*$. Portanto, isso nos diz que $f(x, y) = x + c$ e $g(x, y) = g_0(x) + \beta y$ para $c \in \mathbb{K}$ e $\beta \in \mathbb{K}^*$.

A próxima proposição nos dá uma lista da estrutura de $\mathrm{Aut}(d)$ para alguns casos específicos da derivação de Shamsuddin.

Proposição 5.1.1. *Seja $d = \partial_x + (ay + b)\partial_y$ uma derivação de Shamsuddin com $a \neq 0$. Temos:*

(i) Se $a \in \mathbb{K}^*$ e $b = 0$, então $\mathrm{Aut}(d) = \mathbb{K} \times \mathbb{K}^*$.

(ii) Se $a, b \in \mathbb{K}^*$, então $\mathrm{Aut}(d) = \mathbb{K} \times (\mathbb{K} \ltimes \mathbb{K}^*)$

(iii) Se $\mathrm{gr}(a) \geq 1$, então

$$\mathrm{Aut}(d) = \{\rho,\ \rho(x) = x,\ \rho(y) = g_0 + \beta y,\ g_0' = ag_0 + b(1 - \beta),\ \beta \in \mathbb{K}^*\}.$$

Em particular, se $\mathrm{gr}(a) \geq 1$ e $b = 0$, então $\mathrm{Aut}(d) = \mathbb{K}^*$.

Demonstração. (i) Se $a \in \mathbb{K}^*$ e $b = 0$, segue-se da segunda igualdade de (5.2) que

$$g_0' = \rho(a)g_0 = ag_0,$$

o que implica $g_0 = 0$. Portanto,

$$\mathrm{Aut}(d) = \{\rho \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}[x,y]);\ \rho(x) = x + c,\ \rho(y) = \beta y,\ c \in \mathbb{K} \text{ e } \beta \in \mathbb{K}^*\}.$$

Por fim, note que a aplicação

$$\begin{aligned} \psi : \mathrm{Aut}(d) &\to \mathbb{K} \times \mathbb{K}^* \\ (\rho(x), \rho(y)) &\mapsto (c, \beta) \end{aligned}$$

é um isomorfismo.

(ii) Sejam $a, b \in \mathbb{K}^*$ e $\rho_1, \rho_2 \in \mathrm{Aut}(d)$. Pelo comentário acima, $\rho_i(x) = x + c_i$ e $\rho_i(y) = g_i(x) + \beta_i y$ para cada $i = 1, 2$. Afirmamos que $g_i \in \mathbb{K}$ para cada i. Vamos analisar o caso $i = 1$, pois o caso $i = 2$ é obviamente análogo. Por hipótese, $d(\rho_1(y)) = \rho_1(d(y))$, isto é,

$$d(g_1(x) + \beta_1 y) = \rho_1(ay + b),$$

donde

$$g_1'(x) + (ay + b)\beta_1 = a(g_1(x) + \beta_1 y) + b.$$

Simplificando

$$g_1'(x) + b\beta_1 = ag_1(x) + b. \tag{5.3}$$

Explicitando $g_1(x) = \sum_{j=0}^{n} c_j x^j$, concluímos, de (5.3), que $c_j = 0$ para $j = 1, \ldots, n$ e $c_0 = b(\beta_1 - 1)/a \in \mathbb{K}$, como queríamos. Denotando $g_i = \alpha_i$, temos,

$$\rho_2\rho_1(x) = x + c_1 + c_2 \quad \text{e} \quad \rho_2\rho_1(y) = \alpha_2 + \beta_2\alpha_1 + \beta_1\beta_2 y.$$

Logo, podemos considerar o homomorfismo sobrejetivo

$$\begin{aligned} \psi : \mathrm{Aut}(d) &\to \mathbb{K} \times (\mathbb{K} \ltimes \mathbb{K}^*) \\ (\rho(x), \rho(y)) &\to (c_1 + c_2, (\alpha_2 + \beta_2\alpha_1, \beta_1\beta_2)). \end{aligned}$$

Isso prova ii).

iii) A segunda equação do sistema (5.2) fornece

$$\begin{cases} \beta a(x) = \beta a(x + c) & (5.4) \\ g_0' + \beta b(x) = a(x + c)g_0 + b(x + c). & (5.5) \end{cases}$$

Como $\mathrm{gr}(a) \geq 1$, segue-se, de (5.4), que $c = 0$. Portanto, de (5.5) e o comentário feito após (5.2), temos que

$$\mathrm{Aut}(d) = \{\rho,\ \rho(x) = x,\ \rho(y) = g_0 + \beta y,\ g_0' = ag_0 + b(1 - \beta),\ \beta \in \mathbb{K}^*\}.$$

□

Observe que se $\mathrm{gr}(a) = 0$, então não podemos inferir nada sobre a constante c, de modo que a isotropia da derivação $d = \partial_x + (ay + b)\partial_y$ toma a forma

$$\mathrm{Aut}(d) = \{\rho,\ \rho(x) = x + c,\ \rho(y) = g_0 + \beta y,\ g_0' - ag_0 = b(x + c) - \beta b,\ \beta \in \mathbb{K}^*, c \in \mathbb{K}\}.$$

Nesse caso, se $\rho_1, \rho_2 \in \mathrm{Aut}(d)$ com $\rho_i(x) = x + c_1$ e $\rho_i(y) = g_0 + \beta_i y$, para $i = 1, 2$ então

$$\rho_1\rho_2(x) = x + c_1 + c_2 \quad \rho_1\rho_2(y) = P_{c_1,\beta_2}(x) + \beta_2\beta_1 y,$$

em que $P_{c_1,\beta_2}(x) = g_0(x + c_1) + \beta_2 g_0(x)$. Definimos então o isomorfismo

$$\begin{gathered}\psi : \mathbb{K} \times \mathbb{K}^* \to \mathrm{Aut}(d)\\ (c, \beta) \to (x + c, g_0 + \beta y)\\ (0, 1) \to (x, y).\end{gathered}$$

Proposição 5.1.2. *Seja d uma derivação de Shamsuddin com $a \neq 0$. Se $\mathrm{gr}(a) \geq 1$, então $\mathrm{Aut}(d) \neq \{id\}$ se, e somente se, existe $h(x) \in \mathbb{K}[x]$ tal que $d(h) = ah + b$. Em particular, se $b \neq 0$, então $\mathrm{gr}(b) \geq \mathrm{gr}(a)$.*

Demonstração. ($\Rightarrow$) Seja $\rho \in \mathrm{Aut}(d)$ tal que $\rho \neq id$. Como $\mathrm{gr}(a) \geq 1$, da Proposição 5.1.1 item (iii), temos que existe um polinômio $g_0 \in \mathbb{K}[x]$ e $\beta \in \mathbb{K}^*$ com $\rho(x) = x$ e $\rho(y) = g_0 + \beta y$ em que $g_0' = ag_0 + b(1 - \beta)$. Em segundo lugar, observe que $\beta \neq 1$. De fato, se $\beta = 1$, então teríamos $g_0' = ag_0$, o que implica $g_0 = 0$. Mas, dessa forma, teríamos $\rho = id$, o que não acontece. Tomemos $h = \dfrac{g_0}{1 - \beta}$ e notemos que

$$h' = \frac{g_0'}{1 - \beta} = \frac{ag_0 + b(1 - \beta)}{1 - \beta} = ah + b,$$

isto é, $d(h) = ah + b$.

($\Leftarrow$) Suponhamos agora que exista $h \in \mathbb{K}[x]$ tal que $d(h) = ah + b$. Se $h = 0$, então $b = 0$ e, portanto, da Proposição 5.1.1, temos que $\mathrm{Aut}(d) = \mathbb{K}^*$. Se h é diferente de zero, definamos a familia a 1-parâmetro de automorfismos $\rho_\beta(x) = x$ e $\rho_\beta(y) = (1 - \beta)h + \beta y$ para $\beta \in \mathbb{K}^*$. Note que $\rho_\beta \in \mathrm{Aut}(d)$ para todo $\beta \in \mathbb{K}^*$. Observe que se $b \neq 0$, então

$$\mathrm{gr}(a) \leq \mathrm{gr}(a) + \mathrm{gr}(h) = \mathrm{gr}(b).$$

□

Em [Bal16], R. Baltazar já havia demonstrado que uma derivação simples de Shamsuddin necessariamente tem grupo de isotropia trivial. O próximo teorema fornece uma recíproca desse resultado através do Teorema 4.2.4. Dessa forma, temos uma caracterização dessas derivações via $\mathrm{Aut}(d)$.

Teorema 5.1.3. *Seja d uma derivação de Shamsuddin com $a \neq 0$. Então d é simples se, e somente se,* $\mathrm{Aut}(d) = \{id\}$.

Demonstração. ($\Rightarrow$) Segue-se direto do Teorema 4.2.4.

($\Leftarrow$) Suponhamos que $\mathrm{Aut}(d) = \{id\}$ e que d não seja simples. Então, por 3.2.2, existe $f \in \mathbb{K}[x]$ tal que $\partial_x(f) = af + b$. Isto é $d(f) = af + b$. Agora, se $\mathrm{gr}(a) = 0$, então, do comentário feito após a Proposição 5.1.1, segue-se que $\mathrm{Aut}(d) \neq \{id\}$, o que é um absurdo. Logo, devemos ter $\mathrm{gr}(a) \geq 1$. Da proposição 5.1.2, temos, novamente, que $\mathrm{Aut}(d) \neq \{id\}$, o que mostra que d é simples. □

5.2 O cálculo de alguns grupos de isotropia

Nesta seção apresentaremos explicitamente o grupo de isotropia de algumas derivações e, em vista do teorema 4.2.4, analisaremos sua simplicidade em cada caso. Ao longo da seção usaremos $\rho(x) = f = \sum_{i=0}^{n} f_i y^i$ e $\rho(y) = g = \sum_{j=0}^{m} g_j y^j$.

Exemplo 5.2.1. Consideremos a seguinte derivação de Shamsuddin $d = \partial_x + (2xy + x^3)\partial_y$. Observe que $a = 2x$ e $b = x^3$ e portanto, $\mathrm{gr}(a) \geq 1$. Pela Proposição 5.1.1 item *iii*),

$$\mathrm{Aut}(d) = \{\rho,\ \rho(x) = x,\ \rho(y) = g_0 + dy;\ g_0' = ag_0 + b(1-\beta),\ \beta \in \mathbb{K}^*\}.$$

Vamos determinar explicitamente os automorfismos desse grupo. Observemos que $\mathrm{gr}(g_0) \leq \mathrm{gr}(b) - \mathrm{gr}(a) = 3 - 1 = 2$ e, portanto, $g_0 = c_2x^2 + c_1x + c_0$ com $c_i \in \mathbb{K}$ e $i = 0, \ldots, 2$. Logo, $g_0' - ag_0 = b(1-\beta)$ nos dá

$$(2c_2x + c_1) - 2x(c_2x^2 + c_1x + c_0) = x^3(1-\beta),$$

isto é,

$$-2c_2x^3 - 2c_1x^2 + 2(c_2 - c_0) + c_1 = x^3(1-\beta)$$

Assim,

$$c_0 = c_2 = \frac{(\beta - 1)}{2} \text{ e } c_1 = 0.$$

Dessa forma, para todo automorfismo $\rho \in \mathrm{Aut}(d)$,

$$\rho(x) = x \text{ e } \rho(y) = \frac{(\beta-1)}{2}(x^2+1) + \beta y.$$

Fazendo $\beta \in \mathbb{K}^*$ variar, temos uma família a 1-parâmetro de automorfismos. Observe que, em vista do Teorema 4.2.4, d não é simples. De fato, o ideal $(2y + x^2 + 1)$ é d-estável.

Exemplo 5.2.2. Seja a derivação homogênea $d = x\partial_x + y\partial_y$. Se $\rho \in \mathrm{Aut}(d)$, então

$$\begin{cases} x\partial_x f + y\partial_y f = f & (5.6) \\ x\partial_x g + y\partial_y g = g & (5.7) \end{cases}$$

De (5.6), temos o seguinte sistema

$$\begin{cases} xf_n' + (n-1)f_n = 0 \\ \quad\vdots \\ xf_2' + f_2 = 0 \\ xf_1' = 0 \\ xf_0' = f_0 \end{cases}$$

Logo, $f_i = 0$ para $i = 2, \ldots, n$, $f_1 = \beta \in \mathbb{K}$ e $f_0 = \alpha x$ com $\alpha \in \mathbb{K}$, isto é, $\rho(x) = \alpha x + \beta y$. O sistema presente em (5.7) é análogo ao dado acima, de modo que $\rho(y) = \sigma x + \gamma y$ com $\sigma, \gamma \in \mathbb{K}$. Assim,

$$\mathrm{Aut}(d) = \{\rho, \rho(x) = \alpha x + \beta y, \rho(y) = \sigma x + \gamma y; \alpha, \beta, \sigma, \gamma \in \mathbb{K}\}.$$

Por fim, como $\det J(\rho) = \alpha\gamma - \beta\sigma$ é não-nulo, segue-se que $\mathrm{Aut}(d) = \mathrm{GL}_2(\mathbb{K})$.

Exemplo 5.2.3. Consideremos $a = x^2$ e $b = x^5 + x^4 + x^3 + x^2 - 2x + \varepsilon$ em que $\varepsilon \in \mathbb{R}$. Pelo item *iii)* da Proposição 5.1.1, se $\rho \in \mathrm{Aut}(d)$, então $\rho(x) = x$, $\rho(y) = g_0 + \beta y$ com $\beta \in \mathbb{K}^*$ e $g_0' = ag_0 + b(1-\beta)$. Note que $\deg g_0 \leq \deg b - \deg a = 5 - 2 = 3$ e assim, $g_0(x) = c_3x^3 + c_2x^2 + c_2x^2 + c_1x + c_0$ para $c_i \in \mathbb{K}$ com $i = 0, \ldots, 3$. Substituindo a e b em $g_0' = ag_0 + b(1-\beta)$, concluímos que essa equação possui solução com $\beta \neq 1$, se, e somente se, $\varepsilon = -1$; de modo que $c_3 = c_2 = c_1 = e$ e $c_0 = 4e$ em que $e = \beta - 1$ e $\beta \in \mathbb{K} \setminus \{1\}$. Assim,

$$\rho(x) = x \text{ e } \rho(y) = ex^3 + ex^2 + ex - 4e + \beta y. \tag{5.8}$$

Denotemos por d_ε a derivação de Shamsuddin associada a a, b e ε. Note que (5.8) mostra que $\mathrm{Aut}(d_{-1}) \neq \{id\}$. Por outro lado, se $\varepsilon \neq 1$, então $\beta = 1$ e, portanto, a única solução da equação

$$g_0' = ag_0 + b(1-\beta)$$

é a trivial. Nesse caso, $\mathrm{Aut}(d_\varepsilon) = \{id\}$. Em vista do Teorema 5.1.3, segue-se que d_{-1} não é simples e d_ε é simples para qualquer que seja $\varepsilon \in \mathbb{R} \setminus \{1\}$.

Exemplo 5.2.4. Seja $d = \partial_x + (y^2 - p(x))\partial_y$ para $p(x) \in \mathbb{K}[x] \setminus \mathbb{K}$. Se $\rho \in \mathrm{Aut}(d)$, então

$$\begin{cases} nf_ny^{n+1} + \sum_{k=0}^{n}(f_k' + (k-1)f_{k-1} - (k+1)p(x)f_{k+1})y^k = 1, & (5.9) \\ mg_my^{m+1} + \sum_{l=0}^{m}(g_l' + (l-1)g_{l-1} - (l+1)p(x)g_{l+1})y^l = g^2 - \rho(p(x)), & (5.10) \end{cases}$$

em que $f_k = g_l = 0$ sempre que $l, k < 0$ e $l > m$ e $k > n$. De (5.9), segue-se que $f(x, y) = x + c$ com $c \in \mathbb{K}$. Agora, se $m > 1$, então $m + 1 < 2m$, o que contradiz a equação

$0 = g_m^2$ presente em (5.10). Logo, podemos escrever $g = g_0 + g_1 y$ e, portanto, (5.10) dá origem ao sistema

$$\begin{cases} g_1 = g_1^2 & (5.11) \\ g_1' = 2g_0 g_1 & (5.12) \\ g_0' - p(x)g_1 = g_0^2 - \rho(p(x)). & (5.13) \end{cases}$$

De (5.11), temos que $g_1 = 0$ ou $g_1 = 1$. O primeiro caso contradiz o fato de que $\det J(\rho) \in \mathbb{K}^*$. Agora, se $g_1 = 1$, então, de (5.12), segue-se que $g_0 = 0$ e, de (5.13), obtemos a condição

$$p(x) = \rho(p(x)) = p(x + c).$$

Como $\mathrm{gr}(p) \geq 1$, temos que $c = 0$. Portanto, $\mathrm{Aut}(d) = \{id\}$.

Em vista do Exemplo 5.2.4, tomando $p(x) = x^{2m} - mx^{m-1}$ para $m \in \mathbb{N}^*$, segue-se que $\mathrm{Aut}(d)$ é trivial. Porém, por [MMN01, p.5106], a derivação $d = \partial_x + (y^2 - x^{2m} + mx^{m-1})\partial_y$ com $m \in \mathbb{N}^*$, não é simples.

Esse último exemplo nos mostra duas coisas. A primeira delas é que não vale a recíproca do Teorema 4.2.4, pois a simplicidade da derivação $d = \partial_x + (y^2 - p(x))\partial_y$ está associada ao polinômio $p(x) \in \mathbb{K}[x]$.

A segunda coisa, e que decorre da primeira, é que a estratégia de estudar uma derivação através de seu grupo de isotropia nem sempre é efetiva, pois, como no exemplo 5.2.4, os automorfismos parecem não captar as sutilezas do polinômio $p(x)$.

Bibliografia

[Abh06] S. S. Abhyankar. *Lectures on algebra*. Vol. 1. World Scientific, 2006.

[Bal14] R Baltazar. "Sobre soluções de derivações em k-algebras Noetherianas e simplicidade". Tese de dout. Tese de doutorado, Universidade Federal do Rio Grande do Sul, 2014.

[Bal16] R. Baltazar. "On simple Shamsuddin derivations in two variables". Em: *Anais da Academia Brasileira de Ciências* 88.4 (2016), pp. 2031–2038.

[BFL14] C. Bisi, J.-P. Furter e S. Lamy. "The tame automorphism group of an affine quadric threefold acting on a square complex". Em: *Journal de l'École polytechnique-Mathématiques* 1 (2014), pp. 161–223.

[Bia62] M. Bialynicki-Birula A. e Rosenlicht. "Injective morphisms of real algebraic varieties". Em: *Proceedings of the American Mathematical Society* 13.2 (1962), pp. 200–203.

[BL20] L. N. Bertoncello e D. Levcovitz. "On the isotropy group of a simple derivation". Em: *Journal of Pure and Applied Algebra* 224.1 (2020), pp. 33–41.

[BNS12] V. G. Bardakov, M. V. Neshchadim e Yu. V. Sosnovsky. "Groups of triangular automorphisms of a free associative algebra and a polynomial algebra". Em: *Journal of Algebra* 362 (2012), pp. 201–220.

[Bou59] N. Bourbaki. *Eléments de mathématique: Livre II: Algèbre. XI*. Hermann, 1959.

[BP15] R. Baltazar e I. Pan. "On solutions for derivations of a Noetherian k-algebra and local simplicity". Em: *Communications in Algebra* 43.7 (2015), pp. 2739–2747.

[BS13] J. Blanc e I. Stampfli. "Automorphisms of the plane preserving a curve". Em: *arXiv preprint arXiv:1304.2549* (2013).

[FM09] V. M. Futorny e L. S. I. Murakami. "Polinômios e seus automorfismos". Em: *Matemática Universitária* 44 (2009), pp. 60–69.

[Fre06] G. Freudenburg. *Algebraic theory of locally nilpotent derivations*. Vol. 136. Springer, 2006.

[GW04] Kenneth R Goodearl e Robert Breckenridge Warfield Jr. *An introduction to noncommutative Noetherian rings*. Vol. 61. Cambridge university press, 2004.

[KS95] H. Kraft e G. Schwarz. "Finite automorphisms of affine n-space". Em: *Automorphisms of affine spaces*. Springer, 1995, pp. 55–66.

[Lan75] D.R. Lane. "Fixed points of affine Cremona transformations of the plane over an algebraically closed field". Em: *American Journal of Mathematics* 97.3 (1975), pp. 707–732.

[Leq08] Yves Lequain. "Simple Shamsuddin derivations of $K[x_1, \ldots, y_n]$: An algorithmic characterization". Em: *Journal of Pure and Applied Algebra* 212.4 (2008), pp. 801–807.

[Men17] Mendes, L. e Pan, I. "On plane polynomial automorphisms commuting with simple derivations". Em: *Journal of Pure and Applied Algebra* 221.4 (2017), pp. 875–882.

[MMN01] A. Maciejewski, J. Moulin-Ollagnier e A. Nowicki. "Simple quadratic derivations in two variables". Em: (2001).

[Nag72] M. Nagata. *On automorphism group of $k[x, y]$*. Kinokuniya, 1972.

[Now94] Nowicki, A. *Polynomial derivations and their rings of constants*. N. Copernicus University Press: Torun, 1994.

[PB19] I. Pan e R Baltazar. "On the Automorphism Group of a Polynomial Differential Ring in Two Variables". Em: *arXiv preprint arXiv:1910.05278* (2019).

[Rei95] M. Reid. *Undergraduate commutative algebra*. Vol. 29. Cambridge University Press, 1995.

[Sei67] A Seidenberg. "Differential ideals in rings of finitely generated type". Em: *American Journal of Mathematics* 89.1 (1967), pp. 22–42.

[Sha77] A. Shamsuddin. "Automorphisms and skew polynomial rings". Tese de dout. University of Leeds, 1977.

[SU04] I. Shestakov e U. Umirbaev. "The tame and the wild automorphisms of polynomial rings in three variables". Em: *Journal of the American Mathematical Society* 17.1 (2004), pp. 197–227.

[Van12] A. Van den Essen. *Polynomial Automorphisms: and the Jacobian Conjecture*. Vol. 190. Birkhäuser, 2012.

[Wri13] D. Wright. "The amalgamated product structure of the tame automorphism group in dimension three". Em: *arXiv preprint arXiv:1310.8325* (2013).

[ZS75] O. Zariski e P. Samuel. "Commutative Algebra. Vol. 1. With the cooperation of IS Cohen. Corrected reprinting of the 1958 edition". Em: *Graduate Texts in Mathematics* 28 (1975), p. 29.