Sobre a simplicidade de derivações em anéis finitamente gerados

Este exemplar corresponde à redação final da dissertação/tese devidamente corrigida e defendida por Guilherme Chaud Tizziotti e aprovada pela comissão julgadora.

Campinas, 10 de março de 2004 .

Prof. Dr. : Paulo Roberto Brumatti
Orientador

Banca Examinadora
1- Prof. Dr. Paulo Roberto Brumatti
2- Prof. Dr. Fernando Eduardo Torres Orihuela
3- Profª. Drª. Aparecida Francisco da Silva

Dissertação/tese apresentada ao instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de MESTRE em Matemática.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Tizziotti, Guilherme Chaud

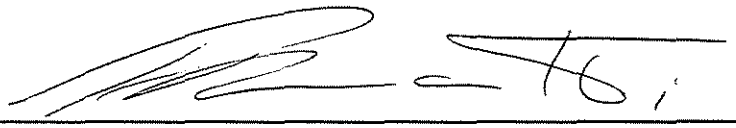
T546s Sobre a simplicidade de derivações em anéis finitamente gerados/Guilherme Chaud Tizziotti -- Campinas, [S.P. :s.n.], 2004.

Orientador : Paulo Roberto Brumatti.

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

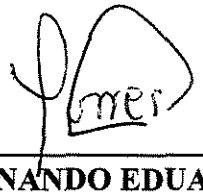
1. Álgebra comutativa. 2. Álgebra diferencial. 3. Anéis polinomiais. I. Brumatti, Paulo Roberto. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Dissertação de Mestrado defendida em 10 de março de 2004 e aprovada pela Banca Examinadora composta pelos Profs. Drs.



Prof (a). Dr (a). PAULO ROBERTO BRUMATTI

Prof (a). Dr (a). APARECIDA FRANCISCO DA SILVA



Prof (a). Dr (a). FERNANDO EDUARDO TORRES ORIHUELA

Agradecimentos

Agradeço :

primeiramente ao professor Paulo Roberto Brumatti, meu orientador, por tudo que ele fez por mim com muita dedicação e sempre tendo muita paciência. Muito obrigado por tudo professor Paulo.

aos meus pais por terem me dado muita motivação, oportunidade e exemplo para eu poder estudar e realizar este trabalho.

aos meus irmãos e avós que sempre estiveram do meu lado.

à minha família, tios, tias, primos e primas que torceram para mim.

a todos os meus professores que também foram fundamentais para a realização deste trabalho.

aos meu amigos, tanto os de Campinas como os "véi de guerra" de Guará, em especial ao Diego, que além de um grande companheiro, sempre me motivou.

à CAPES pela concessão da bolsa.

e principalmente a Deus que sempre me iluminou e colocou estas grandes pessoas em minha vida.

E obrigado à todos que de certa forma me ajudaram neste trabalho.

Resumo

O principal objeto de estudos nesta dissertação é uma k-álgebra comutativa e finitamente gerada A , com k sendo um corpo de característica zero. Utilizando conceitos básicos e fundamentais de álgebra comutativa apresentamos, no capítulo 2, um estudo de A através de seu módulo de k-derivações. Na verdade tal estudo trata da regularidade de A em termos do fato de A ser $\mathcal{D}$-simples, para algum subconjunto, $\mathcal{D}$, do módulo de k-derivações de A.

Para completar tal estudo, no capítulo 3, apresentamos exemplos clássicos de k-derivações d que tornam simples o anel de polinômios em um número finito de variáveis sobre k.

Abstract

The focus of this dissertation is a commutative k-algebra finitely generated A, with k being a field of zero characteristic. Using basic and fundamental concepts of commutative algebra we show, in chapter 2, a study of A through its k-derivation module. Actually, this study is about the A regularity within limits of the fact of A to be D-simple for some subset, D, of the k-derivation module of A.

To complete this study, in the chapter 3, we present classic examples of k-derivations d that make simple the polynomial ring with a finite number of variables over k.

Sumário

Introdução

Em 1965 A. Seindenbeg mostrou , em [13] , que se k é um corpo de característica zero, $A = k[x_1,\ldots,x_n]$ é uma k-álgebra finitamente gerada e $\mathcal{D}$ é sua família de k-derivações então : A é regular se, e somente se, A é $\mathcal{D}$-simples, ou seja, os únicos ideais I de A que satisfazem $d(I) \subseteq I$ para qualquer derivação $d \in \mathcal{D}$ são os triviais. Anos mais tarde, em 1974, R. Hart mostrou em [4] que quando $k[x_1,\ldots,x_n]$ é $\mathcal{D}$-simples , não necessariamente existe uma derivação $d \in \mathcal{D}$ tal que $k[x_1,\ldots,x_n]$ seja d-simples, ou seja pode não existir uma derivação d tal que $d(P) \not\subseteq P$, para todo ideal primo P de $k[x_1,\ldots,x_n]$. Agora se M é um ideal maximal de $k[x_1,\ldots,x_n]$, para o anel local $k[x_1,\ldots,x_n]_M$ temos uma melhor situação, pois Hart também, no mesmo artigo, mostrou que se $k[x_1,\ldots,x_n]_M$ é regular, então sempre existirá uma k-derivação d de $k[x_1,\ldots,x_n]_M$ tal que $k[x_1,\ldots,x_n]_M$ será d-simples. A partir destes resultados vemos que o fato de existir uma k-derivação d de $k[x_1,\ldots,x_n]_M$ que torna $k[x_1,\ldots,x_n]_M$ d-simples é uma caracterização da propriedade geométrica do anel $k[x_1,\ldots,x_n]_M$ ser regular.

No capítulo 2 vamos apresentar uma descrição completa das provas dos importantes resultados de A. Seindenberg e R. Hart. Nesta descrição aparecerão os conceitos de derivações, d-ideal e resultados ligados a eles, tais como o fundamental lema de Zariski.

Encontrar derivações d que tornam tais k-álgebras A d-simples não é, geralmente, muito simples mesmo quando A é o anel de polinômios. Os primeiros exemplos gerais de tais derivações foram dados em 1977 por A. Shamsuddin , sendo estas derivações de grau um. Mais recentemente , em 2001 , A. Maciejewski , J. Moulin-Ollagnier e A. Nowicki, em [12], apresentaram exemplos de k-derivações d de uma anel de polinômios A tais que d tem grau 2 e A é d-simples. Aqui vale a pena citarmos, para ressaltar a atualidade do tema, que os exemplos citados acima têm tido fundamental importância para se exibir exemplos de ideais maximais à esquerda da álgebra de Weyl $A_n(k)$ e tais ideais geram importantes exemplos na teoria dos módulos irredutíveis da álgebra de Weyl $A_n(k)$, veja por exemplo [2] , [7] , [8] e [14]. O capítulo 3 será dedicado para apresentar os exemplos de Shamsuddin e os resultados e derivações obtidos por A. Maciejewski , J. Moulin-Ollagnier e A. Nowicki.

Encerramos a introdução dizendo que, para familiarizar o leitor com a linguagem que será utilizada na dissertação, no capítulo 1 faremos uma breve apresentação de definições e resultados gerais, na maioria da vezes sem prova, da álgebra comutativa.

Capítulo 1
Notações e Preliminares

Neste capítulo introduziremos conceitos e resultados de álgebra comutativa que serão utilizados nos capítulos seguintes e que serão supostos conhecidos nestes. Observamos que as demonstrações destes resultados clássicos não serão feitas aqui mas poderão ser encontradas nas referências [3], [5], [6] e [13].

Devemos ressaltar que este primeiro capítulo tem a intenção de familiarizar o leitor com as notações e definições que aparecerão nos capítulos seguintes.

Observamos que trabalharemos aqui e no restante desta dissertação sempre com anel comutativo noetheriano com identidade diferente do zero , e com corpos de característica zero.

1.1 Teoria de Corpos

Iniciaremos enunciando alguns resultados e definições de teoria de corpos que nos servirão de base para os primeiros resultados de derivação que serão apresentados neste mesmo capítulo.

Começaremos com a seguinte definição.

Definição 1.1.1 : *Dado um corpo k , dizemos que um corpo L é uma extensão de k , se $k \subseteq L$ e k é subcorpo de L .*

Notação : Denotaremos por L/k quando L for uma extensão de k.

Levando-se em conta que para uma extensão de corpos L/k , tem-se que L é um k-espaço vetorial definimos :

Definição 1.1.2 : *Seja L/k uma extensão de corpos. Definiremos o grau de L/k como sendo a dimensão de L como k-espaço vetorial. O grau de uma extensão será denotado por $[L : k]$, isto é , $[L : k] = \dim_k L$. Quando L não tem base finita escrevemos apenas $[L : k] = \infty$.*

Como em todo este texto vamos nos referir a corpos de característica zero , vale apena lembrar a definição deste conceito .

Definição 1.1.3 : *Dizemos que um corpo k é de característica zero se k contém uma cópia de $\mathbb{Q}$ como subcorpo.*

No capítulo 2 , mais precisamente nos teoremas 2.1.12 e 2.1.13 , vamos nos deparar com o conceito de extensão algébrica, para sabermos o que de fato é uma extensão deste tipo precisaremos antes da seguinte definição.

Definição 1.1.4 : *Sejam L/k uma extensão de corpos e $\alpha \in L$. Dizemos que α é algébrico sobre k se existe $f \in k[X]\backslash\{0\}$ tal que $f(\alpha) = 0$. Caso contrário dizemos que α é transcendente sobre k.*

Agora sim podemos enunciar o conceito que desejávamos.

Definição 1.1.5 : *Uma extensão de corpos L/k é dita algébrica se todo $\alpha \in L$ é algébrico sobre k.*

O resultado a seguir é um teorema clássico com respeito a extensão algébrica .

Teorema 1.1.6 : *Seja L/k uma extensão de corpos tal que $[L : k] = m < \infty$. Então L/k é uma extensão álgébrica.*

Demostração : Ver S. Lang ([6] , cap.VII , proposição 1.1)

Também no capítulo 2 encontraremos na proposição 2.1.5 os conceitos de conjunto algebricamente independente e extensão puramente transcendental. Vejamos então estas definições :

Definição 1.1.7 : *Sejam L/k uma extensão de corpos e $B = k[X_1,\ldots,X_n]$ o anel de polinômios a n variáveis sobre k . Dados $y_1,\ldots,y_n \in L$, dizemos que $y_1,\ldots,y_n$ são algebricamente independentes sobre k se dado $f \in B$ temos que:*
$f(y_1,\ldots,y_n) = 0$ se, e somente se, $f(X_1,\ldots,X_n) = 0$, ou seja , se $V \subset \mathbb{N}^r$ é um conjunto finito então $\sum_{v=(v_1,\ldots,v_r)\in V} a_v.y_1^{v_1}\ldots y_r^{v_r} = 0$, $a_v \in k$ se, e somente se, $a_v = 0$, para todo $v \in V$.

Definição 1.1.8 : *Se $L = k(y_1,\ldots,y_n)$, com $\{y_1,\ldots,y_n\}$ algebricamente independentes sobre k , então dizemos que a extensão L/k é puramente transcendental.*

Para encerrarmos esta seção vamos descrever alguns conceitos que utilizaremos no capítulo 3 na demonstração de um resultado apresentado por A. Maciejewski , J. Moulin-Ollagnier e A. Nowicki em [12] . As demonstrações destes resultados podem ser vistas em [6].

Definição 1.1.9 : *Sejam L/k , F/k extensões de corpos e $\varphi : L \to F$ uma aplicação. Dizemos que φ é um k-isomorfismo de corpos se φ é homomorfismo sobrejetor de corpos e $\varphi \mid_k = Id_k$, onde Id_k é a função identidade de k em k.*

Definição 1.1.10 : *Seja k um corpo. Dizemos que uma extensão $\overline{k}$ de k é um fêcho algébrico de k se $\overline{k}/k$ é algébrica e $\overline{k}$ é algebricamente fechado, isto é, todo polinômio não constante $g(x) \in \overline{k}[x]$ tem raiz em $\overline{k}$.*

O principal resultado sobre o fêcho algébrico de um corpo é o seguinte :

Teorema 1.1.11 : *Seja k um corpo , então existe , a menos de um k–isomorfismo, um único fêcho algébrico de k*

A partir deste teorema nos parece natural apresentar a seguinte definição:

Definição 1.1.12 : *Sejam k um corpo , $\overline{k}$ fêcho algébrico de k e $f(x) \in k[x]$ um polinômio não constante. Dizemos que $K \subseteq \overline{k}$ é um corpo de raízes de $f(x)$ sobre k se f decompõe-se em fatores lineares em K , isto é, $f(X) = c(X-\alpha_1)\ldots(X-\alpha_n)$, com $\alpha_i \in K$ para todo $i = 1,\ldots,n$, e tal que $K = k(\alpha_1,\ldots,\alpha_n)$.*

Como consequência imediata do teorema 1.1.11 tem-se que:

Corolário 1.1.13 : *Quaisquer dois corpos de raízes de um polinômio não constante $f(x) \in k[x]$ são k-isomorfos.*

Ainda a respeito de corpo de raízes, em característica zero, é importante citar o seguinte resultado.

Proposição 1.1.14 : *Sejam k um corpo , $\overline{k}$ um fêcho algébrico de k , $f(X) \in k[X]$ um polinômio não constante e irredutível e $K \subseteq \overline{k}$ o corpo de raízes de $f(X)$ sobre k. Então:*

1) *$\sigma : K \to \overline{k}$ é um k-homomorfismo de corpos se, e somente se, é σ um k-automorfismo de K ;*

2) *Se $G(K/k)$ é o grupo de k-automorfismos de K, conhecido como grupo de Galois de K sobre k, então $|G| = [K : k]$. Mais ainda , $a \in k$ se, e somente se, $\sigma(a) = a$ para todo $\sigma \in G(K/k)$;*

3) *Se $y \in K$ é raiz de $f(x)$ e $\sigma \in G(K/k)$ então $\sigma(y)$ também é raiz de $f(x)$.*

4) *Se $y,z \in K$ são raízes de $f(x)$ então existe $\sigma \in G(K/k)$ tal que $\sigma(y) = z$.*

Definição 1.1.15 : *Sejam k um corpo , $\overline{k}$ um fêcho algébrico de k e $f(X) \in k[X] \setminus k$.* Se $f(X) = a_n(X-t_1)\ldots(X-t_n)$, *com $a_n \in k$ e $t_i \in \overline{k}$* para todo *i. Definimos o discriminante de f como sendo:*

$$D(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{i \neq j} (t_i - t_j).$$

A partir da proposição 1.1.14 e desta definição obtem-se o seguinte resultado.

Proposição 1.1.16 : *Dados um corpo k e um polinômio irredutível não constante $f(x) \in k[x]$ então $D(f) \in k$.*

1.2 Anéis Regulares e Decomposição Primária

Nesta seção , assumido conhecido a definição de anel noetheriano , vamos definir e enunciar alguns conceitos que dizem respeito a localização em ideais primos e sobre a decomposição primária de um ideal.

Primeiramente vejamos algumas definições e conceitos de teoria dos ideais, observando que assumiremos sempre que quando mencionamos anéis , significa que estes são comutativos com identidade e noetherianos.

Assim seja R um anel, denotaremos por $Spec(R)$ o conjunto de todos os ideais primos de R , e por $Max(R)$ o conjunto de todos os ideais maximais de R. Sendo R um anel local com $\mathfrak{m}$ seu ideal maximal , denotaremos este por $(R,\mathfrak{m})$, e por $(R,\mathfrak{m}_1,\ldots,\mathfrak{m}_r)$ o anel semi-local com $Max(R) = \{\mathfrak{m}_1,\ldots,\mathfrak{m}_r\}$.

Feitas estas menções vejamos agora o que é a dimensão de Krull de um anel R e altura de um ideal $P \in Spec(R)$.

Definição 1.2.1 :*Seja R um anel,a dimensão de Krull de R,denotada por* $\dim(R)$, *é definida por :*

$$\dim(R) = Sup\{n \in \mathbb{N}\,;\exists\, P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_n\,;\, P_i \in Spec(R)\,,\, i = 0,1,\ldots,n\}$$

Observemos que tal dimensão pode ser infinita. Por exemplo se $R = k[X_1,X_2,\ldots]$ é o anel de polinômios a infinitas variáveis sobre k tem-se que $(X_1) \subsetneq (X_1,X_2) \subsetneq \ldots$.

De forma análoga definimos a altura de um ideal primo $P \in Spec(R)$ por:

Definição 1.2.2 : *Seja R um anel e $P \in Spec(R)$, a altura de P, que é denotada por $ht(P)$ é definida por:*

$$ht(P) = Sup\{n \in \mathbb{N}\,;\exists\, P_0 \subsetneq \ldots \subsetneq P_n = P\,;\, P_i \in Spec(R),\, i = 0,1,\ldots,n\}$$

Lembrando que a localização de um anel R num ideal primo p é denotada por: $R_p = S^{-1}R = \{\frac{r}{s}\ ;\ r \in R \text{ e } s \in S = R \setminus p\}$.

Vale apena observar que $ht(P) = \dim(R_p)$.

Definição 1.2.3 : *Seja J um ideal do anel R. O número mínimo de geradores de J é definido como sendo* $\min\{s \in \mathbb{N}\ ;$ *existem* $a_1,\ldots,a_s \in J$ *que geram* $J\}$ *, e será denotado por* $\mu(J)$.

Agora estamos prontos para definir o que é um anel regular , definição esta que será frequentemente usada no decorrer deste trabalho. Então vejamos.

Definição 1.2.4 : *Seja (R,m) um anel noetheriano local , dizemos que (R,m) é regular se* $\dim(R) = ht(m) = \mu(m)$.

O teorema e a proposição a seguir são resultados clássicos que valem a pena serem citados .

Teorema 1.2.5 : *Sejam R um anel noetheriano local de dimensão d , e m seu ideal maximal. Seja $k = \frac{R}{m}$, então são equivalentes :*

i) $\dim_k\left(\frac{m}{m^2}\right) = d$;

ii) m é gerado por d elementos.

Demonstração : Ver em [9] (teorema 11.22)

Proposição 1.2.6 : *Todo anel regular é um domínio.*

Demonstração : Ver em [4] (cap.V , corolário 5.15a)

A proposição que citaremos a seguir nos será útil em resultados apresentados no capítulo 2.

Proposição 1.2.7 : *Se (R,m) é regular , então $R[X]_p$ é regular para todo $p \in Spec(R[X])$, com $p \cap R = m$.*

Demonstração : Ver em [4] (cap.VI , proposição 1.7)

No capítulo 2 vamos utilizar o conceito de decomposição primária de um ideal num resultado importante de A. Seidenberg.

Para podermos definir e enunciar resultados relacionados a decomposição primária de ideais precisamos saber o que é um ideal primário, portanto iniciamos com a definição:

Definição 1.2.8 : *Dizemos que um ideal Q do anel R é primário se $Q \neq R$ e se $x.y \in Q$ então $x \in Q$ ou $y^n \in Q$ para algum número natural $n \geq 1$.*

Em outras palavras, Q é primário se, e somente se, $\frac{R}{Q} \neq 0$ e todo divisor de zero em $\frac{R}{Q}$ é nilpotente.

Observamos que uma consequência imediata da definição de um ideal primário Q é que seu ideal radical P é ideal primo e por isto dizemos que Q é P-primário quando $P = \sqrt{Q}$. Agora estamos prontos para dar a definição de ideal decomponível.

Definição 1.2.9 : *Dado um ideal J de um anel R dizemos que J admite uma decomposição primária ou que é decomponível se existem ideais primários $Q_1, \cdots, Q_n$ tal que $J = Q_1 \cap \cdots \cap Q_n$.*

Na verdade todo ideal decomponível admite uma decomposição primária minimal, a saber:

Definição 1.2.10 : *Uma decomposição primária minimal de um ideal J é definida por: $J = Q_1 \cap \ldots \cap Q_m$, onde os Q_i são primários e :*

i) $\sqrt{Q_i} = P_i \neq P_j = \sqrt{Q_j}$, *se* $i \neq j$;

ii) $\bigcap_{j \neq i} Q_j \not\subseteq Q_i$, $\forall\, i = 1, \ldots, m.$

Para anéis noetherianos tem-se o seguinte resultado:

Teorema 1.2.11 : *Todo ideal próprio de um anel noetheriano é decomponível.*

Demonstração : Ver em [1] (cap.IV)

O teorema a seguir nos garante uma certa unicidade de uma decomposição primária minimal de um ideal qualquer. Este teorema é chamado de "1º da unicidade", e será de extrema importância no capítulo 2, pois o utilizaremos na demonstração do teorema 2.2.8.

Teorema 1.2.12 (1° da unicidade) : *Seja um anel R. Se $J \subset R$ é um ideal decomponível e $J = Q_1 \cap \ldots \cap Q_m$ é uma decomposição primária minimal com Q_i sendo P_i-primário, para todo $i = 1, \ldots, m$. Então:*

1) $\{P_1, \ldots, P_m\} = Spec(R) \cap \{\sqrt{J : x} \; ; x \in R\}$;

2) Se $J = \tilde{Q}_1 \cap \ldots \cap \tilde{Q}_r$ é decomposição primária minimal, então $r = m$ e,depois de rearranjar se necessário, $\sqrt{\tilde{Q}_i} = P_i$ para todo i.

Demonstração : Ver em [1] (cap.IV , teorema 4.5)

O teorema da unicidade citado acima nos leva para a seguinte definição:

Definição 1.2.13 : *Seja $J \subsetneq R$ um ideal com $J = Q_1 \cap \ldots \cap Q_m$ decomposição primária minimal tal que Q_i é P_i -primário para todo i. Dizemos que cada P_i é um primo associado de J . Mais ainda , se P_i for minimal entre os ideais primos P_j, dizemos que ele é primo associado minimal (ou primo isolado) de J ,caso contrário dizemos que P_i é primo imerso de J.*

1.3 Completamento

Nesta seção faremos uma exposição suscinta de alguns conceitos e resultados que utilizaremos a respeito do completamento de um anel R em relação à topologia I-ádica, onde I é um ideal de R. Todos enunciados e resultados podem ser encontrados no livro de M. Nagata, referência [11].

Iniciamos com a descrição de tal topologia.

Seja I um ideal do anel R e considere a família $\mathcal{F}$ de subconjuntos de R dada por $\mathcal{F} = \{b + I^n \; ; \; b \in R \; , \; n \in \mathbb{N}\}$. Verifica-se que a partir de $\mathcal{F}$ pode-se definir uma topologia sobre R que tem $\mathcal{F}$ como base de abertos e que torna R um anel topológico, isto é, suas operações são contínuas em relação a tal topologia. Esta topologia é chamada de I-ádica.

Agora quando $\cap I^n = (0)$ pode-se provar que o anel R com a topologia I-ádica é um espaço métrico, em particular isto acontece quando $(R,\mathfrak{m})$ é um anel noetheriano local e $\mathfrak{m} = I$ ou, mais geralmente, quando $(R,\mathfrak{m}_1, \ldots, \mathfrak{m}_t)$ é um anel semi-local e $\mathcal{J}(R) = I$, com $\mathcal{J}(R) = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_t$ sendo o radical de jacobson de R. Vamos nos referir à topologia natural de R sempre que consideramos a $J(R)$ –ádica topologia de R.

Resumimos os comentários que acabamos de fazer no seguinte resultado :

Proposição 1.3.1 : *Sejam R um anel noetheriano e I um ideal de R tal que $I \subseteq J(R)$. Então $\bigcap_{i \in \mathbb{N}} I^i = 0$ e a função $d : R \times R \to R$ definida por $d(r,r) = 0$ e se $r \neq s$,: $d(r,s) = 2^{-n}$ se ,*

e somente se , $r-s \in I^n$ e $r-s \notin I^{n+1}$ define uma métrica para o espaço topológico R com a topologia I-ádica

No que segue , vamos assumir que R é um anel noetheriano semi-local munido da topologia natural, e portanto munido de uma métrica d. Com esta métrica, podemos introduzir o conceito de completamento da maneira usual :

Definição 1.3.2 : *Um completamento de R é um anel $\hat{R}$ que satisfaz as seguintes propriedades :*

1) $\hat{R}$ é um espaço métrico com uma função distância $\hat{d} : \hat{R} \times \hat{R} \to \hat{R}$ tal que:
$\hat{d}(x,y) = d(x,y)$para todo par $x,y \in R$;
2) $\hat{R}$ é completo :
3) R é um subespaço denso de $\hat{R}$;

A existência e unicidade do completamento é citada no seguinte resultado :

Teorema 1.3.3 : *O anel local (R,m) possui, a menos de isomorfismo, um único completamento $\hat{R}$. E mais ainda o anel $\hat{R}$* satisfaz:

1) $(\hat{R},\hat{m})$ é local com $\hat{m} = m\hat{R}$.
2) $dim(R) = dim(\hat{R})$
3) R é regular se, e somente se, $\hat{R}$ é regular

Na teoria do completamento de anéis um dos principais exemplos é o anel de séries de potências sobre um anel, a saber:

Definição 1.3.4 : *Sejam R um anel, $X_1,\ldots,X_r$ variáveis sobre R e $d \in \mathbb{N}$. O polinômio $F_d = \sum_{i_1+\ldots+i_r=d} a_i.X_1^{i_1}.X_2^{i_2}\ldots X_r^{i_r}$ é denominado forma homogênea de grau d. O conjunto de somas infinitas (de tais formas) é chamado de anel de séries de potências com coeficientes em R , e será denotado por $R[[\underline{X}]] = R[[X_1,\ldots,X_r]] = \{\sum_{d=0}^{\infty} F_d$; : F_d* é uma forma de grau *$d\}$.*

Feita esta definição podemos enunciar o seguinte resultado, que será de extrema importância para a demonstração de um resultado obtido por R. Hart em [4], mais precisamente no teorema 2.3.2. Observamos que a demonstração deste resultado está em [10].

Teorema 1.3.5 : *Seja* (R,m) *um anel local com* $m = (a_1,\cdots,a_r)$. *Então o completamento* $\hat{R}$ *de* R *é o anel* $\dfrac{R[[X_1,\ldots,X_r]]}{\sum(X_i - a_i)R[[X_1,\ldots,X_r]]}$, *onde* $X_1,X_2,\ldots,X_r$ *são indeterminadas sobre* R.

O último resultado desta seção é de extremo valor na demonstração do teorema de Seidenberg , que apresentaremos no capítulo 2.

Proposição 1.3.6 : *Suponha* R *um anel regular local completo de dimensão* n *e com corpo de resíduos* k . *Se* R *contém um corpo , então* R *é isomorfo ao anel de séries formais* $k[[X_1,\ldots,X_n]]$.

Demonstração : Ver em D. Eisenbud [3] (cap. 10 , proposição 10.16)

Capítulo 2

Regularidade e Simplicidade em k-álgebras finitamente geradas

O estudo dos resultados obtidos por A. Seindenbeg, em [13], e por R. Hart, em [4], é o principal objetivo deste capítulo. Mas para fazer tal estudo necessitamos de alguns conceitos e resultados fundamentais sobre derivação. Para isso vamos desenvolver uma seção preliminar que nos dará as ferramentas para nosso objetivo final.

2.1 Derivações de Anéis

Esta seção é a principal base para os resultados que serão vistos daqui para frente. Nesta vamos introduzir o conceito de derivação, estudá-las em anéis polinômiais, séries de potências, corpos algebricamente fechados, sistemas de equações diferenciais e em extensões algébricas e transcendentais . Os resultados que serão descritos nesta seção foram estudados em "Polynomial Derivations and their rings of constants" , de A. Nowicki [12].

Adiantamos que algumas das demonstrações dos resultados não estarão aqui descritas mas será indicado onde se possa encontrá-las.

Para começarmos a estudar derivações precisamos saber o que de fato é uma derivação , então começaremos com a definição .

Definição 2.1.1 : *Seja R um anel . Uma aplicação aditiva $d : R \to R$ é dita ser uma derivação de R se, para todo $x,y \in R$ tem-se:*

$$d(xy) = x.d(y) + y.d(x).$$

Se R é uma k-álgebra, com k anel então a derivação d de R é chamada de k-derivação se $d(\alpha x) = \alpha.d(x)$, para todo $\alpha \in k$.

Notação : Denotaremos por $Der(R)$ o conjunto de todas as derivações de R, e por $Der_k(R)$ o conjunto de todas as k-derivações de R.

A primeira propriedade fundamental sobre derivações é dada na seguinte proposição:

Proposição 2.1.2: *Sejam R um anel e $S \subset R$ um sistema multiplicativo. Se d é uma derivação de R então existe uma única derivação $\tilde{d}$ do anel de frações $S^{-1}R$ satisfazendo $\tilde{d}(\frac{r}{1}) = \frac{\tilde{d}(r)}{1}$. para todo $r \in R$. Em particular, se R é domínio e K é seu corpo de frações então existe uma única derivação $\tilde{d}$ de K tal que $\tilde{d}|R = d$.*

Demonstração : Vamos supor que exista tal $\tilde{d}$. Logo ao tomarmos $\alpha = \frac{r}{s} \in S^{-1}R$ teremos:

$$\tilde{d}(\frac{r}{1}) = \tilde{d}(\frac{r}{s}.\frac{s}{1}) = \tilde{d}(\alpha).\frac{s}{1} + \alpha\tilde{d}(\frac{s}{1})$$

portanto $\tilde{d}(\alpha) = \frac{d(r)s - rd(s)}{s^2}$. Agora é bastante simples mostrar que a igualdade acima define a única derivação que satisfaz a propriedade requerida.

■

Observamos que se $R[X] = R[x_i \; ; \; i \in I]$ é o anel de polinômios,nas variáveis $\{x_i, i \in I\}$, sobre R a derivada parcial $\frac{\partial}{\partial x_i}$ é uma R-derivação de $R[X]$, para todo $i \in I$. E mais ainda, é a única R-derivação d de $R[X]$ tal que $d(x_i) = 1$ e $d(x_j) = 0$ para todo $j \neq i$.

Na verdade gostaríamos de apresentar um resultado bem mais geral que afirma que:

Proposição 2.1.3: *Dada uma derivação d do anel R existe uma única derivação $\tilde{d}$ do anel de polinômios $R[X] = R[x_i \; ; \; i \in I]$ tal que $\tilde{d}|R = d$ e $d(x_i) = 0$ para todo $i \in I$. Mais ainda se $f : I \to R[X]$ é uma função , então existe uma única derivação D de $R[X]$ tal que $D \mid_R = d$ e $D(x_i) = f(i)$, para todo $i \in I$.*

Demonstração : Dado $F = \sum_{\lambda=(\lambda_1,\cdots,\lambda_n)} a_\lambda x_{\lambda_1}^{j_1} \cdots x_{\lambda_n}^{j_n} \in R[X]$, definimos:

$$\tilde{d}(F) = F^d = \sum_{\lambda=(\lambda_1,\cdots,\lambda_n)} d(a_\lambda) x_{\lambda_1}^{j_1} \cdots x_{\lambda_n}^{j_n}.$$

Do fato de d ser derivação é muito simples provar que $\tilde{d}$ também é.

Agora a derivação D é definida da seguinte maneira : se $G \in R[X]$, então $D(G) = \tilde{d}(G) + f(i_1)\frac{\partial G}{\partial x_{i_1}} + \ldots + f(i_n)\frac{\partial G}{\partial x_{i_n}}$, onde $\{i_1, \ldots, i_n\}$ é um subconjunto finito de I tal que $G \in R[x_{i_1}, \ldots, x_{i_n}]$.

A unicidade das derivações $\tilde{d}$ e D segue imediatamente dos fatos de que elas estão definidas num conjunto de geradores do anel $R[X]$.

■

Uma primeira consequência fundamental do teorema que acabamos de provar é o seguinte resultado:

Teorema 2.1.4 : *Seja* $k[X] = k[x_1, \ldots, x_n]$ *um anel de polinômios sobre k. Então temos :*

1) Se $f_1, \ldots, f_n \in k[X]$, *então existe uma única k-derivação* D *de* $k[X]$ *tal que* $D(x_1) = f_1, \ldots, D(x_n) = f_n$. *Essa derivação é da forma* $D = f_1 \frac{\partial}{\partial x_1} + \ldots + f_n \frac{\partial}{\partial x_n}$.

2) $Der_k(k[X])$ *é um* $k[X]$*-módulo livre com base* $\{\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}\}$.

3) $\frac{\partial}{\partial x_i}\frac{\partial}{\partial x_j} = \frac{\partial}{\partial x_j}\frac{\partial}{\partial x_i}$, *para todo* $i, j \in \{1, \ldots, n\}$.

4) Se $D \in Der_k(k[X])$ *e* $f \in k[X]$ *, então* $D(f) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} d(f)$.

Demonstração : 1) Basta usar a proposição anterior tomando $d = 0$, $X = \{x_1, \cdots, x_n\}$ e $f(i) = x_i$ para todo $i \in X$.

2) Por 1) basta verificarmos que $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}$ são linearmente independentes, ou seja basta mostrar que se $D = \sum_{i=1}^{n} f_i \frac{\partial}{\partial x_i} = 0$ então para todo i tem-se que $f_i = 0$. Mas observe que 1) nos diz que $D(x_i) = f_i = 0$ para todo i.

3) A igualdade é clara se $i = j$. Logo vamos tomar i, j com $i \neq j$.

Como se trata de k-derivações basta verificar que a igualdade

$$(\frac{\partial}{\partial x_i}\frac{\partial}{\partial x_j})(M) = (\frac{\partial}{\partial x_j}\frac{\partial}{\partial x_i})(M)$$

é válida para todo monômio $M = x_1^{r_1} \ldots . x_n^{r_n}$, onde $r_1, \ldots, r_n \in \mathbb{N}$. Então vejamos:

1°) se $r_i > 0$ e $r_j > 0$.

$$\frac{\partial}{\partial x_i}\left(\frac{\partial(M)}{\partial x_j}\right) = \frac{\partial}{\partial x_i}(r_j x_1^{r_1} \ldots . x_j^{r_j - 1} \ldots . x_n^{r_n}) = r_j r_i x_1^{r_1} \ldots . x_j^{r_j - 1} \ldots x_i^{r_i - 1} \ldots . x_n^{r_n}$$

e

$$\frac{\partial}{\partial x_j}\left(\frac{\partial(M)}{\partial x_i}\right) = \frac{\partial}{\partial x_j}(r_i x_1^{r_1} \ldots . x_i^{r_i - 1} \ldots . x_n^{r_n}) = r_i r_j x_1^{r_1} \ldots . x_j^{r_j - 1} \ldots x_i^{r_i - 1} \ldots . x_n^{r_n}$$ e vemos claramente que nossa igualdade é válida.

2°) Se $r_i = 0$ ou $r_j = 0$.

Sem perda de generalidade suponhamos $r_i = 0$, assim temos que:

$\frac{\partial}{\partial x_i}\left(\frac{\partial(x_1^{r_1} \ldots . \hat{x}_i \ldots . x_n^{r_n})}{\partial x_j}\right) = \frac{\partial}{\partial x_i}(r_j\, x_1^{r_1} \ldots . x_j^{r_j - 1} \ldots \hat{x}_i \ldots . x_n^{r_n}) = 0$ e

$\frac{\partial}{\partial x_j}\left(\frac{\partial(x_1^{r_1} \ldots . \hat{x}_j \ldots . x_n^{r_n})}{\partial x_i}\right) = \frac{\partial}{\partial x_j}(r_i\, x_1^{r_1} \ldots . x_i^{r_i - 1} \ldots \hat{x}_j \ldots . x_n^{r_n}) = 0$ e vemos que a igualdade é satisfeita.Onde o símbolo $\hat{x}_i$ significa a ausência de x_i na expressão $x_1^{r_1} \ldots . \hat{x}_i \ldots . x_n^{r_n}$.

4) Consequência imediata de 1).

■

Como consequências imediatas da proposição 2.1.2 e do teorema 2.1.4 seguem os seguintes resultados.

Proposição 2.1.5 : *Seja S um conjunto algebricamente independente sobre o corpo k e seja $k(S)$ uma extensão puramente transcendental de k. Se d é uma derivação de k e $f : S \to k(S)$ é uma função. Então existe uma única derivação D de $k(S)$ tal que $D \mid_k = d$ e $D(x) = f(x)$, $\forall\, x \in S$.*

Teorema 2.1.6 : *Seja $k(X) = k(x_1, \ldots, x_n)$. Então temos :*

1) Se $f_1, \ldots, f_n \in k(X)$, então existe uma única k-derivação d de $k(X)$ tal que $d(x_1) = f_1, \ldots, d(x_n) = f_n$. Essa derivação é da forma $d = f_1 \frac{\partial}{\partial x_1} + \ldots + f_n \frac{\partial}{\partial x_n}$.

2) As derivações $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}$ formam uma base do $k(X)$-espaço $Der_k(k(X))$.

3) $\frac{\partial}{\partial x_i}\frac{\partial}{\partial x_j} = \frac{\partial}{\partial x_j}\frac{\partial}{\partial x_i}$, para todo $i,j \in \{1, \ldots, n\}$.

4) Se $d \in Der_k(k(X))$ e $f \in k(X)$, então $d(f) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}.d(x_i)$.

Dados um anel R e um conjunto finito de variáveis $T = \{t_1, \cdots, t_m\}$ sobre R. Sabemos que o anel de séries formais $R[[T]] = R[[t_1, \ldots, t_m]]$ é o completamento do anel de polinômios $R[T]$ com a topologia **m**-ádica com $\mathbf{m} = (t_1, \cdots, t_m)$. Assim a partir do lema que apresentamos abaixo podemos, de modo natural, obter as versões da proposição 2.1.3 e do teorema 2.1.4 para séries formais.

Lema 2.1.7: *Sejam d uma derivação de um anel R, $I \subseteq R$ um ideal e $n \in \mathbb{N}$, então $d(I^n) \subset I^{n-1}$.*

Demonstração : Sabemos que todo elemento de I^n é uma soma finita de elementos do tipo $a = a_1 \cdots a_n$ com $a_i \in I$ para todo i, agora $d(a) = d(a_1 \ldots . a_n) = \sum_{i=1}^{n} a_1 \ldots a_{i-1}.d(a_i).a_{i+1} \ldots a_n$ e portanto $d(a) \in I^{n-1}$, como queríamos.

■

Proposição 2.1.8 : *Sejam R um anel e $R[[T]] = R[[t_1, \cdots, t_m]]$ o anel de séries formais a m variáveis sobre R. Se d é uma derivação de R e se $f_1, \ldots, f_n \in R[[T]]$, então existe uma*

única derivação D de $R[[T]]$ tal que $D\mid_R = d$ e $D(t_1) = f_1, \ldots, D(t_n) = f_n$.

Demonstração : Usando o lema anterior para o ideal $\mathbf{m} = (t_1, \cdots, t_n)$ podemos concluir que, para todo i, a derivada parcial $\frac{\partial}{\partial t_i}$ de $R[T]$ é continua em relação à topologia **m**-ádica e assim ela pode ser estendida de modo único para uma derivação, que também chamaremos $\frac{\partial}{\partial t_i}$, de $R[[T]]$. Agora , pela proposição 2.1.3, sabemos que existe uma única $\tilde{d}$ derivação de $R[T]$ tal que $\tilde{d}\mid_R = d$ e $\tilde{d}(t_i) = 0$ para todo i. Tome $u \in R[[T]]$ e para todo $r \in \mathbb{N}$ chame de u_r a componente homogênea de grau r de u.

Usando novamente o lema anterior temos que $\tilde{d}$ é continua em relação à topologia **m**-ádica e assim ela pode ser estendida de modo único para uma aplicação que também chamaremos $\tilde{d}$ de $R[[T]]$ dada por $\tilde{d}(u) = \sum_{r\geq 0} \tilde{d}(u_r)$. Que $\tilde{d}$ é derivação segue imediatamente do fato de $\tilde{d}\mid_R$ ser derivação e de sua continuidade em relação à topologia **m**-ádica. Agora, de modo análogo ao feito na prova da proposição 2.1.3, definimos:

$$D = \tilde{d} + f_1 \frac{\partial}{\partial t_1} + \cdots f_m \frac{\partial}{\partial t_m}$$

■

Teorema 2.1.9 :

1) Se $f_1, \ldots, f_n \in R[[T]]$, então existe uma única R-derivação d de $R[[T]]$ tal que $d(x_1) = f_1, \ldots, d(x_n) = f_n$. Essa derivação é da forma $d = f_1 \frac{\partial}{\partial x_1} + \ldots + f_n \frac{\partial}{\partial x_n}$.

2) $Der_R(R[[T]])$ é um $R[[T]]$-módulo livre com base $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}$.

3) $\frac{\partial}{\partial x_i}\frac{\partial}{\partial x_j} = \frac{\partial}{\partial x_j}\frac{\partial}{\partial x_i}$, para todo $i,j \in \{1, \ldots, n\}$.

4) Se $d \in Der_R(R[[T]])$ e $f \in R[[T]]$, então $d(f) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} . d(x_i)$.

Acabamos de ver, nos resultados precedentes, que se $R = k[X] = k[x_1, \cdots, x_n]$ ou $R = k[[T]] = k[[t_1, \cdots, t_n]]$, com k corpo então $Der_k(R)$ é R-módulo livre de posto n assim gostaríamos apenas de citar mais dois resultados que caracterizam o fato de um conjunto de n k-derivações ser uma base livre de $Der_k(R)$.

Nos próximos dois resultados o anel R é $k[X] = k[x_1, \ldots, x_n]$ ou $k[[X]] = k[[x_1, \ldots, x_n]]$, com k corpo .

Proposição 2.1.10 : *Sejam $d_1, \ldots, d_n$ k-derivações de R.O conjunto $\{d_1, \ldots, d_n\}$ é uma base de $Der_k(R)$ se, e somente se, a matriz $[d_i(x_j)]$ é invertível.*

Demonstração : Ver em A. Nowicki ([7] , proposição 2.5.1)

Teorema 2.1.11 : *Sejam $d_1,\ldots,d_n$ k-derivações de R. As seguintes condições são equivalentes:*

1) O conjunto $\{d_1,\ldots,d_n\}$ é uma base livre de $Der_k(R)$;

2) Existem elementos $F_1,\ldots,F_n \in R$,tais que $d_i(F_j) = \delta_{ij}$, $\forall\ i,j = 1,\ldots n$, onde δ_{ij} é o delta de Kronecker.

Demonstração : Ver em A. Nowicki ([7] , teorema 2.5.2)

Até aqui temos falado a respeito de extensões de derivações quando acrescentamos variáveis a um determinado anel. Agora vamos trabalhar com a situação em que temos extensões algébricas de corpos. O primeiro lema fundamental é o seguinte:

Lema 2.1.12 : *Sejam L/k uma extensão de corpos e d uma derivação de k. Tome um elemento algébrico α em L. Então temos:*

1) Existe uma única derivação $\tilde{d}$ de $k[\alpha]$ tal que $\tilde{d} \mid_k = d$.

2) Se D é derivação de L com $D \mid_k = d$ então $D(k[\alpha]) \subseteq k[\alpha]$, isto é, $\tilde{d} = D \mid_{k[\alpha]}$ é a única derivação de $k[\alpha]$ que estende d.

Demonstração : *1)* Seja $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x]$ o polinômio mínimo de α sobre k. Suponha por ora que existe tal $\tilde{d}$, assim teremos que: $0 = \tilde{d}(f(\alpha)) = \frac{\partial f}{\partial x}(\alpha).\tilde{d}(\alpha) + f^d(\alpha)$ (lembre que $f^d(x)$ é definido por $f^d(x) = d(1)x^n + d(a_{n-1})x^{n-1} + \cdots + d(a_0)$).

Sendo $f(x)$ o polinômio mínimo de α, tem-se que $\frac{\partial f}{\partial x}(\alpha) \neq 0$ e portanto

$$(*)\quad \tilde{d}(\alpha) = -\frac{f^d(\alpha)}{\frac{\partial f}{\partial x}(\alpha)}$$

Agora é muito simples mostrar que dado $\beta = g(\alpha) \in k[\alpha]$ com $g(x) \in k[x]$ a expressão

$$\tilde{d}(\beta) = \frac{\partial g}{\partial x}(\alpha).\tilde{d}(\alpha) + g^d(\alpha)$$

com $\tilde{d}(\alpha)$ dado pela igualdade $(*)$ define de maneira única a derivação que queremos.

2) Seja $\beta \in k[\alpha]$, logo existe $g(x) \in k[x]$ tal que $\beta = g(\alpha)$ e assim $D(\beta) = \frac{\partial g}{\partial x}(\alpha).D(\alpha) + g^d(\alpha)$, onde $D(\alpha) = -\frac{f^d(\alpha)}{\frac{\partial f}{\partial x}(\alpha)}$, onde $f(x) \in k[x]$ é o polinômio mínimo de α sobre k. Portanto temos que $D(\beta) \in k[\alpha]$ como queríamos.

■

Agora estamos em condições de enunciar e provar o resultado fundamental que caracteriza o fato de uma extensão de corpos ser algébrica em termos de suas derivações.

Teorema 2.1.13 : *Seja L/k extensão de corpos. Então as seguintes condições são*

equivalentes :

1) L/k é uma extensão algébrica ;

2) Para toda derivação d de k existe uma única derivação D de L tal que $D\,|_k = d$

3) Se δ é uma k-derivação de L, então $\delta = 0$.

Demonstração : *1)⇒2)* Seja d uma derivação de k e considere a família $\mathcal{X}$ definida por:

$\mathcal{X} = \{(F,d_F);\ L/F/k$ são extensões de corpos e d_F é derivação de F que estende $d\}$

Observe que $(k,d) \in \mathcal{X}$ e assim $\mathcal{X}$ é não vazia. Agora defina em $\mathcal{X}$ a seguinte ordem parcial:

$$(F_1,d_{F_1}) \leq (F_2,d_{F_2}) \Leftrightarrow F_2/F_1 \text{ e } d_{F_2}|F_1 = d_{F_1}$$

É muito simples mostrar que toda cadeia de $\mathcal{X}$ tem elemento maximal em $\mathcal{X}$. Deste fato podemos concluir, pelo lema de Zorn, que $\mathcal{X}$ tem um elemento maximal (F,d_F). Vamos provar que $F = L$. Suponha que não e tome $\alpha \in L \setminus F$. Considere $K = F(\alpha)$ e assim pelo lema anterior sabemos que existe uma derivação d_K de K que estende d_F e portanto $(K,d_K) \in \mathcal{X}$, mas isto nos dá uma contradição já que (F,d_F) é elemento maximal de $\mathcal{X}$ e $(F,d_F) < (K,d_K)$. Assim $F = L$ e $d_F = D$ é uma derivação de L que estende d. A unicidade de D é consequência imediata do lema anterior.

2)⇒3) Basta tomar $d = 0$ em *2)*.

3)⇒1) Tome $S \subset L$ uma base de transcendência de L/k, isto é, S é um conjunto algebricamente independente sobre k e $L/k(S)$ é algébrica. Na verdade queremos mostrar que $S = \emptyset$. Vamos supor que não seja e tome $x \in S$, agora considere a k-derivação $\delta = \frac{\partial}{\partial x}$ de $k(S)$. Como $L/k(S)$ é algébrica podemos, usando que *1)⇒2)*, estender δ a uma k-derivacão não nula de L, o que contradiz a hipótese.

■

Um outro resultado fundamental nesta direção é o seguinte:

Teorema 2.1.14 : *Seja $L = k(p_1,\ldots,p_n)$ uma extensão finitamente gerada do corpo k.*

Sejam $p = (p_1,\ldots,p_n)$ e $\mathcal{M}_p = \{f \in k[x_1,\ldots,x_n]\ ;\ f(p) = 0\}$. Então as seguintes condições são equivalentes :

1) L é algébrica sobre k ;

2) Existem n polinômios $f_1,\ldots,f_n \in \mathcal{M}_p$ tais que $\det\left[\frac{\partial f_i(p)}{\partial x_j}\right] \neq 0$.

Demonstração : *1)⇒2)* Para cada i, $1 \leq i \leq n$, defina f_i da seguinte forma: $f_i = f_i(x_1,\cdots,x_n) = g_i(x_i) \in k[x_i]$, onde $g_i(x_i)$ é o polinômio mínimo de p_i sobre k. Logo $f_i \in \mathcal{M}_p$ e, mais ainda, tem-se que:

$$\frac{\partial f_i}{\partial x_i}(p) \neq 0 \text{ e } \frac{\partial f_i}{\partial x_j}(p) = 0 \text{ se } i \neq j$$

Portanto $\det\left[\frac{\partial f_i(p)}{\partial x_j}\right] = \prod_{i=1}^{n} \frac{\partial f_i}{\partial x_i}(p) \neq 0$.

2)⇒1) Seja δ uma k-derivação de L. Sabemos que $f_i(p) = 0$ para todo i. Logo,pela regra da cadeia, obtemos, para todo i, a igualdade:

$$\sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j}(p).\delta(p_j) = 0$$

agora como $\det\left[\frac{\partial f_i(p)}{\partial x_j}\right] \neq 0$ tem-se que $\delta(p_j) = 0$ para todo j e sendo δ uma k-derivação segue que $\delta = 0$. Assim o teorema anterior nos garante que L/k é algébrica.

■

2.2 Sobre a simplicidade de k-álgebras finitamente geradas

Neste parágrafo vamos fazer um estudo sobre os d-ideais de uma k-álgebra finitamente gerada A sendo k um corpo de característica zero e d uma k-derivação de A.O principal objetivo aqui é o de apresentar a caracterização, dada por Seidenberg em [13], da regularidade de A em termos do fato de A ser $\mathcal{D}$-simples, onde $\mathcal{D} = Der_k(A)$.

Iniciamos com as definições dos conceitos de d-ideais e $\mathcal{D}$-simplicidade que aparecem no comentário feito acima.

Definição 2.2.1 : *Sejam R um anel, $I \subseteq R$ um ideal e d uma derivação de R . O ideal I é dito ser um d-ideal (ou d-invariante ou ainda um ideal d-diferencial) se $d(I) \subseteq I$. Sendo $\mathcal{D}$ uma família de derivações de R, dizemos que I é um $\mathcal{D}$-ideal se para toda $d \in \mathcal{D}$ tem-se que I é um d-ideal. Mais ainda dizemos que R é $\mathcal{D}$-simples (ou simples, se for para a família de todas as derivações de R) se os únicos $\mathcal{D}$-ideais de R são os triviais.*

Um primeiro resultado sobre simplicidade em extensões de anéis é o seguinte.

Proposição 2.2.2 : *Sejam S/R uma extensão integral de domínios, d uma derivação de R e D uma derivação de S tal que $D\,|_R = d$. Então R é d-simples se e somente se S é d-simples.*

Demonstração : Basta observar que sendo S/R extensão integral de domínios, um ideal J de S é não nulo se e somente se $J \cap R$ é ideal não nulo de R.

■

No trabalho de Seidenberg sobre as propriedades de d-ideais dois conceitos são fundamentais. Um deles é o anel de séries formais em uma variável sobre o anel R, isto é, $R[[t]]$. O outro é um automorfismo exponencial de $R[[t]]$ que é determinado a partir de uma derivação de R. Mas antes de apresentar tal automorfismo vamos necessitar de um resultado geral que apresenta uma igualdade muito útil no manuseio com derivações.

Lema 2.2.3 : *Sejam B um anel e d uma derivação de B. Se $n \in \mathbb{N}$ e $a,b \in B$ então* $d^n(ab) = \sum_{i=0}^{n} \binom{n}{j} d^i(a)d^{n-i}(b)$.

Demonstração : Vamos fazer tal a prova por indução em n. Como d^0 é por definição a identidade de B o caso $n = 0$ segue imediatamente. Suponha verdadeiro para $n \geq 0$. Vamos calcular $d^{n+1}(ab)$:

$$\begin{aligned} d^{n+1}(ab) = d(d^n(ab)) &= d(\sum_{i=0}^{n} \binom{n}{i} d^i(a)d^{n-i}(b)) \\ &= \sum_{i=0}^{n} \binom{n}{i} (d^{i+1}(a)d^{n-i}(b) + d^i(a)d^{n+1-i}(b)) \\ &= ad^{n+1}(b) + \sum_{j=1}^{n} (\binom{n}{j-1} + \binom{n}{j}) d^j(a)d^{n+1-j}(b) + d^{n+1}(a)b \\ &= \sum_{j=0}^{n+1} \binom{n+1}{j} d^j(a)d^{n+1-j}(b). \end{aligned}$$

E assim temos provado o que queríamos.

■

Agora estamos em condições de enunciar e provar o resultado que introduz o automorfismo de que falamos anteriormente.

Proposição 2.2.4 : *Sejam R um anel que contem o corpo dos números racionais $\mathbb{Q}$, d uma derivação de R e $R[[t]]$ o anel de séries formais em uma variável sobre R. Então temos:*

1) A aplicação $D : R[[t]] \longrightarrow R[[t]]$ definida por

$$D(\sum_{i=0}^{\infty} r_i t^i) = \sum_{i=0}^{\infty} d(r_i)t^i$$

é uma derivação de $R[[t]]$. Por abuso de linguagem também denotaremos D por d, isto é, para nós $D = d$.

2) A aplicação $e^{td} : R[[t]] \to R[[t]]$ *dada por* $e^{td}(\alpha) = \sum_{i=0}^{\infty} \frac{d^i(\alpha)}{i!} t^i$ *com* $\alpha \in R[[t]]$ *é um endomorfismo de* $R[[t]]$.

3) Se $\tilde{d}$ *é outra derivação de* R *tal que* $\tilde{d} \circ d = d \circ \tilde{d}$ *então:*

$$e^{t(d+\tilde{d})} = e^{td} \circ e^{t\tilde{d}} = e^{t\tilde{d}} \circ e^{td}.$$

4) O endomorfismo e^{td} *é automorfismo de* $R[[t]]$ *cuja inversa é* e^{-td}.

Demonstração : *1)* Consequência imediata da proposição 2.1.8 tomando $D(t) = 0$.

2) Dado $\alpha \in R[[t]]$, observe que a sequência de somas parciais $\alpha_n = \sum_{i=0}^{n} \frac{d^i(\alpha)}{i!} t^i$ é de Cauchy no anel completo $R[[t]]$ com a topologia t-ádica e portanto $e^{td}(\alpha)$ está bem definido. Agora dado $\beta \in R[[t]]$ é muito simples ver que $e^{td}(\alpha + \beta) = e^{td}(\alpha) + e^{td}(\beta)$ e assim vamos provar apenas que $e^{td}(\alpha\beta) = e^{td}(\alpha)e^{td}(\beta)$. Escrevendo: $e^{td}(\alpha)e^{td}(\beta) = \sum_{n=0}^{\infty} c_n t^n$ temos que para todo n, $c_n = \sum_{i=0}^{n} \frac{d^i(\alpha)}{i!} \frac{d^{n-i}(\beta)}{(n-i)!}$. Mas $\frac{\binom{n}{i}}{n!} = \frac{1}{(n-i)!\,i!}$ e assim $c_n = \sum_{i=0}^{n} \frac{\binom{n}{i}}{n!} d^i(\alpha) d^{n-i}(\beta)$. Logo, pelo lema 2.2.3, $c_n = \frac{d^n(\alpha\beta)}{n!}$. Portanto podemos concluir que $e^{td}(\alpha\beta) = e^{td}(\alpha)e^{td}(\beta)$. O que nos dá que e^{td} é um endomorfismo do anel $R[[t]]$.

3) Dos fatos de que $\tilde{d} \circ d = d \circ \tilde{d}$, $d(t) = 0$ e $\tilde{d}(t) = 0$ podemos facilmente concluir que tanto e^{td} quanto $e^{t\tilde{d}}$ comuta com d e com $\tilde{d}$, mais ainda, eles comutam entre si e usando o binômio de Newton tem-se que para todo $n \in \mathbb{N}$ $(d+\tilde{d})^n = \sum_{i=0}^{n} \binom{n}{i} d^i \tilde{d}^{n-i}$.

Tome $\alpha \in R[[t]]$ então temos:

$$\begin{aligned} e^{td} \circ e^{t\tilde{d}}(\alpha) &= e^{td}\left(\sum_{j=0}^{\infty} \frac{\tilde{d}^j(\alpha)}{j!} t^j \right) \\ &= \sum_{j=0}^{\infty} \frac{\tilde{d}^j(e^{td}(\alpha))}{j!} t^j \\ &= \sum_{j=0}^{\infty} \sum_{i=0}^{\infty} \frac{(\tilde{d}^j \circ d^i)(\alpha)}{j!i!} t^{i+j} \\ &= \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} \frac{\tilde{d}^{n-i} \circ d^i(\alpha))}{i!(n-i)!} \right) t^n \end{aligned}$$

Mas de novo usando a igualdade $\frac{\binom{n}{i}}{n!} = \frac{1}{(n-i)!\,i!}$ tem-se que:

$$e^{td} \circ e^{t\tilde{d}}(\alpha) = \sum_{n=0}^{\infty}(\sum_{i=0}^{n} \frac{\binom{n}{i}}{n!}(\tilde{d}^{n-i} \circ d^i)(\alpha))t^n$$
$$= \sum_{n=0}^{\infty} \frac{(d+\tilde{d})^n(\alpha)}{n!} t^n$$
$$= e^{t(d+\tilde{d})}(\alpha)$$

Como queríamos.

4) Consequência imediata de *3)* quando tomamos $\tilde{d} = -d$.

■

Logo a seguir apresentamos algumas propriedades a respeito de extensão e contração de ideais considerando a extensão de anéis $R[[t]]/R$.

Lema 2.2.5 : *Sejam R um anel e U um ideal de R . Então tem-se :*

1) $UR[[t]] = \{b_0 + b_1t + \ldots ;: b_i \in U\}$.

2) Se $U = U_1 \cap U_2$, *com* U_1 e U_2 *ideais então* $UR[[t]] = U_1R[[t]] \cap U_2R[[t]]$, *e mais* $UR[[t]] \cap R = U$.

3) O anel $\frac{R[[t]]}{UR[[t]]}$ *é isomorfo a* $\frac{R}{U}[[t]]$. *Em particular* U *é ideal primo de* R *se e somente se* $UR[[t]]$ *é ideal primo de* $R[[t]]$.

Demonstração: *1)* Vejamos que $UR[[t]] \subset \{b_0 + b_1t + \ldots \ ; \ b_i \in U\}$. Sabemos que todo elemento de $UR[[t]]$ é soma finita de elementos do tipo $\alpha = (r_0 + r_1t + \ldots).u$, com $r_i \in R$, para todo i , e $u \in U$. Logo $\alpha = r_0.u + r_1.u.t + \ldots$ mas U é ideal , logo $r_i.u \in U$, para todo i e então $\alpha \in \{b_0 + b_1t + \ldots \ ; \ b_i \in U\}$. É óbvio que $\{b_0 + b_1t + \ldots \ ; \ b_i \in U\} \subset UR[[t]]$.

2) Consequência imediata de *1)*.

3) Basta tomar o epimorfismo φ de $R[[t]]$ em $\frac{R}{U}[[t]]$ definido por $\varphi(a_0 + a_1t + a_2t^2 + \ldots) = \overline{a_0} + \overline{a_1}t + \overline{a_2}t^2 + \ldots$ e concluir, por *1)*, que $Ker(\varphi) = UR[[t]]$.

■

Agora vamos ver como se comportam os ideais primários com respeito a extensão $R[[t]]/R$.

Lema 2.2.6 : *Sejam R um anel noetheriano e* $\mathbf{q}$ *um ideal* $\mathbf{p}$*-primário. Então* $\mathbf{q}R[[t]]$ *é um ideal* $\mathbf{p}R[[t]]$*-primário.*

Demonstração : Seja n um número natural tal que $\mathbf{p}^n \subset \mathbf{q}$. Assim $(\mathbf{p}R[[t]])^n = \mathbf{p}^nR[[t]] \subset \mathbf{q}R[[t]] \subseteq \mathbf{p}R[[t]]$ e portanto $\mathbf{p}R[[t]]$ é o radical de $\mathbf{q}R[[t]]$.

Nos resta mostrar que se $\alpha\beta \in \mathbf{q}R[[t]]$ e $\alpha \notin \mathbf{p}R[[t]]$, então $\beta \in \mathbf{q}R[[t]]$. Tome $I =: (\mathbf{q} : \mathbf{p}) = \{r \in R; : r\mathbf{p} \subseteq \mathbf{q}\}$ e suponha que $\beta \in IR[[t]]$. Agora, como $\alpha = a_0 + a_1t + \ldots$ com $a_0, \ldots, a_{s-1} \in p$ e $a_s \notin p$, teremos que $a_i\beta \in \mathbf{q}R[[t]]$ para $i = 0, 1, \cdots, s-1$ e portanto $(a_st^s + a_{s+1}t^{s+1} + \ldots).\beta \in \mathbf{q}R[[t]]$. Assim podemos concluir que $a_s\beta \in \mathbf{q}R[[t]]$, com $a_s \notin \mathbf{p}$ e como $\mathbf{q}$ é $\mathbf{p}$ –primário segue, pelo lema 2.2.5 parte *1)*, que $\beta \in \mathbf{q}R[[t]]$.

Para concluir a demonstração basta mostrar que:

$(*)$ $\beta \in \mathbf{q}R[[t]]$ sempre que $\mathbf{q}$ é $\mathbf{p}$-primário, $\alpha\beta \in \mathbf{q}R[[t]]$ e $\alpha \notin \mathbf{p}R[[t]]$.

Vamos fazer a prova deste fato por indução sobre o menor número natural n tal que $\mathbf{p}^n \subseteq \mathbf{q}$. Observe que se $n = 1$ então $\mathbf{q} = \mathbf{p}$ e assim $\beta \in \mathbf{p}R[[t]]$ já que $\alpha \notin \mathbf{p}R[[t]]$.

Tome $n > 1$ e suponha que nossa afirmação $(*)$ é verdadeira para $n-1$. Sejam $\mathbf{q} \subseteq R$ satisfazendo todas as hipóteses de $(*)$ e n o menor inteiro tal que $\mathbf{p}^n \subseteq \mathbf{q}$. Considere $\mathbf{q}_1 = (\mathbf{q} : \mathbf{p})$, sabemos que $\mathbf{q}_1$ é $\mathbf{p}$-primário e que $\mathbf{q} \subseteq \mathbf{q}_1$. Assim $\alpha\beta \in \mathbf{q}_1R[[t]]$, pois $\alpha\beta \in \mathbf{q}R[[t]]$. Mais ainda, como $\mathbf{p}^n = \mathbf{p}\mathbf{p}^{n-1} \subseteq \mathbf{q}$ tem-se que $\mathbf{p}^{n-1} \subseteq \mathbf{q}_1$ e $\mathbf{p}^{n-2} \not\subseteq \mathbf{q}_1$ (caso contrário $\mathbf{p}^{n-1} \subseteq \mathbf{p}\mathbf{q}_1 \subseteq \mathbf{q}$). Logo, por hipótese de indução, $\beta \in \mathbf{q}_1R[[t]] = (\mathbf{q} : \mathbf{p})R[[t]]$, mas então, como já tínhamos feito no início da prova do lema, tem-se que $\beta \in \mathbf{q}R[[t]]$

■

Usando automorfismos, de $R[[t]]$, do tipo dado na Proposição 2.2.4 pode-se caracterizar quando um ideal de R é $\mathcal{D}$-ideal em termos de sua extensão a $R[[t]]$. Mais precisamente tem-se o seguinte resultado.

Lema 2.2.7 : *Seja R noetheriano contendo os números racionais e seja $\mathcal{D}$ uma família de derivações de R. Então o ideal U é um D-ideal se, e somente se, para toda $d \in D$, e^{td} deixa $UR[[t]]$ invariante.*

Prova: $\Leftarrow$) Suponha que para toda $d \in \mathcal{D}$ $UR[[t]]$ é invariante por e^{td} . Tome $a \in U$ e $d \in D$, então : $e^{td}(a) = a + a't + \ldots \in UR[[t]]$, onde $a' = d(a)$, logo, pelo lema 2.2.5, $a' \in U$, e portanto temos que U é um d-ideal. Portanto, como pegamos d arbitrariamente em $\mathcal{D}$ concluímos que U é um $\mathcal{D}$ –ideal.

$\Rightarrow$) Suponha que U seja um $\mathcal{D}$-ideal . Logo $d(U) \subset U$ para toda $d \in \mathcal{D}$. Assim dado $a \in U$ tem-se que $d(a) \in U$, $d^2(a) \in U$,..., ou seja, dado $a \in U$, $e^{td}(a) = a + d(a)t + \frac{d^2(a)}{2!}t^2 + \ldots \in UR[[t]]$, isto é, $e^{td}(UR[[t]]) \subseteq UR[[t]]$ para toda $d \in \mathcal{D}$.

■

O teorema a seguir nos mostra que se um ideal $\wp$ é primo associado de um $\mathcal{D}$-ideal U, então $\wp$ também será um $\mathcal{D}$-ideal, para ser mais preciso.

Teorema 2.2.8 : *Sejam R um anel noetheriano que contem o corpo dos números racionais e $\mathcal{D}$ uma família de derivações de R. Se U é um $\mathcal{D}$-ideal e $\wp_1, \wp_2, \ldots, \wp_s$. são seus ideais primos associados, então $\wp_1, \wp_2, \ldots, \wp_s$ são $\mathcal{D}$-ideais.*

Demonstração : Seja $U = Q_1 \cap Q_2 \cap \ldots \cap Q_s$ uma decomposição primária de U tal que, para todo i, Q_i é $\wp_i$-primário. Agora, pelo lema 2.2.6, temos que $UR[[t]] = Q_1R[[t]] \cap \ldots \cap Q_sR[[t]]$, onde $Q_iR[[t]]$ é $\wp_iR[[t]]$-primário para todo i. Portanto o conjunto dos primos associados de $UR[[t]]$ é $\{\wp_1R[[t]], \cdots, \wp_sR[[t]]\}$. Mas dada $d \in \mathcal{D}$ sabemos, pelo lema anterior, que $e^{td}(UR[[t]]) = UR[[t]]$ e assim

$$\{\wp_1R[[t]], \cdots, \wp_sR[[t]]\} = \{e^{td}(\wp_1R[[t]]), \cdots, e^{td}(\wp_sR[[t]])\},$$

isto é, para todo i existe j tal que $e^{td}(\wp_iR[[t]]) = \wp_jR[[t]]$. Agora dado $a \in \wp_i$, $e^{td}(a) = a + d(a)t + \ldots \in \wp_jR[[t]]$, donde temos $a \in \wp_j$ e portanto $\wp_i \subseteq \wp_j$. Mas $(e^{td})^{-1} = e^{-td}$ e usando o mesmo argumento temos que $\wp_j \subseteq \wp_i$. Portanto $\wp_i = e^{td}(\wp_i)$ para toda $d \in \mathcal{D}$. E, pelo lema 2.2.7, podemos concluir que $\wp_i$ é $\mathcal{D}$-ideal para todo i.
■

Como consequências imediatas deste último teorema obtem-se os seguintes resultados

Corolário 2.2.9 : *Sejam R um anel noetheriano que contem o corpo dos números racionais e $\mathcal{D}$ uma família de derivações de R. Se R não tem ideais primos próprios que são $\mathcal{D}$-ideais , então R é $\mathcal{D}$-simples.*

Corolário 2.2.10 : *Sejam R um anel noetheriano que contem o corpo dos números racionais e $\mathcal{D}$ uma família de derivações de R. Se R é $\mathcal{D}$-simples então R é domínio.*

Demonstração : Basta observar que (0) é $\mathcal{D}$ –ideal. ■

A relação entre a diferenciabilidade de um ideal primo $\wp$ de uma k–álgebra finitamente gerada $R = k[x_1, \ldots, x_n]$ e seu anel local $R_\wp$ é o que veremos no resultado a seguir.

Teorema 2.2.11 : *Seja $R = k[x_1, \ldots, x_n]$ uma k-álgebra finitamente gerada. Seja $\wp \subset R$ um ideal primo e $R_\wp$ o seu anel local . Então $\wp$ é diferencial se, e somente se, $\wp R_\wp$ é diferencial.*

Demonstração : Na verdade vamos demonstrar que $\wp$ não é diferencial se e somente se $\wp R_\wp$ não é diferencial.

Para iniciar a prova considere o seguinte ideal de R:

$$J = \{x \in R;\ rx = 0 \text{ para algum } r \notin \wp\}.$$

O ideal J satisfaz três propriedades que desempenham papel fundamental na prova do teorema. A primeira delas é que $J \subseteq \wp$, o que pode-se verificar diretamente da definição de J. A segunda é que se d é uma derivação de R então J é um d-ideal. De fato tomando $x \in J$ temos que existe $r \notin \wp$ tal que $rx = 0$, calculando $rd(rx)$ tem-se $0 = rd(rx) = r^2 d(x) + rxd(r) = r^2 d(x)$ com $r^2 \notin \wp$ e assim $d(x) \in J$. A terceira propriedade diz respeito ao seguinte isomorfismo de anéis $\varphi : R_\wp \to (\frac{R}{J})_{\frac{\wp}{J}}$ definido por $\varphi(\frac{x}{s}) = \varphi(\frac{x+J}{s+J}) = \varphi(\frac{\overline{x}}{\overline{s}})$. Claramente φ está bem definida e é epimorfismo. Vamos ver que é injetora, de fato, se $\varphi(\frac{x}{s}) = \frac{\overline{0}}{\overline{1}} = \frac{\overline{x}}{\overline{s}}$ então existe $r_1 \notin \wp$ tal que $\overline{r_1 x} = \overline{0}$, isto é, $r_1 x \in J$ e assim existe $r_2 \notin \wp$ tal que $r_1 r_2 x = 0$, logo $\frac{x}{s} = \frac{xr_1r_2}{sr_1r_2} = \frac{0}{1}$, isto é, $Ker(\varphi) = 0$ e φ é injetora. Esta terceira propriedade nos diz que podemos identificar $R_\wp$ com $(\frac{R}{J})_{\frac{\wp}{J}}$.

Agora provadas as três propriedades a respeito de J iniciamos a prova propriamente dita do teorema assumindo primeiro que $\wp$ não é diferencial, logo existe uma derivação d de R tal que $d(\wp) \not\subseteq \wp$. Como $d(J) \subseteq J$, de modo natural, d induz uma derivação $\tilde{d}$ de $\frac{R}{J}$ definida por $\tilde{d}(r+J) = d(r)+J$. Desde que $d(\wp) \not\subseteq \wp$ tem-se que $\tilde{d}(\frac{\wp}{J}) \not\subseteq \frac{\wp}{J}$. Mas, pela proposição 2.1.2, podemos estender de uma única maneira $\tilde{d}$ para $(\frac{R}{J})_{\frac{\wp}{J}} = R_\wp$ (também denotada por $\tilde{d}$) e mais ainda $\wp R_\wp$ não é $\tilde{d}$-ideal e assim temos provado uma das implicações do teorema.

Para mostrar a recíproca seja d' uma derivação de $R_\wp$ tal que $d'(\wp R_\wp) \not\subseteq \wp R_\wp$. Chame $\frac{R}{J} = k[\overline{x_1}, \cdots, \overline{x_n}]$ e como $(\frac{R}{J})_{\frac{\wp}{J}} = R_\wp$ tem-se que $d'(\overline{x_i}) = \frac{u_i}{v_i}$ com $u_i, v_i \in R$ e $v_i \notin \wp$. Tome $v = \prod v_i$ e trocando d' por vd' podemos supor que, para todo i, $d'(\overline{x_i}) \in \frac{R}{J}$, isto é, podemos supor que d' é derivação de $\frac{R}{J}$. Seja $(0) = q_1 \cap \ldots \cap q_s$ uma decomposição primária minimal de (0) em R. Tome $t \in \mathbb{N}$, $1 \leq t \leq s$, tal que $q_i \subset \wp$ se $i \leq t$ e $q_i \not\subseteq \wp$ se $i > t$. Afirmamos que $J = q_1 \cap \cdots \cap q_t$, de fato, se $x \in J$ tome $r \notin \wp$ tal que $0 = rx \in q_i$ observe que q_i é primário, $r \notin \wp$ e para $i \leq t$ $\sqrt{q_i} \subseteq \wp$, portanto $x \in q_i$ para todo $i \leq t$, isto é, $J \subseteq q_1 \cap \cdots \cap q_t$. Agora como $q_{t+1} \cap \cdots \cap q_s \not\subseteq \wp$, tome $a \in q_{t+1} \cap \cdots \cap q_s$ e $a \notin \wp$ e observe que $a.q_1 \cap \cdots \cap q_t = (0)$ e portanto $q_1 \cap \cdots \cap q_t \subseteq J$.

Considere $B = k[X_1, \cdots, X_n]$ o anel de polinômios a n variáveis sobre k e tome os seguintes epimorfismos de anéis, σ de B em R tal que $\sigma(X_i) = x_i$ e ϕ de B em $\frac{R}{J}$ tal que $\phi(X_i) = \overline{x_i}$ (na verdade $\phi = \pi \circ \sigma$ onde π é a projeção canônica de R em $\frac{R}{J}$). Agora para cada $i,:: 1 \leq i \leq s$, seja q_i' ideal de B tal que $\phi(q_i') = q_i$. É bastante simples verificar que $Ker(\sigma) = U = q_1' \cap \cdots \cap q_s'$ e que $Ker(\phi) = \mathcal{N} = q_1' \cap \cdots \cap q_t'$. Por outro lado sabemos que d' é derivação de $\frac{R}{J}$ e portanto para cada $i,: \ 1 \leq i \leq n$ podemos escrever $d'(\overline{x_i}) = h_i + J$ onde

$h_i = h_i(X_1,\cdots,X_n) \in B$. Defina a derivação δ de B dada por $\delta = \sum_{i=1}^{n} h_i \frac{\partial}{\partial X_i}$. Afirmamos que $\delta(\mathcal{N}) \subseteq \mathcal{N}$, de fato, tome $g = g(X_1,\cdots,X_n) \in \mathcal{N}$, logo:

$0 = \phi(g) = g(\phi(X_1),\cdots\phi)(X_n)) = g(\overline{x_1},\cdots,\overline{x_n})$. Portanto $0 = d'(g(\overline{x_1},\cdots,\overline{x_n})$ e então:

$$0 = \sum_{i=1}^{n} d'(\overline{x_i}) \frac{\partial g}{\partial X_i}(\overline{x_1},\cdots,\overline{x_n})$$

$$= \sum_{i=1}^{n} (h_i + J) \frac{\partial g}{\partial X_i}(\overline{x_1},\cdots,\overline{x_n})$$

$$= \phi(\sum_{i=1}^{n} h_i \frac{\partial g}{\partial X_i}(X_1,\cdots,X_n)) = \phi(\delta(g)).$$

Portanto $\delta(g) \in \mathcal{N}$ e assim δ induz a derivação d', isto é, $d'(x+J) = \delta(x) + J$. Agora tomando $\wp'$ o ideal primo de B tal que $\phi(\wp') = \wp$, temos que $\delta(\wp') \not\subseteq \wp'$ já que $d'(\wp) \not\subseteq \wp$.

Seja $a \in q'_{t+1} \cap \cdots \cap q'_s$ e $a \notin \wp'$ e considere $\overline{\delta} = a.\delta$. Afirmamos que $\overline{\delta}(U) \subseteq U$, onde $U = Ker(\sigma)$, de fato, se $x \in U$ tem-se que $x \in \mathcal{N}$ e $\delta(x) \in \mathcal{N}$ também, mas $\overline{\delta}(x) = a\delta(x) \in a\mathcal{N} \subseteq U$. Finalmente temos que $\overline{\delta}$ induz uma derivação D, em $\frac{B}{U} = R$, de tal forma que $D(\wp) \not\subseteq \wp$, já que $\overline{\delta}(\wp')) \not\subseteq \wp'$. E portanto temos o que queríamos.

■

O lema que veremos a seguir é um resultado clássico da teoria das derivações. Ele é devido a O. Zariski e é usado de maneira fundamental na prova do teorema de Seindenberg.

Lema (Zariski) 2.2.12 : *Seja R um anel noetheriano que é completo semi-local e contem os números racionais. Seja* **m** *o radical de Jacobson de R. Assuma que exista uma derivação D de R tal que $D(x)$ é uma unidade em R para algum $x \in \mathbf{m}$. Então R contém um subanel R_1 satisfazendo as seguintes propriedades :*

a) D é uma R_1-derivação

b) Sendo (x) o ideal principal gerado por x, tem-se que $R_1 \simeq \frac{R}{(x)}$

c) O elemento x é analiticamente independente sobre R_1 ;

d) $R = R_1[[x]]$.

Demonstração : Em primeiro lugar desde que $a = D(x) \in R^*$, trocando D por $a^{-1}D$ podemos assumir que $D(x) = 1$.

Agora defina $e^{-xD} : R \to R$ por $e^{-xD}(r) = r - xD(r) + \frac{x^2}{2!}D^2(r) - \ldots$. Por R ser completo em relação a topologia **m**-ádica e $x \in \mathbf{m}$ temos que e^{-xD} é uma aplicação bem definida já que a sequência de somas parciais $S_n(r) = \sum_{i=0}^{n} (-1)^i \frac{D^i(r)x^i}{i!}$ é de Cauchy. A prova de que e^{-xD} é um endomorfismo do anel R é completamente análoga à feita, de fato parecido, na proposição 2.2.4.

Tome R_1 como sendo a imagem de e^{-xD}, isto é, $R_1 = Im(e^{-xD})$. Como e^{-xD} é um endomorfismo de R já temos que R_1 é um subanel de R. Agora vamos mostrar que D é uma R_1-derivação. Dado $r_1 \in R_1 = \mathrm{Im}(e^{-xD})$, então $r_1 = e^{-xD}(r)$ para algum $r \in R$, ou seja $r_1 = r - xD(r) + \frac{x^2}{2!}D^2(r) - \ldots$ e assim temos que :

$$D(r_1) = D(r - xD(r) + \frac{x^2}{2!}D^2(r) - \ldots) = D(r) - D(xD(r)) + D(\frac{x^2}{2!}D^2(r)) - \ldots .$$

Mas $D(x) = 1$, por hipótese, logo $D(r_1) = D(r) - D(r) - xD^2(r) + xD^2(r) + \frac{x^2}{2!}D^3(r) - \ldots = 0$ e portanto D é uma R_1-derivação.

Afirmamos que $\ker(e^{-xD}) = (x) =$ ideal principal gerado por x. De fato, dado $\alpha \in \ker(e^{-xD})$, tem-se que $e^{-xD}(\alpha) = \alpha - xD(\alpha) + \frac{x^2}{2!}D^2(\alpha) - \ldots = 0$, logo temos que $\alpha = xD(\alpha) - \frac{x^2}{2!}D^2(\alpha) + \ldots = x.\beta$ com $\beta \in R$, isto é, $\ker(e^{-xD}) \subseteq (x)$. Por outro lado $D(x) = 1$ e assim $e^{-xD}(x) = 0$ e portanto $(x) \subseteq \ker(e^{-xD})$.

Como $R_1 = Im(e^{-xD})$ e $\ker(e^{-xD}) = (x)$ já temos que $R_1 \simeq \frac{R}{(x)}$. Portanto acabamos de mostrar os itens *a)* e *c)*.

Iniciamos a prova dos outros itens com a seguinte afirmação: se $r_1 \in R_1$ então $e^{-xD}(r_1) = r_1$. De fato, pois neste caso $r_1 = e^{-xD}(r) = r + x\beta$ e então $e^{-xD}(r_1) = e^{-xD}(r)$, já que $(x) \subseteq \ker(e^{-xD})$.

Antes de mostrarmos o item *c)* vamos provar que x não é um divisor de zero de R. Seja $b \in R$ tal que $x.b = 0$, logo temos $D(x.b) = D(x).b + x.D(b) = b + x.D(b) = 0$, ou seja $b = -x.D(b)$. Aplicando D nesta igualdade temos:

$D(b) = D(-x).D(b) - x.D^2(b) = -D(b) - x.D^2(b)$, ou seja $2.D(b) = -x.D^2(b)$, mas $\mathbb{Q} \subseteq R$, logo $D(b) = \frac{-x}{2}.D^2(b)$, aplicando novamente D nesta igualdade temos: $D^2(b) = D\left(\frac{-x}{2}\right).D^2(b) - \frac{x}{2}.D^3(b) = \frac{-1}{2}.D^2(b) - \frac{x}{2}.D^3(b)$, assim $\frac{3}{2}.D^2(b) = -\frac{x}{2}.D^3(b)$, e como $\mathbb{Q} \subseteq R$, então $D^2(b) = -\frac{x}{3}.D^3(b)$. Repetindo este processo indutivo muito simples concluirmos que $D^n(b) = -\frac{x}{n+1}.D^{n+1}(b)$, para $n \in \mathbb{N}$. Agora como $b = -x.D(b)$ e $D^n(b) = -\frac{x}{n+1}.D^{n+1}(b)$, então:

$b = \frac{x^2}{2}.D^2(b) = \frac{x^2}{2}.\left(-\frac{x}{3}.D^3(b)\right) = -\frac{x^3}{2.3}.D^3(b) = \ldots = (-1)^n\frac{x^n}{n!}.D^n(b)$, ou seja $b \in x^n.R$, para todo n, mas $\bigcap x^n.R = (0)$ já que $x \in \mathbf{m}$ e R é noetheriano e portanto $b = 0$.

Agora sabendo que x não é um divisor de zero de R mostraremos que x é analiticamente independente sobre R_1.

Seja $\sum_{i=0}^{\infty} a_i x^i = 0$, onde $a_i \in R_1$, para todo i. Vamos mostrar que $a_i = 0$ para todo i, e assim temos que x é analiticamente independente sobre R_1. Aplicando o operador e^{-xD} na igualdade $\sum a_i x^i = 0$ temos o seguinte: $e^{-xD}(a_0) + e^{-xD}(x\beta) = 0$, onde $\beta = \sum_{i=1}^{\infty} a_i x^i$, agora a restrição de e^{-xD} em R_1 é a aplicação identidade e $\ker(e^{-xD}) = (x)$, logo de nossa última

igualdade temos que $a_0 = 0$. Portanto temos que $x(a_1 + a_2.x + \ldots) = 0$, mas sabemos que x não é um divisor de zero em R, logo $a_1 + a_2.x + \ldots = 0$, e aplicando e^{-xD} nesta igualdade vemos, de modo análogo, que $a_1 = 0$, e assim temos que $x^2(a_2 + a_3.x + \ldots) = 0$. Repetindo este processo vemos que $a_i = 0$ para todo i, e temos o que queríamos.

Prova do item *d)*: Claro que $R_1[[x]] \subseteq R$, pois R é completo ($x \in \mathbf{m}$ é analiticamente independente sobre R_1 e $R_1 \subseteq R$).

Agora mostraremos que $R \subseteq R_1[[x]]$. Vejamos :

Como $R_1 = \mathrm{Im}(e^{-xD})$, a restrição de e^{-xD} em R_1 é a aplicação identidade, e $\ker(e^{-xD}) = xR$, temos que: $R = R_1 \oplus xR$

Primeiramente vejamos que dados $\alpha \in R$ e $n \in \mathbb{N}$ existem $\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots \in R_1$ tais que $\alpha - \sum_{i=0}^{n} x^i \alpha_i \in x^{n+1}R$.

De fato, para $n = 0$, $\alpha = \alpha_0 + x\beta_1$; $\alpha_0 \in R_1$ e $\beta_1 \in R$, implica que $\alpha - \alpha_0 \in xR_1$. Logo já escolhemos α_0.

Agora suponhamos $n \geq 1$ e que já tenhamos escolhido $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\} \subseteq R_1$ tais que $\gamma = \alpha - \sum_{i=0}^{n-1} x^i \alpha_i \in x^n R$. Mas $x^n R = x^n(R_1 \oplus xR) = x^n R_1 \oplus x^{n+1}R$, ou seja temos que $\gamma \in x^n R_1 \oplus x^{n+1}R$, logo existem $\alpha_n \in R_1$ e $\beta_n \in R$ tais que $\gamma = \alpha - \sum_{i=0}^{n-1} x^i \alpha_i = x^n \alpha_n + x^{n+1}\beta_n$, e assim encontramos $\alpha_n \in R_1$ tal que $\alpha - \sum_{i=0}^{n} x^i \alpha_i = x^{n+1}\beta_n \in x^{n+1}R$.

Usando o fato de que R é completo temos que $\alpha = \sum_{i=0}^{\infty} x^i \alpha_i$, e portanto $\alpha \in R_1[[x]]$, e assim vimos que $R \subseteq R_1[[x]]$.

E com isso mostramos o lema de Zariski.

■

Nosso próximo resultado trata de soluções de um sistema linear em um anel local R, o qual é importante para a prova de resultados subsequentes.

Lema 2.2.13 : *Seja R um anel local com ideal maximal $\mathbf{m}$ e $\hat{R}$ seu completamento. Seja $\sum A_{ij}Z_j + B_i = 0$ um número finito de m equações em um número finito, n de indeterminadas Z_j com coeficientes em R. Então se o sistema tem uma solução em $\hat{R}$, terá também uma solução em R.*

Demonstração: Para o caso em que $m = 1$ temos a seguinte expressão: $A_{11}Z_1 + A_{12}Z_2 + \ldots + A_{1n}Z_n + B_1 = 0$, onde $A_{11}, \ldots, A_{1n}, B_1 \in R$, que por hipótese tem solução em $\hat{R}$, ou seja existem $\hat{z}_1, \ldots, \hat{z}_n \in \hat{R}$, tais que $A_{11}\hat{z}_1 + A_{12}\hat{z}_2 + \ldots + A_{1n}\hat{z}_n = -B_1 \in R$, e o resultado segue do fato de que para todo ideal J de R temos $\hat{R}J \cap R = J$. Pois tomando o ideal J de R que é gerado por $A_{11}, \ldots, A_{1n}$, então $A_{11}\hat{z}_1 + A_{12}\hat{z}_2 + \ldots + A_{1n}z_n \in \hat{R}J$ e $A_{11}\hat{z}_1 + A_{12}\hat{z}_2 + \ldots + A_{1n}\hat{z}_n = -B_1 \in R$, e portanto existem $z_1, \cdots, z_n \in A$ tais que $A_{11}z_1 + A_{12}z_2 + \ldots + A_{1n}z_n = -B_1 \in J$. E assim temos o que queríamos.

Vejamos agora o caso em que $m > 1$. Neste caso introduziremos uma indeterminada $\mathcal{U}_i$ para cada equação (onde $i = 1,\ldots,m$), e consideraremos a seguinte equação: $(*)\ \sum_{j=1}^{n}\left(\sum_{i=1}^{m}A_{ij}.\mathcal{U}_i\right)Z_j + \sum_{i=1}^{m}B_i.\mathcal{U}_i = 0$. Consideremos agora no anel $R[\mathcal{U}_1,\ldots,\mathcal{U}_m]$ o ideal primo $\wp = (\mathbf{m},\mathcal{U}_1,\ldots,\mathcal{U}_m)$. Tomando o anel local $B = R[\mathcal{U}_1,\ldots,\mathcal{U}_m]_{\wp}$ tem-se que $\hat{R} \subseteq \hat{B}$. Logo a equação $(*)$ tem solução em $\hat{B}$, pois por hipótese a equação $(*)$ tem solução em $\hat{R}$, e assim tem uma solução em B. Sendo $g_1,\ldots,g_n$ uma solução de $(*)$, podemos escrever $g_j = \frac{h_{j0}+\ldots}{d_0+\ldots}$, onde $h_{j0}+\ldots, d_0+\ldots \in R[\mathcal{U}_1,\ldots,\mathcal{U}_m]$, $h_{j0}, d_0 \in R$, $d_0 \notin \mathbf{m}$, isto é, $d_0 \in R^*$ e os termos omitidos estão em $R[\mathcal{U}_1,\ldots,\mathcal{U}_m].(\mathcal{U}_1,\ldots,\mathcal{U}_m)$. Então teremos que: $\sum(\sum A_{ij}.\mathcal{U}_i)(h_{j0}+\ldots) + \sum B_i.\mathcal{U}_i(d_0+\ldots) = 0$. Tomando os termos lineares apenas temos que : $(**)\ \sum(\sum A_{ij}.\mathcal{U}_i).h_{j0} + \sum(B_i.\mathcal{U}_i).d_0 = 0$, e assim se para cada j fizermos $U_i = \delta_{ij}$ em $(**)$ (δ_{ij} é o δ de Kronecker) vamos ter que $\frac{h_{j0}}{d_0}$, onde $j = 1,\ldots,n$, é uma solução do sistema original equações com queríamos.

■

Com este resultado podemos obter o seguinte teorema que diz respeito a diferenciabilidade de $\mathbf{m}\hat{R}_{\mathbf{m}}$, onde $R = k[x_1,\ldots,x_n]$ e $\mathbf{m}$ é um ideal primo em R.

Teorema 2.2.14 : *Sejam $R = k[x_1,\ldots,x_n]$ uma k–álgebra finitamente gerada sobre o corpo k, $\mathbf{m}$ um ideal primo em R e $\hat{R}_{\mathbf{m}}$ o completamento de $R_{\mathbf{m}}$. Se $\mathbf{m}R_{\mathbf{m}}$ é diferencial (para qualquer família de derivações de R_m) , então $\hat{R}_{\mathbf{m}}.m$ também é diferencial (para a extensão da família de derivações de $R_{\mathbf{m}}$).*

Demonstração : Suponha que exista uma derivação D de $\hat{R}_{\mathbf{m}}$ tal que $D(\mathbf{m}) \not\subseteq \mathbf{m}.\hat{R}_{\mathbf{m}}$. Seja $n = \{s \mid s \in R \text{ e } sx = 0 \text{ para algum } x \in R \setminus \mathbf{m}\}$. Então, como já vimos na prova do teorema 2.2.11, $R_{\mathbf{m}} = \left(\frac{k[x]}{n}\right)_{\frac{\mathbf{m}}{n}}$, e assim podemos assumir $n = 0$. Se $a \in \mathbf{m}$, com $d(a) \notin \mathbf{m}.\hat{R}_{\mathbf{m}}$, podemos supor $a = x_1$ e, mudando D se necessário, que $D(x_1) = 1$. Seja $k[x] = \frac{k[X]}{I}$, onde $k[X] = k[X_1,\ldots,X_n]$, e sejam $f_1,\ldots,f_s$ uma base para o ideal I. Sendo $\overline{D} = \sum_{i=1}^{n}h_i.\frac{\partial}{\partial X_i}$ uma derivação de $k[X_1,\ldots,X_n]$, temos que $\overline{D}$ induz uma derivação D de $\frac{k[X_1,\ldots,X_n]}{I}$, onde $D(\bar{g}) = D(g+I) = \overline{D}(g)+I$; quando $\overline{D}(I) \subseteq I$. Então temos que toda solução em Σ do sistema $\sum\frac{\partial f_i}{\partial X_j}.Z_j = 0$ nos dará uma k-derivação de Σ. Agora este sistema $\sum\frac{\partial f_i}{\partial X_j}.x_j' = 0$ tem uma solução em $\hat{R}_{\mathbf{m}}$ com $D(x_1) = 1$, o lema 2.2.13 nos diz que este sistema tem uma solução em $R_{\mathbf{m}}$ com $D(x_1) = 1$, e está provado o teorema.

■

Como consequência deste teorema obtemos um resultado que requer a seguinte definição:

Definição 2.2.15 : *Seja R o anel de coordenadas de uma variedade afim V sobre um corpo de k de característica zero , e seja $\wp$ um ideal primo não diferenciável de R. Pelo lema de Zariski $\hat{R}_\wp$ é da forma $\hat{R}_1[[t]]$. Dizemos que V é analiticamente um produto em $U = V(p)$ que é a subvariedade de V determinada por $\wp$, se $\hat{R}_\wp$ é da forma $\hat{R}_1[[t]]$, onde $\hat{R}_1$ é um anel local completo com $\dim \hat{R}_1 = \dim \hat{R} - 1$.*

Agora sim podemos enunciar o corolário que é muito importante para demonstrarmos o desejado teorema 2.2.17.

Corolário 2.2.16 : *Seja R um anel de coordenadas de uma variedade afim irredutível V sobre um corpo k de característica zero. Seja $\mathcal{U}$ uma subvariedade irredutível de V sobre k. Então V é analiticamente um produto sobre $\mathcal{U}$ se, e somente se, o ideal de $\mathcal{U}$ em R não é diferencial.*

Demonstração : Tome $\wp$ o ideal primo de R que determina $\mathcal{U}$.

$\Rightarrow$) Sabemos que V é analiticamente um produto sobre $\mathcal{U}$, ou seja, $\hat{R}_\wp$ é da forma $\hat{R}_1[[u]]$. A derivação $D = \frac{\partial}{\partial u}$ é tal que $D(a) = 0$, $a \in \hat{R}_1$, e $D(u) = 1$. O fato de u ser analiticamente independente sobre $\hat{R}_1$ nos garante que u não é uma unidade em $\hat{R}_\wp$, logo $u \in \wp.\hat{R}_\wp$ e, como $D(u) = 1$, temos que $m.\hat{R}_m$ não é diferencial. Assim o teorema anterior nos garante que $\wp.R_\wp$ também não é diferencial. Portanto pelo teorema 2.2.11 temos que $\wp$ não é diferencial.

$\Leftarrow$) Sabemos que o ideal $\wp$ de não é diferencial. Assim $\wp R_\wp$ não é. Agora o lema de Zariski nos diz que $\hat{R}_\wp = \hat{R}_1[[u]]$ com u analiticamente independente sobre o anel $\hat{R}_1$, e temos o que queríamos.

■

Feitas todas estas preparações encerramos esta seção enunciando e demonstrando o resultado de Seidenberg que falamos no início deste capítulo.

Teorema 2.2.17: *Sejam $R = k[x_1, \ldots, x_n]$ uma k-álgebra finitamente gerada sobre o corpo k e $\wp$ um ideal primo não minimal em R tal que $R_\wp$ é regular. Então $\wp$ não é diferencial.*

Demonstração : Suponha primeiro que $R = k[x_1, \ldots, x_n]$ é o anel de uma variedade

irredutível V sobre k, então temos que $\mathcal{U} = \mathcal{V}(\wp)$ é uma subvariedade de V. Como $\wp$ é um ideal primo não minimal, temos que o $ht(\wp) \geq 1$. Mas ,evidentemente, $\hat{R}_\wp$ contém um corpo, e assim a proposição 1.3.6 no garante que $\hat{R}_\wp \simeq K[[x_1, \ldots, x_n]]$, onde K é o corpo de resíduos $\hat{R}_\wp$ e $n \geq 1$. Portanto temos que V é analiticamente um produto sobre $\mathcal{U} = \mathcal{V}(\wp)$ e, pelo corolário anterior $\wp$ não é diferencial, e temos o que queríamos.

No caso em que V não é irredutível fazemos o seguinte: tomamos um primo associado minimal, $\wp_1$, de (0) em R, de tal forma que $\wp_1 \subset \wp$ e trocamos R por $\overline{R} = \frac{R}{\wp}$ e reduzimos ao caso anterior, já que, pelo teorema 2.2.8, $\wp_1$ é D-ideal qualquer que seja a derivação de R.

■

Concluímos o parágrafo apresentando o resultado que caracteriza o fato de uma k-álgebra finita R ser regular em termos de suas derivações.

Corolário 2.2.18 : *Seja R um domínio que é uma k-álgebra finitamente gerada sobre o corpo k. Então: R é regular se e somente se R é simples.*

Demonstração : $\Rightarrow$) Seja $\wp$ um ideal primo não nulo de R. Por hipótese tem-se que $R_\wp$ é regular e assim o teorema anterior nos garante que $\wp R_\wp$ não é diferencial. Agora usando o teorema 2.2.11 tem-se que $\wp$ não é diferencial, logo, pelo teorema 2.2.8, R é simples.

$\Leftarrow$) Seja $\wp$ um ideal primo não nulo de R. Por hipótese tem-se que $\wp R_\wp$ não é diferencial e assim, pelo corolário 2.2.16, $\hat{R}_\wp$ é regular e então $R_\wp$ também é (teorema 1.3.3).

■

2.3 Derivações em Anéis Regulares Locais de Tipo Finitamente Gerados

Nesta seção apresentaremos um resultado demostrado por R. Hart, em [4]. Este resultado é para o caso em que $R = k[x_1, \ldots, x_n]$ é o anel de coordenadas de uma variedade irredutível V e $\mathbf{m}$ é o ideal maximal de um ponto regular de V é mais geral que o resultado de Seidenberg (teorema 2.2.17), pois ele diz que $R_\mathbf{m}$ é d-simples para alguma derivação, d, de $R_\mathbf{m}$

Antes de vermos este resultado vejamos o seguinte.

Seja K um corpo de característica zero , e $K[[t]]$ o anel série de potência. Dado um elemento z em $K[[t]]$ diferente da unidade definimos $log(1+z)$ pela seguinte série de

potências : $log(1+z) = z - \frac{1}{2}z^2 + \frac{1}{3}z^3 - \ldots$. Sejam $\beta_1, \beta_2, \ldots$ elementos não nulos de K, e coloquemos, indutivamente, $\ell_1 = t$, $\ell_{i+1} = log(1 + \beta_i \ell_i)$. Dessa forma temos o seguinte lema:

Lema 2.3.1 : *As séries de potência* $\ell_1, \ell_2, \ell_3, \ldots$ *são algebricamente independentes sobre* K.

Demonstração : Sejam $L_0 = K$, e $L_i = K(\ell_1, \ell_2, \ldots, \ell_i)$ para $i \geq 1$.

Assim para provarmos o que queremos basta mostrarmos que, para todo i, ℓ_{i+1} não é algébrico sobre $L_i = K(\ell_1, \ell_2, \ldots, \ell_i)$, pois sabemos que ℓ_{i+1} é algébrico sobre $L_i = K(\ell_1, \ell_2, \ldots, \ell_i)$ se, e somente se, $\{\ell_1, \ell_2, \ldots, \ell_i, \ell_{i+1}\}$ não é algebricamente independente sobre K.

Então vejamos que ℓ_{i+1} não é algébrico sobre $L_i = K(\ell_1, \ell_2, \ldots, \ell_i)$, para todo i.

Para $j \leq i$, supomos, por indução, que ℓ_j não seja algébrico sobre L_{j-1}. Isso claramente é válido para $i = 1$, pois $\ell_1 = t$ não é algébrico sobre $L_0 = K$.

Se $\ell_{i+1} \in L_i$, temos que $f(\ell_1, \ell_2, \ldots, \ell_i).\ell_{i+1} = g(\ell_1, \ell_2, \ldots, \ell_i)$, onde f e g são polinômios.

Derivando esta igualdade com respeito a t temos :

$$\frac{f^2}{y_1.y_2\ldots y_i} = \sum_{j=1}^{i} f.\frac{\partial g}{\partial y_j}.\frac{1}{y_1.y_2\ldots y_{j-1}} - \sum_{j=1}^{i} g.\frac{\partial f}{\partial y_j}.\frac{1}{y_1.y_2\ldots y_{j-1}} \qquad \text{(eq.1)}$$

onde $y_j = \frac{1 + \beta_j \ell_j}{\beta_j}$.

Por nossa hipótese de indução sabemos que $\ell_1, \ell_2, \ldots, \ell_i$ são algebricamente independentes, logo $y_1, y_2, \ldots, y_i$ também são algebricamente independentes.

Podemos escrever a (eq.1) da seguinte maneira :

$$\frac{f^2}{y_i} = \sum_{j=1}^{i} y_j.y_{j+1}\ldots y_{i-1}.f.\frac{\partial g}{\partial y_j} - \sum_{j=1}^{i} y_j.y_{j+1}\ldots y_{i-1}.g.\frac{\partial f}{\partial y_j}$$

Assim vemos que y_i divide f no anel de polinômios $K[y_1, y_2, \ldots, y_i]$.

Podemos supor que y_i não divide g , ou, caso contrário, que $f = g = 0$.

Agora y_i divide f^2, logo y_i divide $\sum_{j=1}^{i} y_j.y_{j+1}\ldots y_{i-1}.g.\frac{\partial f}{\partial y_j}$.

Para $j \neq i$, temos que y_i divide $\frac{\partial f}{\partial y_j}$, pois y_i divide f, e portanto y_i divide o termo $g.\frac{\partial f}{\partial y_j}$, e como y_i não divide g, temos que y_i divide $\frac{\partial f}{\partial y_j}$, e assim y_i^2 divide f.

Repetindo o processo temos que y_i^3 divide f , y_i^4 divide f, e assim por diante. Isso significa que $f = 0$, ou seja, vimos que não existe f não nula tal que

$f(\ell_1, \ell_2, \ldots, \ell_i) \,.\, \ell_{i+1} = g(\ell_1, \ell_2, \ldots, \ell_i)$.

E portanto ℓ_{i+1} não pertence a L_i.

Se ℓ_{i+1} é algébrico sobre L_i , seja n minimal tal que :

$\ell_{i+1}^n + a_{n-1}\ell_{i+1}^{n-1} + \ldots + a_1\ell_{i+1} + a_0 = 0$, onde $a_r \in L_i$, $r = 0, 1, \ldots, n-1$.

Derivando esta equação temos :

$\ell_{i+1}^{n-1}\left(\frac{n\beta_i\ell_i'}{1+\beta_i\ell_i}+a_{n-1}'\right)+\ldots+a_0'=0$

Como os coeficientes dessa equação estão em L_i e n foi tomado minimal temos que:

$\frac{n\beta_i\ell_i'}{1+\beta_i\ell_i}+a_{n-1}'=0$, e isso implica que : $-a_{n-1}'=\frac{n\beta_i\ell_i'}{1+\beta_i\ell_i}=n.\ell_{i+1}'$

Logo $-a_{n-1}'$ difere de $n.\ell_{i+1}$ por mais de um elemento de K, pois eles têm derivadas iguais. Assim $\ell_{i+1}\in L_i$, que é um absurdo pelo que vimos anteriormente.

Portanto ℓ_{i+1} não é algébrico sobre L_i, e assim temos que $\ell_1,\ell_2,\ell_3,\ldots$ são algebricamente independentes sobre K.

■

Agora, para finalizarmos esta seção, vejamos o resultado obtido por Hart, em [4], que é o seguinte.

Teorema 2.3.2 : *Seja R um anel local em um ponto simples de uma variedade irredutível sobre um corpo k de característica zero. Então existe uma k-derivação $d : R \to R$ tal que nenhum ideal próprio em R é um d-ideal.*

Demonstração: Sabemos que R é do tipo $R=S_{\mathfrak{m}}$, onde $S=k[x_1,\ldots,x_n]$ é o anel de coordenadas da variedade irredutível V e **m** é o ideal maximal de S correspondente ao ponto tomado.

Seja $r=dim(R)=dim(S)$, assim podemos supor que $x_1,\ldots,x_r$ são algebricamente independentes, ou seja, R é algébrico sobre $k[x_1,\ldots,x_r]$. Sejam K o corpo isomorfo a $\frac{R}{MR}$ e $y_i=x_i-a_i$, com $a_1,\ldots,a_r\in K$. Assim pelo teorema 1.3.5 temos que o completamento $\hat{R}$ de R tem a forma $K[[y_1,\ldots,y_r]]$.

Se $a_i\in k$, para todo i ,então podemos substituir x_i por x_i-a_i e assumir $a_i=0$. Em particular podemos assumir $a_i\neq -1$, para todo i .

Sejam $\ell_1=t$, $\ell_{i+1}=log(1+\beta_i\ell_i)$ se $i\geq 1$,onde $\beta_i=\frac{1}{1+a_i}$, e definamos o homomorfismo contínuo $f:\hat{R}\to K[[t]]$ dado por $f(y_i)=\ell_i$.

Como , pelo lema anterior , $dim\, f(R)\geq r$, então temos que $dim\, f(R)=r$. Por R ser um domínio então temos que $R\cap kerf=0$ ou $dim\,\frac{R}{R\cap kerf}<r$. Mas $f(R)$ é isomorfo a $\frac{R}{R\cap kerf}$ logo devemos ter $R\cap kerf=0$.

Agora vamos definir uma K-derivação da seguinte maneira:

$d:\hat{R}\to\hat{R}$, onde $d(y_1)=1$ e $d(y_{i+1})=\frac{(\beta_1\ldots\ldots\beta_i)}{(1+\beta_1\ell_1)\ldots(1+\beta_i\ell_i)}=\frac{1}{(1+x_1)\ldots(1+x_i)}$

Assim d leva $k[x_1,\ldots,x_r]$ em R . Seja Z um elemento de R , como R é algébrico sobre $k[x_1,\ldots,x_r]$ então Z é algébrico sobre $k[x_1,\ldots,x_r]$, e assim dZ pertence ao corpo quociente de R, e portanto dZ também pertence a $\hat{R}$. E assim $dZ\in R$, ou seja , temos que $dR\subset R$.

Como vimos anteriormente R é isomorfo a uma subalgebra fR de $K[[t]]$, e nesse

isomorfismo elementos diferentes da unidade são levados em elementos diferentes da unidade. Agora do fato que :

$$\frac{\partial \ell_{i+1}}{\partial t} = \frac{(\beta_1 \ldots \ldots \beta_i)}{(1+\beta_1\ell_1)\ldots(1+\beta_i\ell_i)} \quad \text{e} \quad \frac{\partial \ell_1}{\partial t} = 1$$

a derivação induzida por d em fR é a própria $\frac{\partial}{\partial t}$. Mas temos que dado um elemento não nulo de $K[[t]]$ ele é levado por alguma potência de $\frac{\partial}{\partial t}$ em uma unidade, e portanto temos que algumas potências de d levam elementos não nulos de R em uma unidade, ou seja, d não deixa nenhum ideal de R invariante.

■

Capítulo 3

Derivações Simples em Anéis Polinomiais

Este é o último capítulo deste trabalho, nele vamos apresentar exemplos de derivações d de um anel de polinômios que o tornam d-simples. Iniciamos com o exemplo que A. Shamsuddin apresentou em 1977 (veja [12]). Exemplos de derivações d que tornam um anel local obtido a partir do anel de polinômios eram conhecidos, mas os exemplos de Shamsuddin foram os primeiros de caráter global que aparecem na literatura. A partir destes exemplos e da relação entre eles e os ideais maximais à esquerda da álgebra de Weyl (veja [1]) passou-se a procurar outros exemplos de grau maior, já que as derivações apresentadas por Shamsuddin são de grau 1.

Seguindo esta linha apresentaremos no parágrafo 2 deste capítulo outros exemplos devido a A. Maciejewski , J. Moulin-Ollagnier e A. Nowicki que foram obtidos em 2001 (veja [9]).

Na verdade este capítulo será dividido em duas seções, na primeira vamos introduzir conceitos e dar alguns resultados a respeito de simplicidade. O principal resultado que aparece na seção será o de Shamsuddin e a partir dele apresentaremos exemplos explícitos de derivações que tornam o anel de polinômios d-simples. Na segunda seção estudaremos os polinômios de Darboux e a partir deles as derivações de A. Maciejewski , J. Moulin-Ollagnier e A. Nowicki, Δ_p, e concluiremos com outros exemplos de derivações que tornam o anel de polinômios d-simples.

3.1 Derivações de Shamsuddin

Nesta seção introduziremos os primeiros resultados com respeito a simplicidade de derivações e iniciamos com a seguinte definição que é mais específica que a definição 2.2.1:

Definição 3.1.1 : *Seja d uma k-derivação de um anel R , dizemos que d é simples ou que R é d-simples, se R não possui d-ideais além do 0 e do próprio R.*

Agora estamos prontos para falar sobre o teorema de Shamsuddin. Tal teorema será importante no desenvolvimento deste capítulo, pois será utilizado na prova de vários outros resultados e também na apresentação de exemplos concretos.

Teorema 3.1.2 (Shamsuddin) : *Seja R um anel contendo o corpo dos números racionais e seja d uma derivação simples de R. Estendendo d a uma derivação δ do anel polinomial $R[t]$ tal que $\delta(t) = at + b$, onde $a, b \in R$. Então as seguintes condições são equivalentes.*

(i) δ é simples ;

(ii) Não existe r em R tal que $d(r) = ar + b$.

Demonstração : (i) $\Rightarrow$ (ii) Suponhamos que existe um $r \in R$ tal que $d(r) = ar + b$. Portanto se provarmos que $(t - r)$ é um δ-ideal teremos um absurdo, pois $(t - r) \neq R$, $(t - r) \neq 0$ e δ é simples. Assim provemos que $(t - r)$ é de fato um δ-ideal.

Dado $x = y(t - r)$, com $y \in R$. Temos que :

$$\begin{aligned}\delta(x) = \delta(y(t-r)) &= y(\delta(t) - \delta(r)) + d(y)(t-r) \\ &= y(at + b - (ar + b)) + d(y)(t-r) \\ &= (y.a + d(y))(t-r),\end{aligned}$$

e portanto temos que $\delta(x) \in (t - r)$, ou seja, $\delta((t - r)) \subset (t - r)$, e portanto $(t - r)$ é um δ-ideal.

(ii) $\Rightarrow$ (i) Suponhamos por absurdo que existe um δ-ideal I não nulo de $R[t]$ tal que $I \neq R[t]$. Então $I \cap R$ é um d-ideal de R e assim, como d é simples, $I \cap R = 0$, pois $1 \notin I$. Agora seja $n = min\{deg(f); 0 \neq f \in I\}$, e seja $\sigma(I) = \{0\} \cup \{r \in R$;existe $f \in I$,$\deg(f) = n$,$c_f = r\}$ onde c_f denota o coeficiente líder do polinômio f, como $I \cap R = 0$ é claro que $n \geq 1$. Agora vejamos que $\sigma(I)$ é um ideal de R.

De fato tome $r \in \sigma(I)$ e considere $f \in I$ tal que $\deg(f) = n$ e $c_f = r$. Suponhamos que $d(r) \neq 0$ e seja $g = \delta(f) - naf$. Então $g \in I$, $\deg(g) = n$ e $c_g = d(r)$, pois $\delta(t) = at + b$. Logo $d(r) \in \sigma(I)$ e assim temos que $\sigma(I)$ é um d-ideal de R.

Como d é simples e $\sigma(I) \neq 0$, então $\sigma(I) = R$. Assim existe um polinômio mônico $f \in I$ tal que $\deg(f) = n$. Seja $f = t^n + r_{n-1}t^{n-1} + \ldots + r_1 t + r_0$, onde $r_0, \ldots, r_{n-1} \in R$. Considerando $g = \delta(f) - naf$, então $g \in I$ e $g = st^{n-1} + s_{n-2}t^{n-2} + \ldots + s_1 t + s_0$, onde $s_0, \ldots, s_{n-2} \in R$ e $s = nb + d(r_{n-1}) - ar_{n-1}$. Agora da minimalidade de n temos que $s = 0$, ou seja, $d(r) = ar + b$, onde $r = -n^{-1}r_{n-1}$, que contradiz nossa hipótese que diz não existir r em R tal que $d(r) = ar + b$. Logo devemos ter $I = R[t]$, e assim mostramos que δ é simples.

■

A partir do teorema de Shamsuddin vamos fazer um breve estudo de uma família de k-derivação do anel de polinômios $k[x, y]$. Começamos com a seguinte definição:

Definição 3.1.3 : *Dados o anel de polinômios $k[x]$ com k sendo um corpo e a, b em $k[x]$. Denotaremos por $D_{a,b}$ a k-derivação do anel de polinômios $k[x, y]$ definida por: $D_{a,b}(x) = 1$ e $D_{a,b}(y) = ay + b$.*

O primeiro resultado com respeito a tal família de derivações é o seguinte:

Proposição 3.1.4 : *Sejam* $a,b \in k[x]$. *Então* $D_{a,b}$ *não é simples se, e somente se, existe* $f \in k[x]$ *tal que* $f' = af + b$, *onde* f' *denota a derivada usual de* f.

Demonstração : Primeiro note que a restrição de $D_{a,b}$ a $k[x]$ é $\frac{\partial}{\partial x}$. Agora basta observar que a proposição acima é a negação do teorema de Shamsuddin tomando $R = k[x]$, $t = y$ e $d = \frac{\partial}{\partial x}$.

■

A seguir damos algumas propriedades das derivações do tipo $D_{a,b}$.

Proposição 3.1.5 : *Sejam* $a,b \in k[x]$. *Então :*

1) $D_{a,0}$ *não é simples ;*

2) $D_{0,b}$ *não é simples ;*

3) Se $a \neq 0$, $b \neq 0$ e $\deg(b) < \deg(a)$, *então* $D_{a,b}$ *é simples ;*

4) Se $a \neq 0$, $b \neq 0$, $\deg(b) = \deg(a)$ e $D_{a,b}$ *é não simples então* $b = \gamma a$, *onde* $\gamma \in k\backslash\{0\}$;

5) Se $D_{a,b}$ e $D_{a,c}$ *não são simples, então* $D_{a,b+ac}$ *não é simples, onde* α *está em* k.

Demonstração : Os itens 1) e 2) são consequências imediatas da proposição anterior tomando $f = 0$ em 1) e $f = bx$ em 2).

Para 3) suponha que $D_{a,b}$ não é simples, assim, pela proposição 3.1.4, sabemos que existe f em $k[x]$ tal que $f' = af + b$. Como $b \neq 0$ tem-se que $f \neq 0$ e assim temos a contradição, $\deg(f) - 1 = \deg(f') = \deg(a) + \deg(f) \geq \deg(f)$.

Para 4) sabemos que $\deg(a) = \deg(b)$ e que $D_{a,b}$ não é simples. Pela proposição 3.1.4 temos que existe $0 \neq f$ em $k[x]$ tal que $f' = af + b$. Agora $0 \neq f'$ não pode acontecer pois neste caso $\deg(f) > \deg(f')$ e $a \neq 0$. Portanto $f = -\gamma \in k\backslash\{0\}$, então $f' = 0$ e temos $0 = -\gamma a + b$, ou seja, $b = \gamma a$.

Na verdade 4) é consequência imediata da proposição 3.1.4 e do fato de que $\frac{\partial}{\partial x}$ é k-linear.

A prova de 5) segue do fato de que $(f_1 + \alpha f_2)' = f_1' + \alpha f_2'$,onde f_1, f_2 são polinômios de $k[x]$, e da proposição 3.1.4.

■

A proposição anterior nos dá condições de apresentar alguns exemplos de derivações simples, a saber.

Exemplo 3.1.6 : *A k-derivação d do anel de polinômios $k[x,y]$ dada por $d(x) = 1$ e $d(y) = xy + 1$ é uma k-derivação simples de $k[x,y]$.*

De fato, basta observar que $\deg(x) = 1 > \deg(1) = 0$ e usar a proposição 3.1.5 (item 3)

Exemplo 3.1.7 : *A k-derivação d do anel de polinômios $k[x,y]$ dada por $d(x) = 1$ e $d(y) = (x^2 + x)y + x^2$ é uma k-derivação simples de $k[x,y]$.*

De fato , aqui temos que $a = x^2 + x$ e $b = x^2$, ou seja é uma derivação do tipo $D_{(x^2+x),x^2}$ e $\deg(a) = \deg(b)$. Assim pela proposição 3.1.5 (item 4) se tal derivação não fosse simples então teríamos que $b = \gamma a$, para algum $\gamma \in k\backslash\{0\}$, o que evidentemente não acontece.

A proposição abaixo fornece mais um critério para decidir quando uma derivação do tipo $D_{a,b}$ é simples.

Proposição 3.1.8 : *Sejam $a,b \in k[x]$ com $a \neq 0$. Assuma que $b = ca + r$, onde $c,r \in k[x]$ e $\deg(r) < \deg(a)$. Então $D_{a,b}$ não é simples se, e somente se , $D_{a,(c'+r)}$ não é simples.*

Demonstração : Para fazermos a prova utilizaremos o seguinte argumento:

$(\star)$ Dado $u \in k[x]$ podemos escrever u' da seguinte forma: $u' = u' + au - au = au + (u' - au)$, e assim pela proposição 3.1.4, $f = u$ e $b = u' - au$ temos que $D_{a,(u'-au)}$ não é simples.

Sabendo disso vejamos a prova da proposição.

$\Rightarrow$) Sabemos que $D_{a,b}$ não é simples , como, por hipótese, $b = ca + r$ então temos que $D_{a,(ca+r)}$ não é simples e pelo que vimos em $(\star)$ também temos que $D_{a,(c'-ca)}$ não é simples.Logo pela proposição 3.1.5 (item 5) temos que $D_{a,(ca+r+c'-ca)}$ não é simples, ou seja $D_{a,(c'+r)}$ não é simples.

$\Leftarrow$) Sabemos que $D_{a,(c'+r)}$ não é simples e que $b = ca + r$. Por $(\star)$ temos que $D_{a,(c'-ca)}$ não é simples , logo pela proposição 3.1.5 (item 5) temos que $D_{a,(ca-c')}$ não é simples, e pelo item1 da mesma proposição temos que $D_{a,(c'+r+ca-c')}$ não é simples , ou seja, $D_{a,(ca+r)} = D_{a,b}$ não é simples.

■

A partir do critério dado na proposição exibimos mais um exemplo de derivação simples.

Exemplo 3.1.9 : *A derivação $D_{a,b}$ com $a = x^3 + 1$ e $b = x^8 + 3x^5 + 1$ é uma derivação simples de $k[x,y]$.*

De fato , suponhamos que a derivação $D_{a,b}$ não seja simples. Sabemos que $b = x^8 + 3x^5 + 1 = (x^5 + 2x^2)(x^3 + 1) + (-2x^2 + 1) = ca + r$, onde é claro $c = x^5 + 2x^2$, $a = x^3 + 1$ e $r = -2x^2 + 1$. Pela proposição 3.1.8 temos que $D_{a,(c'+r)}$ não é simples , onde $c' + r = 5x^4 - 2x^2 + 4x + 1$. Agora escrevendo $b_1 = c' + r = c_1 a + r_1$, onde $c_1 = 5x$ e $r_1 = -2x^2 - x + 1$, tem-se pela mesma proposição 3.1.8 que $D_{a,(c_1' + r_1)}$ não é simples. Agora considerando $b_2 = c_1' + r_1 = -2x^2 - x + 6$, obtem-se que D_{a,b_2} não é simples. E portanto D_{a,b_2} não é simples com $\deg(a) > \deg(b_2)$ e $b_2 \neq 0$ o que contradiz o item 3 da proposição 3.1.5. Logo $D_{a,b}$ com $a = x^3 + 1$ e $b = x^8 + 3x^5 + 1$ é simples.

O algoritmo de Euclides para o anel de polinômios $k[x]$, k corpo, nos dá o seguinte resultado.

Proposição 3.1.10 : *Seja $a \in k[x]$, $a \neq 0$. Então para todo $b \in k[x]$ existe único $c \in k[x]$ com $c = 0$ ou $\deg(c) < \deg(a)$ e tal que $D_{a,(b-c)}$ não é derivação simples do anel de polinômios $k[x]$.*

Demonstração : Dado $b \in k[x]$ temos a seguinte sequência $(\star)$ de igualdades :

$b = u_1 a + r_1$

$u_1' = u_2 a + r_2$

$\vdots$

$u_{n-1}' = u_n a + r_n$

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

onde $r_1, \ldots, r_{n+1}, u_1, \ldots, u_n \in k[x]$ e, para cada i , $r_i = 0$ ou $deg(r_i) < deg(a)$.

Tomando $c = r_1 + \ldots + r_{n+1}$ tem-se $deg(c) < deg(a)$. O que vamos provar agora é que $D_{a,(b-c)}$ não é simples.

Sabemos que $b - c = u_1 a + r_1 - (r_1 + \ldots + r_{n+1}) = u_1 a - r_2 - \ldots - r_{n+1}$. Mas da sequência $(\star)$ temos que para todo i , $2 \leq i \leq n$, $r_i = u_{i-1}' - u_i a$ e $r_{n+1} = u_n'$.

Logo $b - c = u_1 a - u_1' + u_2 a - u_2' + u_3 a + \ldots - u_{n-1}' + u_n a - u_n'$

$= (u_1 + \ldots + u_n).a - (u_1' + \ldots + u_n')$

ou seja $b - c = qa + r$, onde $q = (u_1 + \ldots + u_n)$ e $r = -(u_1' + \ldots + u_n')$.

Assim pela proposição 3.1.8 temos que $D_{a,(b-c)}$ não é simples se, e somente se, $D_{a,(q'+r)}$ não é simples. Mas $q' + r = u_1' + \ldots + u_n' - (u_1' + \ldots + u_n') = 0$, e como vimos na proposição 3.1.5 (item 1) $D_{a,0}$ não é simples, ou seja, $D_{a,(q'+r)}$ não é simples e assim $D_{a,(b-c)}$ não é simples.

Agora vejamos a unicidade de tal c.

Suponha que $c_1, c_2 \in k[x]$ tais que ambos satisfazem as condições da proposição. Então pela proposição 3.1.5 (item1) $D_{a,(b-c_1-b+c_2)} = D_{a,(c_2-c_1)}$ não é simples, mas se $c_2 - c_1 \neq 0$ temos que $\deg(c_2 - c_1) < \deg(a)$ e isto, pela proposição 3.1.5 item 3, é uma contradição.

■

O teorema que vem a seguir apresenta uma k-derivação que generaliza, para o anel de polinômios $k[x_1,\ldots,x_n]$, derivações do tipo $D_{a,b}$ e dá condições para que tal derivação seja simples.

Teorema 3.1.11 : *Se k é um corpo, $d = \frac{\partial}{\partial x_1} + \sum_{i=2}^{n}(a_i x_i + b_i)\frac{\partial}{\partial x_i}$ é a k-derivação do anel de polinômios $k[x_1,\ldots,x_n]$ e para todo $i = 2,\ldots,n$ as condições abaixo são satisfeitas*

1) $a_i, b_i \in k[x_1,\ldots,x_{i-1}]$;

2) $b_i \neq 0$;

3) $deg_{x_{i-1}}(a_i) \geq 1$;

4) $deg_{x_{i-1}}(b_i) < deg_{x_{i-1}}(a_i)$.

Então d é simples.

Demonstração : A prova será feita por indução sobre n.

Se $n = 1$, então $d = \frac{\partial}{\partial x_1}$, e portanto simples.

Para $n > 1$ assumimos que $d' = d \mid_R$, onde $R = k[x_1,\ldots,x_{n-1}]$, seja uma k-derivação simples.

Suponhamos que exista $f \in k[x_1,\ldots,x_{n-1}]$ tal que $d'(f) = a_n f + b_n$, ou seja neste caso temos:

$$\frac{\partial f}{\partial x_1} + (a_2x_2 + b_2)\left(\frac{\partial f}{\partial x_2}\right) + \ldots + (a_{n-1}x_{n-1} + b_{n-1})\left(\frac{\partial f}{\partial x_{n-1}}\right) = a_n f + b_n.$$

Agora como d' é simples e, por hipótese, $b_n \neq 0$ tem-se $f \neq 0$. Considere $s = deg_{x_{n-1}}(f)$.

O grau em x_{n-1} de $\frac{\partial f}{\partial x_1} + (a_2x_2 + b_2)\left(\frac{\partial f}{\partial x_2}\right) + \ldots + (a_{n-1}x_{n-1} + b_{n-1})\left(\frac{\partial f}{\partial x_{n-1}}\right)$ claramente não é maior que s, mas o de $a_n f + b_n$ é maior que s , pois, por hipótese, $deg_{x_{n-1}}(a_n) \geq 1$, e tem-se uma contradição. Portanto não existe tal f e desde que d' é simples, segue pelo teorema de Shamsuddin que d é simples.

■

Para encerrarmos esta seção utilizaremos o teorema acima para conseguirmos as primeiras derivações simples em anéis a n variáveis.

Exemplo 3.1.12 : *As k-derivações de $k[x_1,\ldots,x_n]$ d_1 e d_2 definidas por:*

$d_1(x_1) = 1$

$d_2(x_1) = 1$

$d_1(x_2) = x_1x_2 + 1$

$d_2(x_2) = x_1^2x_2 + 1$

$d_1(x_3) = x_2x_3 + 1$

$d_2(x_3) = x_2^2 x_3 + 1$

$\vdots$

$d_1(x_n) = x_{n-1} x_n + 1$

$d_2(x_n) = x_{n-1}^2 x_n + 1$

são simples.

Se constata facilmente que as duas derivações satisfazem todas as condições do teorema 3.1.11.

3.2 Derivações simples e quadráticas do anel de polinômios k[x,y]

Neste paragráfo vamos trabalhar com derivações quadráticas do anel de polinômios $k[x,y]$ com $d(x) = 1$ e $d(y) = y^2 + a(x).y + b(x)$; $a(x), b(x) \in k[x]$. A idéia aqui, como no caso de Shamsuddin, é dar condições sobre $a(x), b(x)$ para que d seja simples. Isto foi feito por A. Maciejewski, J. Moulin-Ollagnier e A. Nowicki em [9] e é precisamente a parte central deste artigo que apresentaremos no presente paragráfo.

Começamos com a definição de polinômios de Darboux que estão relacionados com soluções algébricas de certas equações diferenciais.

Definição 3.2.1 : *Sejam k um corpo e $\underline{X} = \{x_1, \ldots, x_n\}$ um conjunto de variáveis sobre k, f em $k[\underline{X}]$ e d uma k-derivação de $k[\underline{X}]$, dizemos que f é um polinômio de Darboux de d se $f \notin k$ e $d(f) = h.f$, para algum h em $k[\underline{X}]$. Neste caso dizemos que h é autovalor associado a f.*

Proposição 3.2.2 : *Se $f \in k[\underline{X}]$ é um polinômio de Darboux de d , então todos os fatores irredutíveis de f também são polinômios de Darboux de d.*

Demonstração : Escreva $f = f_1^1 . f_2^2 . \ldots . f_n^n$, onde para $i = 1, \ldots, n$ temos que $r_i \in \mathbb{N}$ e f_i é irredutível em $k[\underline{X}]$. Sendo f um polinômio de Darboux de d, então $d(f) = h.f$ para algum $h \in k[\underline{X}]$, mas $d(f) = \sum_{i=1}^{n} r_i . d(f_i) . f_1^1 . \ldots . f_i^{i-1} . \ldots . f_n^n = h.f$, e mais f_i^i divide $h.f$, ou seja f_i^i divide $\sum_{i=1}^{n} r_i . d(f_i) . f_1^1 . \ldots . f_i^{i-1} . \ldots . f_n^n$, como f_i^i divide cada termo, então temos que f_i^i divide $r_i . d(f_i) . f_1^1 . \ldots . f_i^{i-1} . \ldots . f_n^n$. Mas f_i é irredutível para todo $i = 1, \ldots, n$, então f_i^i divide $r_i . d(f_i) . f_i^{i-1}$, logo f_i divide $d(f_i)$, ou seja $d(f_i) = h_i . f_i$, e temos o que queríamos.

■

Para o caso de duas variáveis a não existência de polinômios de Darboux caracteriza o fato de certas derivações serem simples, para ser mais preciso:

Proposição 3.2.3 : *Se k é corpo e $d : k[x,y] \to k[x,y]$ é uma derivação do anel de polinômios tal que $d(x) = 1$, então d é simples se , e somente se, d não tem polinômio de Darboux.*

Demonstração : Iniciamos supondo que d é simples , ou seja que não existe um ideal próprio I tal que $d(I) \subset I$, logo d não tem polinômio de Darboux , pois se existe $f \in k[x,y]$, $f \notin k$, tal que $d(f) = h.f$, para algum $h \in k[x,y]$ então o ideal gerado por f , isto é, o ideal (f) que é próprio , pois $f \notin k$, seria um d-ideal , pois $d(f) \subset (f)$, que é uma contradição pois d é simples.

Agora supomos que d não tem polinômio de Darboux. Pela proposição 2.2.2 podemos, se necessário, estender a derivação d para $\overline{k}[x,y]$, onde $\overline{k}$ é o fêcho algébrico de k, e assim podemos supor de início de que k é algebricamente fechado.

Vamos supor que d não seja simples e vamos chegar a uma contradição. Como d não simples pelo teorema 2.2.8 existe um d-ideal próprio primo P de $k[x,y]$.

Se P é maximal , então pelo teorema dos zeros de Hilbert, já que k é algebricamente fechado, temos que $P = (x-a\ ,\ y-b)$, para certos $a,b \in k$. Mas $1 = d(x-a) \in d(P) \subset P$, que é uma contradição pois P é um ideal próprio. Logo temos que a altura de P é igual a 1 e portanto P é um d-ideal próprio principal , ou seja $P = (F)$, e assim F é um polinômio de Darboux de d , que contradiz nossa tese. E então concluímos que d tem que ser simples.

■

Dados o corpo k e o corpo de funções racionais $k(x)$ de $k[x]$, denotaremos o fecho algébrico de $k(x)$ por $\overline{k(x)}$. A única extensão da derivação $\frac{\partial}{\partial x} : k(x) \to k(x)$ será denotada por $' : \overline{k(x)} \to \overline{k(x)}$.

Agora vamos apresentar duas proposições que servirão de base para obtermos um resultado (teorema 3.2.6) que relaciona polinômios de Darboux de derivações de $k[x,y]$ com soluções algébricas de equações diferenciais de primeira ordem com coeficientes em $k(x)$.

Proposição 3.2.4 : *Seja d uma derivação de $k[x,y]$, com $d(x) = P(x,y)$ e $d(y) = Q(x,y)$. Se $F \in k[x,y] = k[x][y]$ é um polinômio de Darboux irredutível de d com $deg_y F \geq 1$, então existe um $r \in \overline{k(x)}$ tal que $P(x,r).r' = Q(x,r)$ e $F(x,r) = 0$.*

Demonstração : Como $deg_y F \geq 1$, F tem raiz r no corpo algebricamente fechado $\overline{k(x)}$, isto é, $F(x,r) = 0$ com $r \in \overline{k(x)}$.

Derivando $F(x,r) = 0$ com respeiro a x temos : $\frac{\partial F}{\partial x}(x,r).1 + \frac{\partial F}{\partial y}(x,r).r' = 0$.

Agora usando que $P(x,y) = d(x)$, $Q(x,y) = d(y)$ e que $d(F) = H.F$, obtemos:

$$\frac{\partial F}{\partial x}(x,y).P(x,y) + \frac{\partial F}{\partial y}(x,y).Q(x,y) = H(x,y).F(x,y)$$

Calculando a expressão acima em $y = r$, e usando que $F(x,r) = 0$, segue a igualdade : $\frac{\partial F}{\partial x}(x,r).P(x,r) + \frac{\partial F}{\partial y}(x,r).Q(x,r) = 0.$

Mas $deg_y F \geq 1$ e F é irredutível, logo $\frac{\partial F}{\partial y}(x,r) \neq 0$, e portanto $Q(x,r) = -\frac{\frac{\partial F}{\partial x}(x,r)}{\frac{\partial F}{\partial y}(x,r)}.P(x,r)$, mas como vimos no início, $\frac{\partial F}{\partial x}(x,r).1 + \frac{\partial F}{\partial y}(x,r).r' = 0$, ou seja $r' = -\frac{\frac{\partial F}{\partial x}(x,r)}{\frac{\partial F}{\partial y}(x,r)}$ e assim temos que $Q(x,r) = r'.P(x,r)$.

■

Na próxima proposição usamos um lema devido a Gauss e em tal lema aparece o conceito de conteúdo de um polinômio, assim a seguir apresentamos um breve relato sobre tal conceito.

Seja R um anel fatorial e K seu corpo de frações. Tome $a \in K$, $a \neq 0$ e escreva $a = \frac{x}{y}$, com $x,y \in R$ coprimos. Se p é um irredutível em R , então podemos escrever $a = p^r b$, onde $b \in K$, $r \in \mathbb{Z}$ e p não divide o numerador e o denominador de b. Usando a fatorização única de R vemos que r é único, chamaremos tal r de ordem de a em p e denotaremos por $r = ord_p a$. Se $a = 0$ sua ordem em p será $-\infty$.

Sendo $f \in K[X]$ um polinômio em uma variável então temos que :

$$f(X) = a_n X^n + \ldots + a_1 X + a_0$$

Se $f = 0$, definimos $ord_p f$ como sendo $-\infty$. Se $f \neq 0$, definimos $ord_p f = \min ord_p a_i$, onde esse mínimo é tomado sobre todos os i tais que $a_i \neq 0$.

Definimos o **conteúdo** de f por : $cont(f) = \prod p^{ord_p f}$, onde esse produto é tomado sobre todo p tal que $ord_p f \neq 0$. Mais ainda, dizemos que f é primitivo se $cont(f) = 1$.

Agora podemos enunciar o lema de Gauss, cuja demonstração pode ser vista em [15] (capítulo 1 , lema 1).

Lema de Gauss : *Sejam R um anel fatorial, e K seu corpo de frações. Sejam $f,g \in K[X]$, então $cont(f.g) = cont(f).cont(g)$.*

Feitas estas observações vamos a seguinte proposição.

Proposição 3.2.5 : *Sejam d uma derivação de $k[x,y]$, $d(x) = P(x,y)$ e $d(y) = Q(x,y)$. Se r é solução em $\overline{k(x)}$ da equação diferencial $P(x,r).r' = Q(x,r)$ e $F \in k[x][y]$ é tal que $F(x,r) = 0$ e é primitivo minimal com esta propriedade, então F é um polinômio de Darboux de d com $deg_y F \geq 1$.*

Demonstração : Claramente $\deg_y F \geq 1$, pois $F(x,r) = 0$.

Definamos $H \in k[x,y]$ por :

$$H = H(x,y) = d(F(x,y)) = P(x,y).\frac{\partial F}{\partial x}(x,y) + Q(x,y).\frac{\partial F}{\partial y}(x,y)$$

Temos que $H(x,r) = 0$, pois :

$$H(x,r) = P(x,r).\frac{\partial F}{\partial x}(x,r) + Q(x,r).\frac{\partial F}{\partial y}(x,r) = P(x,r).\frac{\partial F}{\partial x}(x,r) + P(x,r).r'.\frac{\partial F}{\partial y}(x,r)$$

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

Como $F(x,y)$ é o polinômio minimal de r , então H é múltiplo de F em $k(x)[y]$, que significa que existe $\Lambda = \Lambda(x,y) \in k(x)[y]$ tal que $d(F) = H = \Lambda.F$.

Agora sabendo que $F(x,y)$ é primitivo podemos usar o lema de Gauss (com $R = k[X]$, $K = k(x)$ e $\Lambda, F \in k(x)[y]$) para concluir que $cont(H) = cont(\Lambda)$, ou seja o conteúdo de Λ pertence a $k[x]$, pois $H \in k[x,y]$. Portanto $\Lambda \in k[x,y]$ e assim temos que $d(F) = \Lambda.F$, com $\Lambda \in k[x,y]$, ou seja F é um polinômio de Darboux de d.

■

Como consequência imediata destas duas últimas proposições tem-se o seguinte teorema.

Teorema 3.2.6 : *Sejam d uma derivação de $k[x,y]$, $d(x) = P(x,y)$ e $d(y) = Q(x,y)$. Então as seguintes condições são equivalentes :*

1) Existe um polinômio de Darboux $F \in k[x,y]$ de d tal que $\deg_y F \geq 1$;

2) Existe um $r \in \overline{k(x)}$, tal que $P(x,r).r' = Q(x,r)$.

Agora veremos um caso especial do teorema anterior .

Corolário 3.2.7 : *Seja $d : k[x,y] \to k[x,y]$ a derivação definida por : $d(x) = 1$ e $d(y) = a(x).y^2 + b(x).y + c(x)$, onde $a(x), b(x), c(x) \in k[x]$ e $a(x) \neq 0$. Então d tem um polinômio de Darboux $F \in k[x,y]$ com $\deg_y F \geq 1$ se , e somente se , existe uma função algébrica $r \in \overline{k(x)}$ tal que $r' = a(x).r^2 + b(x).r + c(x)$.*

Demonstração : Basta observarmos que estamos nas condições do teorema anterior com $P(x,y) = 1$ e $Q(x,y) = a(x).y^2 + b(x).y + c(x)$.

■

Mais adiante vamos ver que o estudo de derivações d, de $k[x,y]$, com $d(x) = 1$ e $d(y) = y^2 + a(x).y + b(x)$ se reduz ao estudo de derivações, de $k[x,y]$, do tipo que definimos abaixo.

Definição 3.2.8 : *Para $p = p(x) \in k[x]$, a derivação Δ_p de $k[x,y]$ é definida por :*

$$\Delta_p(x) = 1 \text{ e } \Delta_p(y) = y^2 - p(x)$$

Nossos próximos três resultados serão dedicados a estudar polinômios de Darboux de Δ_p. Observamos que , como $\Delta_p(x) = 1$, claro que não existem polinômios de Darboux de Δ_p no subanel $k[x]$, assim se F é um polinômio de Darboux de Δ_p em $k[x,y]$ então $\deg_y F \geq 1$.

Assim temos o seguinte caso especial do corolário 3.2.7 :

Corolário 3.2.9 : *A derivação Δ_p tem um polinômio de Darboux $F \in k[x,y]$ com $\deg_y F \geq 1$ se, e somente se, existe uma função algébrica $r \in \overline{k(x)}$ tal que $r' = r^2 - p$.*

Demonstração : Basta observar que estamos nas condições do corolário 3.2.7 com $a(x) = 1$, $b(x) = 0$ e $c(x) = -p$.

■

Os dois resultados que mostraremos a seguir dizem respeito a polinômios de Darboux F de Δ_p que são irredutíveis e tais que $\deg_y F = 1$. Observe que, pela proposição 3.2.2, o fato de ser irredutível não é restritível.

Proposição 3.2.10 : *Seja F um polinômio irredutível e de Darboux de Δ_p com $\deg_y F = 1$. Tome $\Lambda \in k[x,y]$ tal que $\Delta_p(F) = \Lambda.F$. Escrevendo $F = u.y + v$, onde $u, v \in k[x]$, com $u \neq 0$ e $mdc(u,v) = 1$. Então:*

1) $\Lambda = y + s$, para algum $s \in k[x]$;

2) $su + v = u'$ e $sv = v' - pu$;

3) $u'' - s'u - 2su' + s^2u - pu = 0$;

4) $\deg p = 2\deg s$ (onde ambos podem ser $-\infty$).

Demonstração : Sabemos que $\Delta_p(F) = \Lambda.F$ e que $F = uy + v$, onde $u, v \in k[x]$, logo desenvolvendo a igualdade $\Delta_p(F) = \Lambda.F$ temos que :

$\Lambda.(u.y + v) = \Delta_p(u.y + v) = \Delta_p(u.y) + \Delta_p(v) = u(y^2 - p) + u'.y + v'$, assim temos :

$\Lambda.(u.y + v) = u.y^2 + u'.y + v' - p.u \qquad (*)$

Da equação $(*)$ conclui-se facilmente que $\Lambda = y + s$, para algum $s \in k[x]$ e o item (1) está provado. Agora tem-se:

$\Lambda.(u.y+v) = (y+s).(u.y+v) = u.y^2 + (s.u+v).y + s.v \quad (**)$

Das equações $(*)$ e $(**)$ obtemos a igualdade :

$u.y^2 + (s.u+v).y + s.v = u.y^2 + u'.y + v' - p.u$, identificando os coeficientes em y desta igualdade temos que : $s.u+v = u'$ e $s.v = v' - p.u$, logo acabamos de provar o item (2).

Da igualdade $s.u+v = u'$ podemos ver que $v = u' - s.u$ e substituindo tal v na igualdade $s.v = v' - p.u$ teremos que $s.(u' - s.u) = (u' - s.u)' - p.u.$ Daí segue que $s.u' - s^2.u = u'' - s'u - su' - pu$ e temos a igualdade do item (3).

Agora vamos provar o item (4), para isso usaremos novamente as iguladades $s.u+v = u'$ e $s.v = v' - p.u$.

Em primeiro lugar afirmamos que $p = 0$ se, e somente se, $s = 0$, isto é, $\deg p = -\infty$ se, e somente se, $\deg s = -\infty$.

De fato, primeiro suponha que $p = 0$. Como, por hipótese, $u \neq 0$, as igualdades $s.u+v = u'$ e $s.v = v'$, nos diz que $s = 0$, pois se $s \neq 0$, então $s.v = v'$ nos diz que $v = 0$, e assim teríamos $s.u = u'$, com $s \neq 0$ e $u \neq 0$, que é um absurdo já que estamos trabalhando com polinômios.

Agora suponha que $s = 0$, assim as igualdades $v = u'$ e $v' = p.u$, nos garante que $p = 0$, pois se $p \neq 0$, então substituindo $v = u'$ em $v' = p.u$, teríamos $u'' = p.u$, com $p \neq 0$ e $u \neq 0$, o que, novamente, nos leva a um absurdo.

Depois de analisarmos o caso em que $p = 0$, vejamos agora quando $p \neq 0$, e portanto $s \neq 0$. Das igualdades $s.u+v = u'$ e $s.v = v' - p.u$, temos que:

$$\deg v = \deg s + \deg u \quad \text{e} \quad \deg s + \deg v = \deg p + \deg u$$

Como $u \neq 0$, $\deg u$ pode ser cancelado e portanto temos $\deg p = 2.\deg s$.

■

Proposição 3.2.11 : *Sejam u e v pertencentes a $k[x]$, com $u \neq 0$ e $mdc(u,v) = 1$. Sejam $F = u.y+v \in k[x][y]$ e $r = -\frac{v}{u} \in k(x)$. Então as seguintes condições são equivalentes :*

1) F é um polinômio de Darboux de Δ_p ;

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

Demonstração : $(1) \Rightarrow (2)$: Sabemos que F é um polinômio de Darboux de Δ_p , assim usando a proposição anterior temos que $\Delta_p(F) = (y+s).F$, para certo $s \in k[x]$, e mais ainda $s.u+v = u'$ e $s.v = v' - p.u$. Assim multiplicando a primeira igualdade por v , e a segunda por u teremos : $v.u' - v^2 = s.u.v = u.v' - p.u^2$, agora usando estas igualdades e os fatos , dados por hipótese, que $u \neq 0$ e $r = -\frac{v}{u}$, teremos :

$$r' = \frac{v.u' - u.v'}{u^2} = \frac{v^2}{u^2} - p = r^2 - p$$

$(2) \Rightarrow (1)$: Sabemos que $r' = r^2 - p$, e como $r = -\frac{v}{u}$, temos que : $\frac{v.u' - u.v'}{u^2} = \frac{v^2}{u^2} - p$, agora multiplicando essa igualdade por u^2 conseguimos : $v.u' - u.v' = v^2 - u^2 p$, logo, $u.(v' - p.u) = v.(u' - v)$. Mas, por hipótese, $mdc(u,v) = 1$, assim existe $s \in k[x]$ tal que $v' - p.u = s.v$ e $u' - v = s.u$.

Agora vamos calcular $\Delta_p(F)$, vejamos :

$\Delta_p(F) = \Delta_p(u.y+v) = u'.y + u.(y^2 - p) + v' = u.y^2 + (u' - v).y + v.y + (v' - p.u)$
$= u.y^2 + s.u.y + v.y + s.v = (y+s)(u.y+v) = (y+s).F$

Assim vimos que F é um polinômio de Darboux de Δ_p, com autovalor $(y+s)$.

■

No nosso estudo sobre a simplicidade da derivação Δ_p , estaremos interessados nas soluções algébricas de equações diferenciais da forma $y' = y^2 - p(x)$, onde $p = p(x)$ é um polinômio em $k[x]$, isto é, nas soluções $y \in \overline{k(x)}$ de tal equação diferencial. Equações diferenciais dessa forma são denominadas equações diferenciais de Riccati.

O teorema a seguir nos dirá que as soluções algébricas destes tipos de equações são racionais.

Teorema 3.2.12 : *Para $p \in k[x]$, com k algebricamente fechado, a equação $y' = y^2 - p$, não tem solução $y \in \overline{k(x)} \backslash k(x)$. Em outras palavras , as soluções algébricas de $y' = y^2 - p$ são todas racionais.*

Demonstração : Suponhamos que exista $y \in \overline{k(x)} \backslash k(x)$ que seja solução de $y' = y^2 - p$.

Seja $F = y^n - \sigma_1.y^{n-1} + \ldots + (-1)^n\sigma_n$ o polinômio mônico minimal para y sobre $k(x)$. Este polinômio pertence a $k(x)[y]$, e seu grau n é no mínimo 2.

Agora seja K o corpo de raízes de F sobre $k(x)$ e sejam $y_1, \ldots, y_n$, as n raízes distintas de F em K . Por hipótese , uma delas é raiz da equação $y' = y^2 - p$.

Observamos que para todo $i = 1, \ldots, n$, y_i é raiz de $y' = y^2 - p$. Vejamos a veracidade de tal afirmação.

Como a extensão $K \setminus k(x)$ é algébrica, pelo teorema 2.1.12 temos que $\frac{\partial}{\partial x}$ de $k(x)$ pode ser estendida de maneira única a uma derivação $d : K \to K$. Se σ é um $k(x)$-automorfismo de K então a aplicação $\sigma d \sigma^{-1}$ é uma derivação de K, pois
$\sigma d \sigma^{-1}(a.b) = \sigma d(\sigma^{-1}(a).\sigma^{-1}(b)) = \sigma(d(\sigma^{-1}(a)).\sigma^{-1}(b) + \sigma^{-1}(a).d(\sigma^{-1}(b)))$
$= \sigma(d(\sigma^{-1}(a)).b + a.\sigma(d(\sigma^{-1}(b))$

Logo pela unicidade de tal extensão temos que $\sigma d \sigma^{-1} = d$. Assim temos que os automorfismos do grupo de Galois de K sobre $k(x)$ comutam com a única extensão da derivação $\frac{\partial}{\partial x}$ de $k(x)$. E portanto todos os y_i serão soluções de $y' = y^2 - p$.

Agora cosideremos $D = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (y_i - y_j)$ o discriminante de F.

Logo computando a derivada logarítmica $\frac{D'}{D}$ e substituindo $y_i' = y_i - p$ e $y_j' = y_j - p$, temos :

$\frac{D'}{D} = \sum_{i \neq j} \frac{y_i' - y_j'}{y_i - y_j} = \sum_{i \neq j} (y_i + y_j) = 2(n-1)\sigma_1$, onde esta última igualdade se deve ao fato de que $F = y^n - \sigma_1.y^{n-1} + \ldots + (-1)^n\sigma_n = (y - y_1).\ldots.(y - y_n)$.

Da igualdade $\frac{D'}{D} = 2(n-1)\sigma_1$, temos que σ_1 é , a menos de um fator $\frac{1}{2(n-1)}$, a

derivada logarítmica de $D \in k(x)$. Portanto a decomposição de σ_1 em frações parciais tem a forma da seguinte soma finita :

$\sigma_1 = \sum_{\alpha} \frac{\lambda_\alpha}{x-\alpha}$, onde cada $\alpha \in k$ e cada λ_α é um número racional.

Do fato de que as raízes de F são soluções de $y' = y^2 - p$ tem-se, pela proposição 3.2.5, que F é um polinômio de Darboux da derivação d dada por $d(x) = 1$ e $d(y) = y^2 - p$, e isto pode ser expressado pela seguinte igualdade:

$\frac{\partial F}{\partial x} + (y^2 - p).\frac{\partial F}{\partial y} = (n.y + a)F$, já que $F = y^n - \sigma_1.y^{n-1} + \ldots + (-1)^n\sigma_n$.

O autovalor $(n.y + a)$, é um polinômio de grau 1 em y. O coeficiente líder n neste autovalor vem do fato de que $\frac{\partial F}{\partial y} = n.y^{n-1} + \ldots$. Agora o "termo constante" a será estudado em maiores detalhes.

Na igualdade $\frac{\partial F}{\partial x} + (y^2 - p).\frac{\partial F}{\partial y} = (n.y + a)F$ consideremos todos os graus em y de n a 1 e então o de grau 0.

No sistema (Σ) de $n+1$ equações, todos os coeficientes de F são indutivamente definidos a partir de a e, depois de substituições, a última equação torna uma equação diferencial para a.

$$(\Sigma): \quad \begin{aligned} \sigma_1 &= a\sigma_0 - \sigma_0' && = a \quad (\text{pois }, \sigma_0 = 1) \\ 2\sigma_2 &= a\sigma_1 - \sigma_1' && -n.p.\sigma_0 , \\ 3\sigma_3 &= a\sigma_2 - \sigma_2' && -(n-1).p.\sigma_1 , \\ &\vdots \\ j\sigma_j &= a\sigma_{j-1} - \sigma_{j-1}' && -(n+2-j).p.\sigma_{j-2} , \\ &\vdots \\ n\sigma_n &= a\sigma_{n-1} - \sigma_{n-1}' && -2.p.\sigma_{n-2} , \\ 0 &= a\sigma_n - \sigma_n' && -p.\sigma_{n-1} , \end{aligned}$$

O sistema (Σ) acima também pode ser visto como uma definição indutiva de uma sequência de frações racionais (σ_j) , $j \in \mathbb{N}$, pelos dois valores iniciais $\sigma_0 = 1$ e $\sigma_1 = a$ e pela regra de indução $j.\sigma_j = a.\sigma_{j-1} - \sigma_{j-1}' - (n+2-j).p.\sigma_{j-2}$. E tomando-se $\sigma_{n+1} = \sigma_{n+2} = \ldots = 0$.

Para todo pólo α de $\sigma_1 = a$, p não está envolvido nessa parte polar de decomposição em frações parciais de cada equação de (Σ) ; assim temos que α é um pólo de σ_j com ordem no máximo j . Seja $\overline{\sigma_j}$ o candidato para a parte polar de σ_j de ordem j no pólo α ; $\overline{\sigma_j}$ pode ser computado pela indução :

$$j!.\overline{\sigma_j} = \frac{\lambda_\alpha(\lambda_\alpha + 1)\ldots(\lambda_\alpha + j - 1)}{(x-\alpha)^j}$$

A equação $0 = a\sigma_n - \sigma_n' - p.\sigma_{n-1}$, de (Σ) , nos dá a seguinte equação para λ_α :

$$\lambda_\alpha(\lambda_\alpha + 1)\ldots(\lambda_\alpha + n) = 0$$

Assim λ_α são inteiros negativos no intervalo $[-n\ ,\ -1]$, para todo α .

Assumiremos agora que $p \neq 0$. Podemos fazer análises do sistema (Σ) em torno de cada pólo, que significa que consideraremos os graus e os coeficientes líderes de

$\sigma_1, \ldots, \sigma_n$. Nessa projeção p está fortemente envolvido. Como $\deg(p) \geq 0$, do sistema (Σ) temos que $\deg(\sigma_{2j}) = j.\deg(p)$ e $\deg(\sigma_{2j+1}) \leq j.\deg(p) - 1$, assim vemos que a igualdade é válida para índices pares, por exemplo $\deg(\sigma_0) = 0$, pois $\sigma_0 = 1$, e para índices ímpares podemos ter a desigualdade, especialmente se $a = \sigma_1 = 0$, pois nesse caso temos $\deg(\sigma_1) = -\infty < -1$.

Denotaremos por $\overline{p}$ o coeficiente líder de p e por $\overline{\sigma_j}$ o coeficiente de σ_j correspondendo ao grau de maior grau em x : $\overline{\sigma_{2j}}$ o coeficiente de σ_{2j} de grau $j.\deg(p)$, enquanto $\overline{\sigma_{2j+1}}$ o coeficiente de σ_{2j+1} de grau $j.\deg(p) - 1$. Sejam $\Lambda = -\sum \lambda_a$ e $\delta = \deg(p)$, que são inteiros não negativos. O sistema (Σ) nos fornece as seguintes relações entre os coeficientes líderes :

$$\begin{aligned}
\overline{\sigma_1} &= \overline{a} = -\Lambda \\
2\overline{\sigma_2} &= -n.\overline{p} \ , \\
3\overline{\sigma_3} &= \overline{a\sigma_2} - \overline{\sigma_2}' - (n-1).\overline{p.\sigma_1} \ , \\
&\vdots \\
(2.j)\overline{\sigma_{2j}} &= -(n+2-2.j).\overline{p.\sigma_{2j-2}} \ , \\
(2.j+1)\overline{\sigma_{2j+1}} &= \overline{a\sigma_{2j}} - \overline{\sigma_{2j}}' - (n+2.j+1).\overline{p.\sigma_{2j-2}}
\end{aligned}$$

Podemos escrever as igualdades acima da seguinte forma : $\overline{\sigma_{2s}} = (-1)^s \overline{p}^s M_{2s}$ para índices pares , e $\overline{\sigma_{2s+1}} = -(-1)^s \overline{p}^s M_{2s+1}$ para índices ímpares , onde M_i são racionais não negativos que satisfazem a seguinte regra :

$$\begin{aligned}
M_0 &= 1 \ , \\
M_1 &= \Lambda \ , \\
M_{2s} &= \frac{n+2-2s}{2s}.M_{2s-1} \ , \\
M_{2s+1} &= (\Lambda + s\delta)M_{2s} + (n+1-2s).M_{2s-1}.
\end{aligned}$$

Assim se $n = 2s+1$ é ímpar , $M_{n+1} = M_{2s+2}$ tem que ser nulo , que é impossível. Logo temos que n é par, $n = 2s$, e $M_{n+1} = M_{2s+1} = 0$, que implica $\Lambda = \delta = 0$, pois $M_{2s} > 0 \Rightarrow \Lambda + s\delta = 0 \Rightarrow \Lambda = 0$ e, como $s > 0$, $\delta = 0$.

Agora podemos concluir que se existe uma solução estritamente algébrica para a equação $y' = y^2 - p$, então p seria uma constante e o coeficiente $a = \sigma_1$ seria zero. Nesse caso F teria grau par $n = 2s$ e pelo sistema em $\overline{\sigma_j}$, temos (substituindo os coeficientes em (Σ)), $\sigma_2 = -s$, logo $4\sigma_4 = -(2s+2-4)\sigma_2 \Rightarrow \sigma_4 = \frac{-2(s-1)}{4}(-s) = \frac{s(s-1)}{2}$, e vemos que $\sigma_{2j} = (-1)^j \binom{s}{j}$. Então F teria a forma $(y^2 - p)^s$ e como F é irredutível, então F seria igual a $y^2 - p$, com p uma constante, mas o corpo k é algebricamente fechado, logo temos uma contradição.

Portanto provamos que a equação $y' = y^2 - p$, onde p é um polinômio não nulo, não tem solução estritamente algébrica.

No caso $p = 0$, a análise local também nos dará $\Lambda = 0$, significando $\sigma_1 = a = 0$, e então todos os σ_j serão nulos, que é uma contradição, e nossa prova está concluída.

■

Como consequência do teorema anterior vamos apresentar uma série de resultados que permitirão dar exemplos de famílias de derivações simples e quadráticas. Portanto em alguns resultados vamos necessitar da hipótese de que k é algebricamente fechado.

O primeiro resultado geral e fundamental que apresentaremos é sobre a simplicidade da derivação Δ_p de $k[x,y]$, com $p = p(x) \in k[x]$, lembramos que tal k-derivação é definida da seguinte forma: $\Delta_p(x) = 1$ e $\Delta_p(y) = y^2 - p(x)$.

Teorema 3.2.13 : *Se a derivação Δ_p não é simples e k é um corpo algebricamente fechado, então existe um polinômio de Darboux F, em $k[x,y]$, de Δ_p tal que* $\deg_y F = 1$.

Demonstração : Sabemos que Δ_p não é simples. Se $p = 0$, então $F = y$ é um polinômio de Darboux de Δ_p, pois $\Delta_p(F) = y^2 = y.y$. Assim podemos supor $p \neq 0$.

Como Δ_p não é simples, e $\Delta_p(x) = 1$, então a proposição 3.2.3 nos garante a existência de um polinômio de Darboux F de Δ_p. Evidentemente $F \notin k[x]$, pois $\Delta_p(x) = 1$, e assim se $F \in k[x]$ teríamos $\Delta_p(F) = \frac{\partial F}{\partial x} = H.F$, que é um absurdo, pois F é não constante.

Assim $\deg_y F \geq 1$ e o corolário 3.2.9 nos garante a existência de uma função algébrica $r \in \overline{k(x)}$ tal que $r' = r^2 - p$. Isso siginifica que a equação $y' = y^2 - p$ tem uma solução algébrica. Mas, pelo teorema 3.2.12, tal equação não possui solução em $\overline{k(x)} \setminus k(x)$, portanto a equação $y' = y^2 - p$ tem uma solução $y \in k(x)$. Agora, como $p \neq 0$, então $y \neq 0$, e assim, pela proposição 3.2.11, temos que a derivação Δ_p tem um polinômio de Darboux $F \in k[x,y]$ tal que $\deg_y F = 1$.

■

Claro que a recíproca deste resultado acima é válida, pois se existe um polinômio de Darboux F, em $k[x,y]$, de Δ_p tal que $\deg_y F = 1$, então $\Delta_p(F) \subseteq (F)$, e portanto Δ_p não é simples.

O resultado a seguir nos dará uma família de derivações do tipo Δ_p que são simples.

Teorema 3.2.14 : *Se $p = p(x)$ é um polinômio não nulo de grau ímpar, então Δ_p é simples.*

Demonstração : Iniciamos observando que a proposição 2.2.2 nos garante que $k[x,y]$ é Δ_p simples se, e somente se, $\bar{k}[x,y]$ é Δ_p simples, onde $\bar{k}$ é o fecho algébrico de k. Assim podemos supor que k é algébricamente fechado. Agora suponhamos que Δ_p não é simples, então o teorema 3.2.11 nos diz que existe um polinômio de Darboux $F \in k[x,y]$ de Δ_p, com $\deg_y F = 1$. Seja $\Lambda \in k[x,y]$ o autovalor correspondente, isto é, Λ é tal que

$\Delta_p(F) = \Lambda.F$. Com isso a proposição 3.2.10 (itens 1 e 4) nos diz que $\Lambda = y + s$, com $s \in k[x]$, e que $\deg p = 2.\deg s$, e assim o grau de p seria par, que contradiz nossa hipótese que diz que o grau de p é ímpar.

Portanto temos que Δ_p tem que ser simples, se o grau de p for ímpar.

■

A proposição que veremos agora nos garante a simplicidade de Δ_p para uma família específica de $p = p(x)$.

Proposição 3.2.15 : *Se d é uma derivação de $k[x,y]$ tal que $d(x) = 1$ e $d(y) = y^2 \pm x^n$, $0 \neq n \in \mathbb{N}$, então d é simples.*

Demonstração : Fazendo a mesma observação feita na prova do teorema anterior podemos supor que k é algebricamente fechado.

O caso n ímpar é teorema anterior.

Portanto podemos assumir que $n = 2m$, onde $0 \neq m \in \mathbb{N}$. Suponhamos que d não seja simples. Logo, pelo teorema 3.2.13, temos que existe um polinômio de Darboux F, em $k[x,y]$, de d tal que $\deg_y F = 1$, ou seja, $F = u.y + v$, onde $u, v \in k[x]$, $u \neq 0$. Assim pela proposição 3.2.10 (item 3) temos que: $(*)$ $u'' - s'u - 2su' + s^2u - pu = 0$ para $p = \pm x^{2m}$, e algum $0 \neq s \in k[x]$ com $\deg s = m$ (pelo item 4 da mesma prop.3.2.10).

Seja $s = s_m.x^m + \ldots + s_1.x + s_0$, onde $s_0, s_1, \ldots, s_m \in k$ e $s_m \neq 0$.

Agora comparando os coeficientes das potências de x em $(*)$, vemos que $s_m^2 = \mp 1$ e que $s_{m-1} = s_{m-2} = \ldots = s_0 = 0$. Portanto temos que $s = s_m.x^m$, e substituindo este em $(*)$ temos a seguinte igualdade : $(**)$ $u'' - m.s_m x^{m-1}u - 2s_m.x^m u' = 0$

Fazendo uma comparação com os coeficientes das potências de x em $(**)$ obtemos a seguinte igualdade: $m + 2\deg u = 0$, que é um absurdo, pois $m > 0$. Logo temos que d tem que ser simples.

■

Veremos agora um exemplo onde a derivação Δ_p não é simples.

Exemplo 3.2.16 : *Toda derivação Δ_p onde p tem a forma $p = p(x) = x^{2m} - m.x^{m-1}$, onde $0 \neq m \in \mathbb{N}$, não é simples.*

Demonstração : De fato , sabemos que neste exemplo a derivação Δ_p tem a forma: $\Delta_p(x) = 1$ e $\Delta_p(y) = y^2 - p = y^2 - x^{2m} + m.x^{m-1}$, onde $0 \neq m \in \mathbb{N}$.

Vejamos que o polinômio $F = y - x^m$ é um polinômio de Darboux de Δ_p.

$$\Delta_p(F) = \Delta_p(y - x^m) = \Delta_p(y) - \Delta_p(x^m)$$
$$= y^2 - x^{2m} + m.x^{m-1} - m.x^{m-1}$$
$$= y^2 - x^{2m} = (y + x^m).(y - x^m) = (y + x^m).F$$

Assim temos que $F = y - x^m$ é um polinômio de Darboux de Δ_p, e portanto ela não é simples.

■

Muitas vezes pode-se deduzir a simplicidade de uma derivação através de uma outra derivação que sabemos ser simples. Vamos iniciar tal estudo com a seguinte definição:

Definição 3.2.17 : *Duas derivações d e δ de $k[x,y]$ são ditas equivalentes se existe um k-automorfismo de k-álgebras σ de $k[x,y]$ tal que $\delta = \sigma d \sigma^{-1}$.*

Claramente, se d e δ são equivalentes temos que d é simples se, e somente se, δ é simples.

Os dois resultados a seguir giram em torno deste conceito.

Proposição 3.2.18 : *Sejam $a, b, \varphi \in k[x]$ e sejam d e δ derivações de $k[x,y]$ definidas por:* $d(x) = 1$, $d(y) = y^2 - ay + b$ e

$$\delta(x) = 1 \quad , \quad \delta(y) = y^2 + (2\varphi + a)y + b + \varphi^2 + a\varphi - \varphi'$$

Então d e δ são equivalentes.

Demonstração : Consideremos o automorfismo $\sigma : k[x,y] \to k[x,y]$ tal que $\sigma(x) = x$ e $\sigma(y) = y + \varphi$. Vejamos que $\delta = \sigma d \sigma^{-1}$.

De fato , $\sigma d \sigma^{-1}(y) = \sigma d(y - \varphi) = \sigma(d(y) - \varphi') = \sigma(y^2 + ay + b - \varphi')$

$$= \sigma(y^2) + \sigma(ay) + \sigma(b) - \sigma(\varphi')$$
$$= (y + \varphi)^2 + a(y + \varphi) + b - \varphi'$$
$$= y^2 + 2\varphi y + \varphi^2 + ay + a\varphi + b + \varphi'$$
$$= y^2 + (2\varphi + a)y + b + \varphi^2 + a\varphi - \varphi' = \delta(y)$$

E $\sigma d \sigma^{-1}(x) = \sigma d(x) = \sigma(1) = 1 = \delta(x)$

Logo $\delta = \sigma d \sigma^{-1}$, e portanto d e δ são equivalentes.

■

Proposição 3.2.19 : *Seja* $d : k[x,y] \to k[x,y]$ *uma derivação tal que :* $d(x) = 1$ *e* $d(y) = y^2 + ay + b$, *onde* $a,b \in k[x]$. *Essa derivação é equivalente a derivação* Δ_p , *onde* $p = \frac{1}{4}(a^2 - 4b) - \frac{1}{2}a'$.

Demonstração : Tomando a,b do enunciado e mais $\varphi = -\frac{a}{2}$, podemos verificar que, neste caso, $\delta = \Delta_p$, onde δ é dado pela proposição anterior e p é o dado na presente proposição. Logo temos o que queríamos.

■

O teorema a seguir diz respeito a simplicidade da k-derivação d de $k[x,y]$, dada por: $d(x) = 1$ e $d(y) = y^2 + ay + b$, onde $a,b \in k[x]$.

Teorema 3.2.20 : *Seja* $d : k[x,y] \to k[x,y]$ *uma derivação tal que:* $d(x) = 1$ *e* $d(y) = y^2 + ay + b$, *onde* $a,b \in k[x]$. *A derivação d não é simples se, e somente se, existe um polinômio de Darboux F de d tal que* $\deg_y F = 1$.

Demonstração : Seja $F \in k[x,y]\backslash k$, e tome $p = \frac{1}{4}(a^2 - 4b) - \frac{1}{2}a'$ (como na proposição 3.2.19), assim temos que d e Δ_p são equivalentes. Logo d não é simples se, e somente se, Δ_p não é simples. Mais ainda $\Delta_p = \sigma d \sigma^{-1}$, onde $\sigma(x) = x$ e $\sigma(y) = y - \frac{a}{2}$. Isso implica que F é um polinômio de Darboux de d se, e somente se, $\sigma(F)$ é um polinômio de Darboux de Δ_p . E $\deg_y F = 1$ se, e somente se, $\deg_y \sigma(F) = 1$ (pois σ preserva o grau de y). Agora o teorema 3.2.13 nos diz que a derivação Δ_p não é simples se, e só se, existe um polinômio de Darboux G, em $k[x,y]$, de Δ_p tal que $\deg_y G = 1$. Sendo $G = \sigma(F)$, temos o que queríamos.

■

O próximo resultado dá condições sobre $a,b \in k[x,y]$ para que uma k-derivação do tipo dado na proposição anterior seja simples.

Teorema 3.2.21 : *Seja* $d : k[x,y] \to k[x,y]$ *uma derivação tal que:* $d(x) = 1$ *e* $d(y) = y^2 + ay + b$, *onde* $a,b \in k[x]$ e $b \neq 0$. *Se* $\deg b$ *é ímpar e* $a = 0$ *ou* $\deg b > 2\deg a$, *então d é simples.*

Demonstração : Sabemos, pela proposição 3.2.19, que d e Δ_p são equivalentes, onde $p = \frac{1}{4}(a^2 - 4b) - \frac{1}{2}a'$. Assim d é simples se, e somente se, Δ_p é simples. Agora como $\deg b > 2\deg a$, então p tem o mesmo grau que b, logo o grau de p é ímpar , pois $\deg b$ é ímpar. Portano o teorema 3.2.14 nos garante que Δ_p é simples , e então d é simples.

■

O que estudaremos agora são casos da derivação Δ_p, onde $\deg p = 2$, ou seja $p = Ax^2 + Bx + C$, onde $A, B, C \in k$. Mostraremos que nestes casos o problema da simplicidade da derivação Δ_p se reduz ao mesmo problema para derivações δ_r, para $r \in k$, onde $\delta_r = \Delta_{x^2-r}$, isto é, δ_r é a derivação de $k[x,y]$ definida por: $\delta_r(x) = 1$ e $\delta_r(y) = y^2 - x^2 + r$.

Iniciamos nossos estudos com os seguintes lemas.

Lema 3.2.22 : *Sejam $p = p(x) \in k[x]$, $\alpha \in k$ e seja $q(x) = p(x + \alpha)$. Então as derivações Δ_p e Δ_q são equivalentes.*

Demonstração : Considere σ o k-automorfismo de $k[x,y]$ dado por $\sigma(x) = x + \alpha$ e $\sigma(y) = y$. Logo temos que:

$\sigma\Delta_p\sigma^{-1}(y) = \sigma\Delta_p(y) = \sigma(y^2 - p) = y^2 - \sigma(p) = y^2 - p(x + \alpha) = \Delta_q(y)$ e;

$\sigma\Delta_p\sigma^{-1}(x) = \sigma\Delta_p(x - \alpha) = \sigma(\Delta_p(x) - \Delta_p(\alpha))$

$= \sigma(1 - 0) = \sigma(1) = 1 = \Delta_q(x)$

Portanto temos que $\Delta_q = \sigma\Delta_p\sigma^{-1}$, ou seja, Δ_p e Δ_q são equivalentes.

■

Lema 3.2.23 : *Sejam $p = p(x) \in k[x]$, $0 \neq \beta \in k$ e $r(x) = \beta^2 p(\beta x)$. Então Δ_p é simples se, e somente se, Δ_r é simples.*

Demonstração : Cosidere o k-automorfismo σ de $k[x,y]$ definido por: $\sigma(x) = \beta x$ e $\sigma(y) = \beta^{-1} y$. Pode-se verificar facilmente que $\sigma\Delta_p\sigma^{-1} = \beta^{-1}\Delta_r$, assim temos o que queríamos.

■

Para os próximos quatro lemas vamos assumir que k é corpo algebricamente fechado e que $p = Ax^2 + Bx + C$, onde $A, B, C \in k$ e $A \neq 0$, e consideraremos a derivação $d = \Delta_p$. Sendo k algebricamente fechado podemos tomar $\gamma \in k \setminus \{0\}$ tal que $A\gamma^4 = 1$. Seja $r = r(x) = \gamma^2 p(\gamma x)$. Logo temos que : $r(x) = \gamma^2(A^2\gamma^2 x^2 + B\gamma x + C) = x^2 + \gamma^3 Bx + \gamma^2 C$.

Dessa maneira vemos que podemos assumir $A = 1$, na derivação d, definida como acima, para estudarmos o problema da simplicidade de d. E mais, o lema 3.2.23 nos garante que podemos assumir que d é da forma δ_r, para $r \in k$.

Os três lemas que veremos a seguir serão utilizados na prova do segundo resultado mais importante desta seção que é o teorema 3.2.27 que será visto após os lemas.

Lema 3.2.24 : *Se* F *e* Λ *são polinômios em* $k[x,y]$ *tais que* $\delta_r(F) = \Lambda.F$, $F \neq 0$ *e* $\deg_y F = 1$, *então* $\Lambda = y \pm x$.

Demonstração : Como $\deg_y F = 1$, então podemos escrever $F = u.y + v$, onde $u, v \in k[x]$ e $u \neq 0$. De acordo com o proposição 3.2.10 (itens 1 e 4) $\Lambda = y + s$ para algum $s \in k[x]$ de grau 1 (pois aqui $\deg p = 2$). Logo podemos escrever $s = ax + b$, onde $a, b \in k$ e $a \neq 0$. Agora pelo item 3 da mesma proposição 3.2.10 (com $s = ax + b$) temos as seguintes igualdades, que denotaremos por $(*)$: $u' = v + (ax + b)u$ e $v' + (-x^2 + r)u = (ax + b)v$

Sejam u^* e v^* os coeficientes líderes dos polinômios u e v, respectivamente. Assim $u^* \neq 0$ e $v^* \neq 0$, e pelas igualdades $(*)$ acima temos que: $v^* = -axu^*$ e $axv^* = -x^2u^*$, logo, como $a \neq 0$, $v^* = -\frac{xu^*}{a} = -axu^* \Rightarrow a^2 = 1 \Rightarrow a = \pm 1$

Portanto já temos que $\Lambda = y \pm x + b$. Agora vejamos que $b = 0$.

Denotando $g = axu + v$, escrevemos $(*)$ como: $u' = ub + g$ e $(r - a)u + g' = (2ax + b)g$. Assim se $b \neq 0$, então pela igualdade $u' = ub + g$, temos $\deg(g) = \deg(u)$, pois $\deg u' < \deg u$. Mas se $\deg(g) = \deg(u)$ temos uma contradição com a igualdade $(r - a)u + g' = (2ax + b)g$, pois como $r, a, b \in k$, temos dessa igualdade que $\deg u = 1 + \deg g$. Portanto concluímos que $b = 0$, e assim $\Lambda = y \pm x$.

■

Lema 3.2.25 : *Se* $r \in k$. *A derivação* δ_r *tem um polinômio de Darboux* F *tal que* $\deg_y F = 1$ *se, e somente se, existe um polinômio não nulo* $u \in k[x]$ *tal que:* $u'' - 2xu' + (r - 1)u = 0$ *ou* $u'' + 2xu' + (r + 1)u = 0$.

Demonstração : $\Rightarrow$) Sabemos que a derivação δ_r tem um polinômio de Darboux F tal que $\deg_y F = 1$. Assim seja $F = u.y + v$, onde $u, v \in k[x]$ e $u \neq 0$, o polinômio de Darboux de δ_r, e Λ tal que $\delta_r(F) = \Lambda.F$. O lema 3.2.24 nos diz que $\Lambda = y \pm x$, e assim pela proposição 3.2.10 (item 3) temos que $v = u' - axu$ e $v' = axv + (x^2 - r)u$, onde $a = \pm 1$. Portanto temos:

Se $a = 1$, substituindo $v = u' - xu$ em $v' = xv + (x^2 - r)u$, temos que: $u'' - 2xu' + (r - 1)u = 0$.

Se $a = -1$, substituindo $v = u' + xu$ em $v' = -xv + (x^2 - r)u$, temos que: $u'' + 2xu' + (r + 1)u = 0$.

$\Leftarrow$) Sabemos que existe um polinômio não nulo $u \in k[x]$ tal que: $u'' - 2xu' + (r - 1)u = 0$ ou $u'' + 2xu' + (r + 1)u = 0$.

Se $u'' - 2xu' + (r - 1)u = 0$, tomando $F = u.y + (u' - xu)$, então :

$$\begin{aligned}\delta_r(F) &= \delta_r(u.y + (u' - xu)) = \delta_r(u.y) + \delta_r(u' - xu) \\ &= u'y + u(y^2 - x^2 + r) + u'' - u - xu' \\ &= u'' + (y - x)u' + uy^2 - ux^2 + u(r - 1) ,\end{aligned}$$

Agora usando o fato de que $u'' - 2xu' + (r - 1)u = 0$, temos que $u'' + (r - 1)u = 2xu'$ e assim teremos que $\delta_r(F) = (y + x)u' + uy^2 - ux^2 = (x + y).F$. Portanto temos que a derivação δ_r tem um polinômio de Darboux F tal que $\deg_y F = 1$.

Se $u'' + 2xu' + (r+1)u = 0$, tomando $F = u.y + (u' + xu)$ teremos de maneira análoga ao caso anterior que $\delta_r(F) = (y-x)u' + uy^2 - ux^2 = (y-x).F$.

■

Lema 3.2.26 : *Seja $r \in k$. A derivação δ_r tem um polinômio de Darboux F tal que $\deg_y F = 1$ se, e somente se, r é um inteiro ímpar.*

Demonstração : $\Rightarrow$) Sabemos que a derivação δ_r tem um polinômio de Darboux F tal que $\deg_y F = 1$, logo, pelo lema 3.2.25, temos que existe um polinômio não nulo $u \in k[x]$ que satisfaz uma das seguintes igualdades: $u'' - 2xu' + (r-1)u = 0$ ou $u'' + 2xu' + (r+1)u = 0$

Sem perda de generalidade, pois k é corpo, podemos assumir que u é um polinômio mônico, ou seja, $u = x^s + a_{s-1}x^{s-1} + \cdots + a_1x + a_0$, onde $s \geq 1$ e $a_0, \ldots, a_{s-1} \in k$.

Se $u'' - 2xu' + (r-1)u = 0$, então comparando os coeficientes de x^s nessa igualdade, temos que $-2s + (r-1) = 0$, e portanto $r = 2s+1$, ou seja, r é um inteiro ímpar.

Se $u'' + 2xu' + (r+1)u = 0$, fazendo a comparação dos coeficientes de x^s nessa igualdade teremos $2s + (r+1) = 0$, assim $r = -2s - 1$, logo r é um inteiro ímpar.

$\Leftarrow$) Sabemos, por hipótese, que r é um ímpar. Vamos supor primeiro que $r = 2s+1$, com $s \in \mathbb{N}$. Seja u_s um polinômio mônico de grau s definido, indutivamente, em $k[x]$ da seguinte maneira: $u_0 = 1$, $u_1 = x$ e para $s \geq 2$, $u_s = a_s x^s + a_{s-1}x^{s-1} + \cdots + a_1x + a_0$, onde $a_s = 1$, $a_{s-1} = 0$ e $a_i = \frac{(i+1)(i+2)}{2(i-s)}.a_{i+2}$, para $i = 0, 1, \ldots, s-2$.

Vejamos que, para todo s , u_s satisfaz a igualdade : $u_s'' - 2xu_s' + (r-1)u_s = 0$

De fato , se $s = 0$, então $r = 1$ e $u_0 = 1$, e assim a igualdade é satisfeita.

Para $s = 1$, então $r = 3$ e $u_1 = x$, logo temos:

$u_1'' - 2xu_1' + (r-1)u_1 = 0 - 2x + (3-1)x = 0$, e portanto a igualdade é satisfeita .

Para $s \geq 2$, temos $r = 2s+1$ e $u_s = a_s x^s + a_{s-1}x^{s-1} + \cdots + a_1x + a_0$, onde $a_s = 1$, $a_{s-1} = 0$ e $a_i = \frac{(i+1)(i+2)}{2(i-s)}.a_{i+2}$, para $i = 0, 1, \ldots, s-2$. Olhando para a forma dos coeficientes de x^i , temos que : para i ímpar , $a_{s-i} = 0$ e $a_{s-2} = \frac{(s-1)s}{-4}$, $a_{s-4} = \frac{(s-3)(s-2)(s-1)s}{(-4)(-8)}$, ...

Assim temos que :

$$u_s'' = s(s-1)x^{s-2} + (s-3)(s-2)a_{s-2}x^{s-4} + \ldots + 3.4.a_4x^2 + 2a_2$$

$$2xu_s' = 2x[sx^{s-1} + (s-2)a_{s-2}x^{s-3} + \ldots + 4a_4x^3 + 2a_2x]$$
$$= 2sx^s + 2(s-2)a_{s-2}x^{s-2} + \ldots + 8a_4x^4 + 4a_2x^2$$

$$(r-1)u_s = (2s+1-1)u_s = 2su_s$$
$$= 2sx^s + 2sa_{s-2}x^{s-2} + \ldots + 2sa_2x^2 - 2a_2 \quad (\text{pois } a_0 = \tfrac{a_2}{-s})$$

Substituindo estes valores em $u_s'' - 2xu_s' + (r-1)u_s$, teremos :

$$u_s'' - 2xu_s' + (r-1)u_s = [s(s-1)x^{s-2} + (s-3)(s-2)a_{s-2}x^{s-4} + \ldots + 3.4.a_4x^2 + 2a_2] +$$
$$+ [-2sx^s - 2(s-2)a_{s-2}x^{s-2} - \ldots - 8a_4x^4 - 4a_2x^2]$$
$$+ [2sx^s + 2sa_{s-2}x^{s-2} + \ldots + 2sa_2x^2 - 2a_2]$$

E vemos que $u_s'' - 2xu_s' + (r-1)u_s = 0$. Logo o lema 3.2.25 nos garante a existência de

um polinômio de Darboux F de δ_r tal que $\deg_y F = 1$.

Agora para o caso $r = -2s-1$, com $s \in \mathbb{N}$. De maneira similar ao que fizemos anteriormente tomamos v_s um polinômio mônico de grau s definido em $k[x]$ da seguinte maneira: $v_0 = 1$, $v_1 = x$ e para $s \geq 2$, $v_s = a_s x^s + a_{s-1}x^{s-1} + \cdots + a_1 x + a_0$, onde $a_s = 1$, $a_{s-1} = 0$ e $a_i = -\dfrac{(i+1)(i+2)}{2(i-s)}.a_{i+2}$, para $i = 0, 1, \ldots, s-2$.

Repetindo o que foi feito anteriormente verificamos que para todo s, v_s satisfaz a igualdade: $v_s'' + 2xv_s' + (r+1)v_s = 0$ e portanto o lema 3.2.25 nos garante a existência de um polinômio de Darboux F de δ_r tal que $\deg_y F = 1$.

■

O resultado abaixo nos dá mais uma grande família de k-derivações simples e quadráticas de $k[x,y]$, a saber as do tipo Δ_{x^2-r} com $r \in k$ e r não sendo inteiro ímpar.

Teorema 3.2.27 : *Seja $r \in k$. A derivação δ_r não é simples se, e somente se, r é um inteiro ímpar.*

Demonstração : Iniciamos observando que passando o fecho algébrico de k e usando a proposição 2.2.2 podemos supor k algebricamente fechado e portanto podemos usar todos os lemas provados anteriormente.

$\Rightarrow$) Sabemos que a derivação $\delta_r = \Delta_{x^2-r}$ não é simples. Assim o teorema 3.2.13 nos garante a existência de um polinômio de Darboux F de δ_r tal que $\deg_y F = 1$. Com isso pelo lema 3.2.26 temos que r é um inteiro ímpar.

$\Leftarrow$) Sabemos que r é um inteiro ímpar. Logo o lema 3.2.26 nos diz que existe um polinômio de Darboux F de δ_r tal que $\deg_y F = 1$.

■

Usando os lemas 3.2.24 , 3.2.25 e 3.2.26 podemos dar o seguinte exemplo :

Exemplo 3.2.28 : Se $r = 1,3,5,7$ então $\delta_r(F) = (y+x)F$, onde F é dada da seguinte forma:

Para $r = 1$, temos $F = y - x$;

De fato , $\delta_1(F) = \delta_1(y-x) = \delta_1(y) - \delta_1(x) = y^2 - x^2 + 1 - 1$
$= y^2 - x^2 = (y+x)F$

Para $r = 3$, podemos verificar de maneira análoga que $F = xy - x^2 + 1$;

Para $r = 5$, podemos verificar de maneira análoga que $F = (2x^2 - 1)y - 2x^3 + 5x$;

Do mesmo modo para $r = 7$, tem-se que $F = (2x^3 - 3x)y - 2x^4 + 9x^2 - 3$.

Para encerrar este capítulo vamos apresentar alguns resultados que nos garante que k-derivações simples de $k[x,y]$ podem gerar interessantes k-derivações simples de anéis de polinômios em muitas variáveis.

O que será visto a seguir são duas consequências do teorema de Shamsuddin (teorema 3.1.2), tais resultados dizem respeito a derivações de $k[x,y,z]$.

Proposição 3.2.29 : *Seja* $d : k[x,y,z] \to k[x,y,z]$ *uma derivação tal que:* $d(x) = 1$; $d(y) = f(x,y)$ *e* $d(z) = y$, *onde* $f(x,y) \in k[x,y]$, $\deg_y f(x,y) \geq 2$. *Seja* $\delta : k[x,y] \to k[x,y]$ *a restrição de* d *em* $k[x,y]$. *Se* δ *é simples, então* d *é simples.*

Demonstração : Aqui vamos usar o teorema de Shamsuddin (teorema 3.1.2) tomando $R = k[x,y]$ e $t = z$. assim como δ é a restrição de d a R e $d(t) = d(z) = y$ dizer δ é simples é equivalente a dizer que não existe $r \in R = k[x,y]$ tal que $\delta(r) = y$. Vamos supor por absurdo que exista um $r \in k[x,y]$ tal que $\delta(r) = y$, logo $\deg_y r \geq 1$. Assim, seja $r = r_n y^n + \ldots + r_1 y + r_0$, onde $n \geq 1$, $r_0, \ldots, r_n \in k[x]$ e $r_n \neq 0$.

Mas podemos escrever $f(x,y)$ da seguinte forma: $f(x,y) = f_m y^m + \ldots + f_1 y + f_0$, onde $m \geq 2$, $f_0, \ldots, f_m \in k[x]$ e $f_m \neq 0$. Então temos :

$$y = \delta(r) = d(r) = r_n' y^n + \ldots + r_1' y + r_0' + (n r_n y^{n-1} + \ldots + r_1).f(x,y)$$
$$= r_n' y^n + \ldots + r_1' y + r_0' + (n r_n y^{n-1} + \ldots + r_1).(f_m y^m + \ldots + f_1 y + f_0)$$

Agora comparando os coeficientes de y^{m+n-1} temos a seguinte contradição $0 = n r_n f_m \neq 0$, pois $n \geq 1$, $r_n \neq 0$ e $f_m \neq 0$.

Portanto vimos que não existe $r \in k[x]$ tal que $\delta(r) = y$, e assim o teorema de Shamsuddin (teorema 3.1.2) nos garante que d é simples.

■

Proposição 3.2.30 : *Seja* $d : k[x,y,z] \to k[x,y,z]$ *uma derivação tal que:* $d(x) = 1$, $d(y) = g(x,y)$ *e* $d(z) = a(x)z + b(x)y + c(x)$, *onde* $g(x,y) \in k[x,y]$, $\deg_y g(x,y) = 2$, $a(x), b(x), c(x) \in k[x]$ *e* $b(x) \neq 0$. *Seja* $\delta : k[x,y] \to k[x,y]$ *a restrição de* d *em* $k[x,y]$. *Se* δ *é simples , então* d *é simples.*

Demonstração : Usando a mesma argumentação do início da proposição anterior vemos que dizer que d é simples é equivalente a dizer que não existe $r \in k[x,y]$ tal que $\delta(r) = a(x)r + b(x)y + c(x)$. Vamos supor que exista um $r \in k[x,y]$ tal que $\delta(r) = a(x)r + b(x)y + c(x)$. Como $b(x) \neq 0$, então temos que $\deg_y r \geq 1$. Seja $r = r_n y^n + \ldots + r_1 y + r_0$, onde $n \geq 1$, $r_0, \ldots, r_n \in k[x]$ e $r_n \neq 0$. E seja $g(x,y) = g_m y^m + \ldots + g_1 y + g_0$, onde $m \geq 2$, $g_0, \ldots, g_m \in k[x]$ e $g_m \neq 0$. Então temos :

$$a(x)r + b(x)y + c(x) = \delta(r) = d(r) = r_n' y^n + \ldots + r_1' y + r_0' + (n r_n y^{n-1} + \ldots + r_1).g(x,y)$$
$$= r_n' y^n + \ldots + r_1' y + r_0' + (n r_n y^{n-1} + \ldots + r_1)(g_m y^m + \ldots + g_1 y + g_0)$$

Agora comparando os coeficientes de y^{m+n-1} temos a seguinte contradição $0 = nr_n g_m \neq 0$, pois $n \geq 1$, $r_n \neq 0$ e $g_m \neq 0$.

Logo vimos que não existe $r \in k[x]$ tal que $\delta(r) = y$, e assim o teorema de Shamsuddin (teorema 3.1.2) nos garante que d é simples.

■

Para encerrar este capítulo podemos apresentar, com os mesmos argumentos utilizados nas demonstrações das duas proposições anteriores, dois exemplos de k-derivações simples do anel de polinômios com $n+3$ variáveis sobre o corpo k (n é um número natural qualquer).

Exemplo 3.2.31 : Seja d uma derivação de $k[x,y,z,t_1,\ldots,t_n]$ definida da seguinte maneira :

$d(x) = 1$,
$d(y) = y^2 + x$,
$d(z) = y$
$d(t_1) = zt_1 + 1$
$d(t_2) = t_1t_2 + 1$
$d(t_3) = t_2t_3 + 1$
$\vdots$
$d(t_n) = t_{n-1}t_n + 1$

Então d é simples .

De fato , seja γ a restrição de d em $k[x,y]$, ou seja $\gamma(x) = 1$ e $\gamma(y) = y^2 + x$, pelo teorema 3.2.21 temos que γ é simples. Seja δ_0 a restrição de d em $k[x,y,z]$ assim, como γ é simples, a proposição 3.2.29 nos garante que δ_0 também é simples.

Sabendo que a derivação $\delta_0 : k[x,y,z] \to k[x,y,z]$ é simples, vejamos que a restrição de d em $k[x,y,z,t_1]$, que denotaremos por δ_1, também será simples. Para isso usaremos os mesmos argumentos utilizados na demonstração da proposição 3.2.29, então vejamos:

Suponhamos que exista um $r \in k[x,y,z]$ tal que $\delta_0(r) = zr + 1$, assim vemos que $\deg_z r \geq 1$, logo podemos escrever $r = r_m z^m + \ldots + r_1 z + r_0$, onde $m \geq 1$, $r_0,\ldots,r_m \in k[x,y]$ e $r_m \neq 0$. Daí temos a seguinte igualdade:

$$\begin{aligned} zr + 1 = \delta_0(r) = d(r) &= d(r_m z^m + \ldots + r_1 z + r_0) \\ &= r_m' z^m + \ldots + r_1' z + r_0' + (mr_m z^{m-1} + \ldots + r_1).d(z) \\ &= r_m' z^m + \ldots + r_1' z + r_0' + (mr_m z^{m-1} + \ldots + r_1).y \end{aligned}$$

Assim analizando o coeficiente de z^{m+1}, temos a seguinte contradição: $0 = r_m \neq 0$. Portanto temos que não é possível existir um $r \in k[x,y,z]$ tal que $\delta_0(r) = zr + 1$, e então o teorema de Shamsuddin (teorema 3.1.2) nos garante que δ_1, que é a restrição de d em

$k[x,y,z,t_1]$, é simples.

De maneira completamente análoga se vê que a restrição de d em $k[x,y,z,t_1,\ldots,t_i]$, δ_i é simples para todo $i = 2,3,\ldots,n-1$. Aqui vamos mostrar que $\delta_n = d$ é simples, sabendo que δ_{n-1}, que é a a restrição de $\delta_n = d$ em $k[x,y,z,t_1,\ldots,t_{n-1}]$, é simples.

Suponhamos que exista um $r \in k[x,y,z,t_1,\ldots,t_{n-1}]$ tal que $\delta_{n-1}(r) = t_{n-1}r + 1$, assim vemos que $\deg_{t_{n-1}} r \geq 1$, logo podemos escrever $r = r_m t_{n-1}^m + \ldots + r_1 t_{n-1} + r_0$, onde $m \geq 1$, $r_0,\ldots,r_m \in k[x,y,z,t_1,\ldots,t_{n-2}]$ e $r_m \neq 0$. Daí temos a seguinte igualdade:

$$\begin{aligned} t_{n-1}r + 1 = \delta_{n-1}(r) &= d(r_m t_{n-1}^m + \ldots + r_1 t_{n-1} + r_0) \\ &= r_m' t_{n-1}^m + \ldots + r_1' t_{n-1} + r_0' + (m r_m t_{n-1}^{m-1} + \ldots + r_1).d(t_{n-1}) \\ &= r_m' t_{n-1}^m + \ldots + r_1' t_{n-1} + r_0' + (m r_m t_{n-1}^{m-1} + \ldots + r_1).(t_{n-2}t_{n-1} + 1) \end{aligned}$$

Agora analizando o coeficiente de t_{n-1}^{m+1}, temos a seguinte contradição: $0 = r_m \neq 0$. Logo não existe $r \in k[x,y,z,t_1,\ldots,t_{n-1}]$ tal que $\delta_{n-1}(r) = t_{n-1}r + 1$, portanto o teorema de Shamsuddin (teorema 3.1.2) nos garante que d é simples.

■

Exemplo 3.2.32 : Seja d uma derivação de $k[x,y,z,t_1,\ldots,t_n]$ definida da seguinte maneira :

$$\begin{aligned} d(x) &= 1, \\ d(y) &= y^2 + x^5 + 2x, \\ d(z) &= x^2 z + xy \\ d(t_1) &= z^2 t_1 + z \\ d(t_2) &= t_1^2 t_2 + t_1 \\ d(t_3) &= t_2^2 t_3 + t_2 \\ &\vdots \\ d(t_n) &= t_{n-1}^2 t_n + t_{n-1} \end{aligned}$$

Então d é simples .

A prova de que neste caso d é simples é absolutamente análoga a dada no exemplo anterior e portanto vamos omití-la.

Bibliografia

[1] Atiyah, M. F. , MacDonald, I.G. , "*Introduction to Commutative Algebra*", Addison-Wesley Publishing Company (1969).

[2] Coutinho, S. C. , "*d-simple rings and simple D-modules*", Math. Proc. Camb. Phil. Soc. 125 (1999), 405-415.

[3] Eisenbud, D. , "*Commutative Algebra With a View Toward Algebraic Geometry*", Springer-Verlag (1995).

[4] Hart, R. , "*Derivations on Regular Local Rings of Finitely Generated Type*", J. London Math. Soc. (2), 10 (1975).

[5] Kunz, E. , "*Introdution to Commutative Algebra and Algebraic Geometry*", Birkhauser Boston (1985).

[6] Lang, S. , "*Algebra*" , Addison-Wesley Publishing Company (1984).

[7] Lequain, Y. , "*Simple Shamsuddin derivations of $K[X_1,\ldots,X_n]$ and cyclic maximal left ideals of the Weyl Algebra $A_n(K)$*", pre-print.

[8] Lequain, Y. , Levcovitz, D. , Souza Junior, J.C. , "*D-simple rings and maximal ideals of the Weyl algebra*", pre-print.

[9] Maciejewski, A. , Moulin-Ollagnier, J. and Nowicki, A. , "*Simple Quadratic Derivations in Two Variables*", Communications in Algebra, 29 (11) , 2001.

[10] Nagata, M. , "*Local Rings*" , Interscience, Kyoto Univ. (1962).

[11] Nagata, M. , "*Field Theory*", Marcel Dekker (1977).

[12] Nowicki, A. , "*Polynomial Derivations and Their Rings of Constantes*", Uniwersytet Mikolaja Kopernika, Torun (1994).

[13] Seidenberg, A. , "*Differential Ideals in Rings of Finitely Generated Type*", Amer. J. Math. , 89 (1967).

[14] Stafford, J.T. , "*Non-holonomic modules over Weyl algebras*", Invent. Math. 79 (1985), 619-638.

[15] Zariski, O. , Samuel, P. , "*Commutative Algebra*", vol.1 , Springer-Verlag (1958).