Universidade Federal do Rio Grande do Sul

Derivações em Anéis Primos e Semiprimos

por
Claus Haetinger

março de 1994

"Se trabalharmos sobre o mármore, o trabalho perecerá. Se o fizermos sobre o metal, o tempo apagará. Se erguermos templos, eles desmoronarão, transformando-se em pó. Mas, se trabalharmos a inteligência imortal dos homens, se lhes incutirmos princípios elevados, gravaremos nessas placas algo que nenhum tempo poderá apagar e que brilhará por toda a eternidade". *Daniel Webster*

Ao exemplo do meu pai Armindo,
à memória de minha mãe Ingeborg,
e à minha noiva Rosmarie, aos quais
qualquer tentativa de agradecimento
seria insignificante em relação a tudo
o que significam para mim.

Dissertação submetida ao Curso de Pós-Graduação em Matemática da Universidade Federal do Rio Grande do Sul, sob orientação do Prof.Dr. Miguel Angel Alberto Ferrero, como requisito parcial para obtenção do grau de Mestre.

AGRADECIMENTOS:

Agradeço sinceramente ao Prof. Miguel, a orientação segura e paciente desde a Iniciação Científica bem como os constantes incentivos.

Do mesmo modo, agradeço à Profa. Cydara e ao Prof. Engler o pronto aceite em participar da banca, e as inúmeras sugestões.

Na pessoa dos Professores Miguel, Cydara e Vilmar, quero externar meu agradecimento a todos os Professores do Mestrado.

Agradecendo aos Professores Manoel, Antônio Carlos, Bedregal e Israel, expresso minha gratidão a todos os Professores e amigos de Recife.

Da mesma forma, minha gratidão aos Professores Clóvis, Porto, Cármen e Eduardo, é extensiva a todos os Professores do Bacharelado.

Particularmente, agradeço:

ao amigo e colega Prof. Ingo, a motivação e apoio;

ao Steffenon, o estímulo, amizade e a hilariante convivência desde os tempos de CEFAV;

à Virgínia, ao Alvino, Marilaine, Pedro, Malásquez e Flamarion, bem como aos demais colegas, a amizade sincera e estímulo;

ao Laboratório de Informática do CEAT, na pessoa do Prof. Hugo, como também aos amigos Carlos Alberto, Paulo e Marcelo, o auxílio no uso do LaTeX;

à minha família, o apoio;

a todo pessoal da Academia Stágio, a amizade e a preparação física e psicológica.

Finalmente, agradeço à **"Nega"** o amor, compreensão e carinho. Agradeço-lhe também agüentar meu mau-humor e, especialmente, perdoar minhas faltas durante esta fase final da dissertação.

A todos vocês, meu sincero **MUITO OBRIGADO**!

RESUMO

Esta dissertação é essencialmente sobre derivações em anéis. Inicialmente mostramos que toda derivação de Jordan num anel primo e livre de 2-torção é uma derivação usual. Depois disso, encontramos um resultado original, provando que toda derivação de Hasse-Schmidt-Jordan definida num anel semiprimo e livre de 2-torção é uma derivação de Hasse-Schmidt. Por último, trabalhamos com derivações algébricas d definidas num anel primo R (com unidade) e com suas respectivas extensões $d^\star$ ao anel de quocientes (à direita) de Martindale de R denotado por $\mathbf{Q}$. Neste ponto, demonstramos uma equivalência entre as R, $\mathbf{Q}$ e $\mathbf{C}$-algebricidades de d e de $d^\star$, onde $\mathbf{C}$ denota o centróide estendido de R.

ABSTRACT

This thesis is essentially about derivations on rings. First, we show that every Jordan derivation on a 2-torsion free prime ring is an ordinary derivation. After this, we obtain an original result, proving that every Hasse–Schmidt–
–Jordan derivation defined on a 2-torsion free semiprime ring is a Hasse–
–Schmidt derivation. At last, we work with algebraic derivations d defined on a prime ring R (with unity) and with their respectively extensions $d^\star$ to the ring of right quocients of Martindale of R denoted by $\mathbf{Q}$. In this point, we prove an equivalence among the R, $\mathbf{Q}$ and $\mathbf{C}$-algebricities of d and $d^\star$, where $\mathbf{C}$ denotes the extended centroid of R.

Introdução

O presente trabalho trata essencialmente sobre derivações em anéis. Nosso primeiro objetivo é a demonstração de um resultado de I.N.Herstein [8], segundo o qual toda derivação de Jordan em um anel primo e livre de 2-torção é uma derivação usual (teorema 1.1.2). Depois disto, generalizamos esta idéia, provando que toda derivação de Hasse-Schmidt-Jordan definida num anel semiprimo e livre de 2-torção é uma derivação de Hasse-Schmidt (teorema 2.2.1). Por último, trabalhamos com derivações algébricas d definidas num anel primo R (com unidade) e com suas respectivas extensões $d^\star$ ao anel de quocientes (à direita) de Martindale de R denotado por $\mathbf{Q}$. Neste ponto, demonstramos uma equivalência, devida a A.Leroy e J.Matczuk [16], entre as R, $\mathbf{Q}$ e $\mathbf{C}$-algebricidades de d e de $d^\star$ (teorema 3.2.13), onde $\mathbf{C}$ denota o centróide estendido de R.

No capítulo 0, apresentamos alguns tópicos que são pré-requisitos para a leitura do que segue. Dividimo-lo em três secções. Na primeira, revisamos alguns conceitos sobre anéis primos e semiprimos. A seguir, construímos o anel de quocientes (à direita) de Martindale $\mathbf{Q}$ de R, e o centróide estendido $\mathbf{C}$ de R, segundo W.Martindale [17]. Encerramos o capítulo introduzindo a noção de derivação em um anel, bem como demonstrando algumas propriedades elementares.

No capítulo 1, definimos as derivações de Jordan em um anel R qualquer. Na primeira secção, mostramos que, embora toda derivação seja uma derivação de Jordan, a recíproca nem sempre é verdadeira. Demonstramos ainda um teorema devido a I.N.Herstein [8], o qual afirma que se o anel é primo e livre de 2-torção, então toda derivação de Jordan é uma derivação. A seguir, provamos, segundo M. Bresăr [5], que, se o anel é semiprimo e livre de 2-torção, então vale a mesma equivalência acima.

No capítulo 2 generalizamos os resultados obtidos no capítulo 1, descobrindo condições sob as quais derivações de Hasse-Schmidt e derivações de Hasse-Schmidt--Jordan são equivalentes. O principal teorema deste capítulo prova que toda derivação de Hasse-Schmidt–Jordan definida num anel semiprimo e livre de 2-torção é uma derivação de Hasse-Schmidt, e foi obtido pelo autor desta dissertação.

No último capítulo seguimos o trabalho de A.Leroy e J.Matczuk [16]. Consideramos R um anel primo com unidade (não necessariamente comutativo), d uma derivação usual definida em R e $d^\star$ sua extensão a $\mathbf{Q}$. O capítulo trata das derivações algébricas sobre um anel. Estendemos um resultado de V.K.Kharchenko [13], segundo o qual se R tem característica zero, então toda derivação R-algébrica é X-interna, provando que R, $\mathbf{Q}$ e $\mathbf{C}$-algebricidades de d e de $d^\star$ são equivalentes (teorema 3.2.13).

Os resultados básicos da teoria de anéis podem ser vistos em N.H.McCoy [18], M.F.Atiyah [2], N.Bourbaki [3], J.Lambek [15], A.Jones [12] ou em I.N.Herstein [9].

Finalmente, a notação $\mathcal{I}_r$ indica ideais à direita de R, enquanto $\mathcal{I}$ indica ideais biláteros (neste caso diremos simplesmente ideais).

Índice

Capítulo 0

Prolegômenos

0.1 Anéis Primos e Semiprimos

Iniciamos lembrando algumas definições que serão usuais no que segue. Seja R um anel qualquer.

Definição 0.1.1 *O conjunto dos elementos $c \in R$ que comutam com todo elemento de R é denominado* CENTRO de R *e denotado por $Z(R)$. Em outras palavras*

$$Z(R) = \{c \in R \mid cr = rc \ \forall r \in R\}.$$

Definição 0.1.2 *Seja $\mathcal{I}_r$ um ideal à direita não-nulo de R. Diremos que o conjunto $\mathcal{W}_r$ é o* ANULADOR À DIREITA *de $\mathcal{I}_r$ se $\mathcal{W}_r = \{x \in R \mid \mathcal{I}_r x = 0\}$.*

Note que nestas condições também $\mathcal{W}_r$ é um ideal à direita de R.

Definição 0.1.3 *Um ideal $\mathcal{P}$ de R é dito* IDEAL PRIMO *de R se satisfaz a seguinte propriedade: se x e $y \in R$ são tais que $xRy \subseteq \mathcal{P}$, então $x \in \mathcal{P}$ ou $y \in \mathcal{P}$.*

O próximo teorema estabelece propriedades equivalentes à definição 0.1.3 . Sua demonstração pode ser encontrada em [18] (teorema 4.3).

Teorema 0.1.4 *Sejam R um anel e $\mathcal{P}$ um ideal de R. São equivalentes:*
(i) $\mathcal{P}$ é um ideal primo de R;
(ii) se $\mathcal{A}$ e $\mathcal{B}$ são ideais de R, tais que $\mathcal{AB} \subseteq \mathcal{P}$, então $\mathcal{A} \subseteq \mathcal{P}$ ou $\mathcal{B} \subseteq \mathcal{P}$;
(iii) se $\mathcal{U}_r$ e $\mathcal{V}_r$ são ideais à direita de R, tais que $\mathcal{U}_r\mathcal{V}_r \subseteq \mathcal{P}$, então $\mathcal{U}_r \subseteq \mathcal{P}$ ou $\mathcal{V}_r \subseteq \mathcal{P}$;
(iv) se $\mathcal{I}$ é um ideal de R e $b \in R$ é tal que $b\mathcal{I} \subseteq \mathcal{P}$ e $\mathcal{I} \not\subseteq \mathcal{P}$, então $b \in \mathcal{P}$.

Definição 0.1.5 *Um anel R é chamado* ANEL PRIMO *se o ideal $\mathcal{O} = \{0\}$ é um ideal primo de R. Isto é, se para quaisquer elementos x e $y \in R$*

$$xRy = 0 \Rightarrow x = 0 \ \ ou \ \ y = 0.$$

Corolário 0.1.6 *As seguintes condições são equivalentes:*
(i) R é um anel primo;
(ii) se $0 \neq \mathcal{H}$ é um ideal de R tal que $a\mathcal{H}b = 0$ para a, $b \in R$, então $a = 0$ ou $b = 0$;
(iii) dados dois ideais $\mathcal{A}$ e $\mathcal{B}$ de R tais que $\mathcal{AB} = (0)$, então $\mathcal{A} = (0)$ ou $\mathcal{B} = (0)$;
(iv) o anulador à direita $\mathcal{W}_r$ de um ideal à direita não-nulo $\mathcal{I}_r$ de R é zero.

prova : $(i) \rightarrow (ii)$ Como $a\mathcal{H}b = 0$, $a\mathcal{H}Rb = 0$. Se $b \neq 0$, por definição temos que $a\mathcal{H} = 0$, donde $aR\mathcal{H} = 0$. Como $\mathcal{H} \neq (0)$, segue que $a = 0$.

$(i) \leftrightarrow (iv)$ Suponhamos que $xRy = 0 \Rightarrow x = 0$ ou $y = 0$ para todo x, $y \in R$. Sejam $0 \neq \mathcal{I}_r$ um ideal à direita de R e $\mathcal{W}_r$ seu anulador à direita. Pelo teorema 0.1.4 (iii), $\mathcal{I}_r\mathcal{W}_r = (0) \Rightarrow \mathcal{W}_r = (0)$. Reciprocamente, suponhamos $xRy = 0$ com $x \neq 0$. Como $0 \neq xR$ é um ideal à direita de R, $(xR)y = 0 \Rightarrow y = 0$, pela hipótese.

As outras implicações são evidentes. □

Definição 0.1.7 *Diremos que um anel R é* LIVRE DE 2-TORÇÃO *se para qualquer $x \in R$ tivermos $2x = 0 \Rightarrow x = 0$.*

Definição 0.1.8 *Diremos que um anel R é* SEMIPRIMO *se, para todo $a \in R$, $aRa = 0 \Rightarrow a = 0$.*

Observe que todo anel primo é semiprimo.

Lema 0.1.9 *Sejam R um anel semiprimo livre de 2-torção e a, $b \in R$. Se para qualquer $x \in R$ $axb + bxa = 0$, então $axb = bxa = 0$.*

prova : Sejam a, $b \in R$. Por hipótese, $azb + bza = 0$ para todo $z \in R$, isto é, $azb = -bza$. Então, para x, $y \in R$,

$$\begin{aligned} [a(x)b]yaxb &= (-bxa)yaxb = -[b(xay)a]xb = \\ &= -[-a(xay)b]xb = ax[a(y)b]xb = \\ &= ax(-bya)xb = -axbyaxb. \end{aligned}$$

Portanto, $2(axb)y(axb) = 0$ para todo $x, y \in R$.

Uma vez que R é livre de 2-torção, segue que $(axb)y(axb) = 0$ para todo $y \in R$ e, por ser R um anel semiprimo, concluimos que $axb = 0$ para todo $x \in R$. Logo, pela hipótese, $bxa = 0$ para todo $x \in R$. □

Note que, se R é primo, então livre de 2-torção é equivalente a característica $\neq 2$. Mas, em geral, dizer que um anel tem característica $\neq 2$ não é o mesmo que dizer que o anel é livre de 2-torção, conforme:

Exemplo 0.1.10 *Consideremos o anel Z_4 dos inteiros módulo 4. Ora, é evidente que Z_4 tem característica $\neq 2$. No entanto, temos $2 \cdot \overline{2} = \overline{4} = \overline{0}$ com $\overline{2} \neq \overline{0}$. Logo Z_4 não é livre de 2-torção.*

Definição 0.1.11 *Sejam R um anel e x um elemento não-nulo de R. Diremos que x é* NILPOTENTE *se existir um número natural n (não-nulo) tal que $x^n = 0$. O menor n tal que $x^n = 0$ é dito o* ÍNDICE DE NILPOTÊNCIA *do elemento $x \in R$.*

Lema 0.1.12 *Sejam R um anel semiprimo e $Z(R)$ o seu centro. Então $Z(R)$ não contém elementos nilpotentes não-nulos.*

prova : De fato, suponhamos por absurdo que exista um elemento não-nulo $x \in Z(R)$ nilpotente de índice n.

Se $n = 2$, então para todo $r \in R$ temos $x^2r = 0$. Como $x \in Z(R)$, temos $0 = x^2r = xrx$. Mas, R é semiprimo. Logo $x = 0$, uma contradição.

Se $n > 2$, então $(x^{n-1})^2 = 0$, pois $2n - 2 > n$. Portanto, $(x^{n-1})^2r = 0$ para todo $r \in R$ e $x^{n-1}rx^{n-1} = 0$. Donde $x^{n-1} = 0$, uma contradição.

Conseqüentemente, $Z(R)$ não contém elementos nilpotentes não-nulos. □

Definição 0.1.13 *Sejam R um anel e $a \in R$. Definimos $\mathcal{T}(a)$ por*

$$\mathcal{T}(a) = \{r \in R \mid r(ax - xa) = 0, \ \forall x \in R\}$$

Lema 0.1.14 *Sejam R um anel e $a \in R$. Então $\mathcal{T}(a)$ é um ideal bilátero de R.*

prova : Claramente $\mathcal{T}(a)$ é um ideal à esquerda de R. Resta-nos mostrar que, se $u \in \mathcal{T}(a)$ e $x \in R$, então $ux \in \mathcal{T}(a)$.

Visto que $u \in \mathcal{T}(a)$, temos que, para $xr \in R$ vale $u(axr - xra) = 0$. Portanto, $u[(ax - xa)r + x(ar - ra)] = 0$. Novamente, $u \in \mathcal{T}(a)$ fornece-nos $u(ax - xa) = 0$. Assim sendo, $ux(ar - ra) = 0$ para todo $r \in R$. Então $ux \in \mathcal{T}(a)$ e o lema está provado. □

Lema 0.1.15 *Sejam R um anel primo e $a \in R$. Se $a \notin Z(R)$, então $\mathcal{T}(a) = (0)$.*

prova : Visto que $a \notin Z(R)$, existe algum $b \in R$ tal que $ab - ba \neq 0$.
Se $\mathcal{T}(a) \neq 0$, como $\mathcal{T}(a)\,(ab - ba) = (0)$, o ideal $\mathcal{T}(a)$ seria anulado por um elemento não-nulo, contrariando o fato do anel R ser primo, conforme corolário 0.1.6 (iv). Por conseguinte, $\mathcal{T}(a) = (0)$. □

O resultado a seguir caracteriza anéis **primos** livres de 2-torção.

Teorema 0.1.16 *Seja R um anel livre de 2-torção. Então são equivalentes:*
(i) R é um anel primo;
(ii) se $a, b \in R$ e $axb + bxa = 0\ \forall x \in R$, então $a = 0$ ou $b = 0$;
(iii) se $a, b \in R$ e $axa = bxb\ \forall x \in R$, então $a = b$ ou $a = -b$.

demonstração : $(i) \to (ii)$ É conseqüência imediata do lema 0.1.9.
$(ii) \to (i)$ Suponhamos (ii) e que para todo $y \in R$ vale $ayb = 0$. Então, $(bxa)y(bxa) + (bxa)y(bxa) = 2bx(ayb)xa = 2bx(0)xa = 0$ para todo x, $y \in R$ donde, pela hipótese (ii), $bxa = 0$ para todo $x \in R$. Portanto, $axb + bxa = 0$ para todo $x \in R$. Logo, por (ii), $a = 0$ ou $b = 0$, e R é primo.
$(ii) \to (iii)$ Suponhamos $axa = bxb$ para todo $x \in R$. Neste caso, $(a-b)x(a+b)+(a+b)x(a-b) = 0$ para todo $x \in R$. Por (ii), $a-b = 0$ ou $a+b = 0$. Sendo assim, $a = b$ ou $a = -b$.
$(iii) \to (ii)$ Suponhamos $axb + bxa = 0$ para todo $x \in R$. Conseqüentemente, $(a - b)x(a - b) = (a + b)x(a + b)$ para todo $x \in R$. Portanto, por (iii), $a - b = a + b$ ou $a - b = -(a + b)$.
Visto que R é livre de 2-torção, segue que $a = 0$ ou $b = 0$. □

<u>Nota</u>: Para provar $(ii) \to (i)$ e $(ii) \to (iii)$ não utilizamos o fato de R ser livre de 2-torção.

0.2 Anel de Quocientes (à direita) de Martindale

Seja R um anel primo com unidade. Aqui construímos o anel de quocientes (à direita) de Martindale de R, denotando-o por $\boldsymbol{Q}$. No caso particular em que R é um domínio de integridade (comutativo), $\boldsymbol{Q}$ coincide com o corpo de frações de R. Já no final, definimos o centróide estendido de R.

Seja $\mu = \{\mathcal{U}\}$ a coleção de todos os ideais biláteros não-nulos de R e seja $\boldsymbol{T}$ o conjunto de todos os R-homomorfismos $f : \mathcal{U}_R \to R_R$, com $\mathcal{U}$ percorrendo μ, onde $\mathcal{U}$ e R são tomados como R-módulos à direita ($f(ar) = f(a)r$ para todo $a \in \mathcal{U}$ e para todo $r \in R$).

Denotaremos os elementos $\mathcal{U}$ de μ por $\mathcal{U} \lhd R$ e os elementos $f : \mathcal{U}_R \to R_R$ de $\boldsymbol{T}$ por $(\mathcal{U}, f)$.

Observação 0.2.1 *Seja $\mathcal{U} \in \mu$. Como R é primo com unidade, temos, para todo $r \in R$, $r\mathcal{U} = 0 \Rightarrow r = 0$. Conseqüentemente, se $\mathcal{U}$, $\mathcal{V} \in \mu$, então $\mathcal{UV}$ e $\mathcal{U} \cap \mathcal{V}$ estão em μ.*

Definição 0.2.2 *Sejam $\mathcal{U}, \mathcal{V} \in \mu$ e $(\mathcal{U}, f), (\mathcal{V}, g) \in T$. Diremos que $(\mathcal{U}, f)$ é equivalente a $(\mathcal{V}, g)$ (e denotaremos $(\mathcal{U}, f) \sim (\mathcal{V}, g)$) se existir um ideal $\mathcal{W} \in \mu$ tal que $\mathcal{W} \subseteq \mathcal{U} \cap \mathcal{V}$ satisfazendo $(\mathcal{W}, f\,|_{\mathcal{W}}) = (\mathcal{W}, g\,|_{\mathcal{W}})$.*

Observação 0.2.3 Se existe tal $\mathcal{W}$, então $f\,|_{\mathcal{U}\cap\mathcal{V}} = g\,|_{\mathcal{U}\cap\mathcal{V}}$.

De fato, para todo $w \in \mathcal{W}$, temos $f(w) = g(w)$. Seja $x \in \mathcal{U} \cap \mathcal{V}$. Como $\mathcal{W} \lhd R$, temos $xw \in \mathcal{W}$. Logo, $f(xw) = g(xw)$, donde $f(x)w = g(x)w$. Em outras palavras, $(f(x) - g(x))w = 0$ para todo $w \in \mathcal{W}$. Pelo corolário 0.1.6 (ii), $f(x) - g(x) = 0$, isto é, $f(x) = g(x)$ para todo $x \in \mathcal{U} \cap \mathcal{V}$.

É fácil ver que a definição 0.2.2 define uma relação de equivalência sobre $\boldsymbol{T}$. Seja $\boldsymbol{Q}$ o conjunto de todas as classes de equivalência determinadas por esta relação. Dado $(\mathcal{U}, f) \in \mathbf{T}$, denotamos por $[\mathcal{U}, f]$ a classe de equivalência de $(\mathcal{U}, f)$.

Agora podemos definir em $\boldsymbol{Q}$ as operações de adição e multiplicação como segue:

Definição 0.2.4 *Dados $[\mathcal{U}, f], [\mathcal{V}, g] \in \mathbf{Q}$, definimos as seguintes operações:*
(i) $[\mathcal{U}, f] + [\mathcal{V}, g] = [\mathcal{U} \cap \mathcal{V}, f + g]$;
(ii) $[\mathcal{U}, f][\mathcal{V}, g] = [\mathcal{VU}, f \circ g]$.

Verifiquemos que estas operações estão bem definidas. Sejam $[\mathcal{U}, f] = [\mathcal{U}', f']$ e $[\mathcal{V}, g] = [\mathcal{V}', g']$ pertencentes a $\boldsymbol{Q}$. Assim, existem $\mathcal{W}, \mathcal{W}' \in \mu$, tais que $\mathcal{W} \subseteq \mathcal{U} \cap \mathcal{U}'$ e $\mathcal{W}' \subseteq \mathcal{V} \cap \mathcal{V}'$, satisfazendo $f|_{\mathcal{W}} = f'|_{\mathcal{W}}$ e $g|_{\mathcal{W}'} = g'|_{\mathcal{W}'}$. Logo, $(f + g)(a) = (f' + g')(a)$ para todo $a \in \mathcal{W} \cap \mathcal{W}'$, ou seja, $(\mathcal{W} \cap \mathcal{W}', f + g) = (\mathcal{W} \cap \mathcal{W}', f' + g')$. Como $\mathcal{W} \cap \mathcal{W}' \subseteq \mathcal{U} \cap \mathcal{V} \cap \mathcal{U}' \cap \mathcal{V}'$, obtemos que $[\mathcal{U} \cap \mathcal{V}, f + g] = [\mathcal{U}' \cap \mathcal{V}', f' + g']$. Portanto, a adição está bem definida.

Antes de provarmos a boa definição da multiplicação, convém observar que faz sentido falarmos em $[\mathcal{VU}, f \circ g]$, ou equivalentemente, em $f \circ g : \mathcal{VU} \to R$, pois $g(\mathcal{VU}) \subseteq g(\mathcal{V})\mathcal{U} \subseteq \mathcal{U}$.

Tomemos $a \in \mathcal{W}'\mathcal{W}$ $(\subseteq (\mathcal{V} \cap \mathcal{V}')(\mathcal{U} \cap \mathcal{U}'))$. Assim, $a \in \mathcal{W}'\mathcal{W} \Rightarrow a = \sum_i w_i' w_i \Rightarrow$ $\Rightarrow g(a) = \sum_i g(w_i')w_i \in \mathcal{W}$. Como $a \in \mathcal{W}'$, segue que $g(a) = g'(a)$.

Como $[\mathcal{U}, f] = [\mathcal{U}', f']$ e $g'(a) \in \mathcal{W}$, temos que $f(g'(a)) = f'(g'(a))$. Ademais, $g(a) = g'(a) \in \mathcal{W}$, donde $f(g(a)) = f(g'(a))$. Conseqüentemente,

$$(f \circ g)(a) = f(g(a)) = f(g'(a)) = f'(g'(a)) = (f' \circ g')(a)$$

e agora é fácil ver que $[\mathcal{U}, f][\mathcal{V}, g] = [\mathcal{U}', f'][\mathcal{V}', g']$. □

Mostremos que $\boldsymbol{Q}$, munido destas operações, é um anel.

Proposição 0.2.5 $(\mathbf{Q}, +, \cdot)$ *é um anel com unidade.*

prova : Sejam $[\mathcal{U}, f]$, $[\mathcal{V}, g]$, $[\mathcal{W}, h] \in \mathbf{Q}$.

(i) associatividade da adição

$([\mathcal{U}, f] + [\mathcal{V}, g]) + [\mathcal{W}, h] = [\mathcal{U} \cap \mathcal{V}, f + g] + [\mathcal{W}, h] = [\mathcal{U} \cap \mathcal{V} \cap \mathcal{W}, (f + g) + h] =$
$= [\mathcal{U} \cap \mathcal{V} \cap \mathcal{W}, f + (g + h)] = [\mathcal{U}, f] + [\mathcal{V} \cap \mathcal{W}, g + h] = [\mathcal{U}, f] + ([\mathcal{V}, g] + [\mathcal{W}, h])$.

(ii) comutatividade da adição

$[\mathcal{U}, f] + [\mathcal{V}, g] = [\mathcal{U} \cap \mathcal{V}, f + g] = [\mathcal{V} \cap \mathcal{U}, g + f] = [\mathcal{V}, g] + [\mathcal{U}, f]$.

(iii) $[R, 0]$ é o elemento neutro da adição, onde $\mathbf{0}$ denota a aplicação $0 : R \to R$ tal que $0(r) = 0$ para cada $r \in R$. Temos:

$$[R, 0] + [\mathcal{U}, f] = [R \cap \mathcal{U}, 0 + f] = [\mathcal{U}, f].$$

(iv) $[\mathcal{U}, -f]$ é o elemento simétrico de $[\mathcal{U}, f]$ em relação à adição, pois

$$[\mathcal{U}, -f] + [\mathcal{U}, f] = [\mathcal{U}, -f + f] = [\mathcal{U}, 0] = [R, 0].$$

(v) A associatividade da multiplicação mostra-se com argumentos análogos aos usados em (i).

(vi) Para provar que a multiplicação é distributiva em relação à adição, tomamos $\mathcal{L} = (\mathcal{V} \cap \mathcal{W})\mathcal{U} \subseteq \mathcal{VU} \cap \mathcal{WU}$ e é fácil ver que $[\mathcal{L}, f \circ (g + h)] = [\mathcal{L}, f \circ g + f \circ h]$ e segue a distributividade. □

Definição 0.2.6 *O anel* $\boldsymbol{Q}$ *é dito o* ANEL DE QUOCIENTES (À DIREITA) DE MARTINDALE DE R.

Proposição 0.2.7 *Sejam R um anel primo com unidade e $\boldsymbol{Q}$ o anel de quocientes (à direita)de Martindale de R. Então $R \subseteq Q$.*

prova : Consideremos o homomorfismo de anéis $\varphi : R \to \mathbf{Q}$ definido por $\varphi(a) = [R, a_l]$ para todo $a \in R$, onde $a_l : R_R \to R_R$ é definido por $a_l(r) = ar$ para cada $r \in R$ (multiplicação à esquerda). Verifiquemos que φ é um monomorfismo. Sejam $a, b \in R$. Então temos que $(a+b)_l = a_l + b_l$, pois dado $r \in R$, $(a+b)_l(r) = = (a+b)r = ar + br = a_l(r) + b_l(r) = (a_l + b_l)(r)$. Logo,

$$\varphi(a+b) = (a+b)_l = a_l + b_l = \varphi(a) + \varphi(b).$$

Analogamente, $(ab)_l = a_l \circ b_l$ e assim $\varphi(ab) = \varphi(a)\varphi(b)$.

Concluimos que φ é um homomorfismo de R em $\boldsymbol{Q}$.

Suponhamos que $[R, a_l] = 0$ para algum $a \in R$. Segue que $ar = 0$ para todo $r \in R$, e então $a = 0$, pois $1 \in R$. Isto é, $\ker(\varphi) = 0$, e então φ é injetivo. Logo,

$$R \simeq \varphi(R) \subseteq \mathbf{Q}.$$

A prova está completa. □

Para simplificar a notação, consideraremos sempre $R \subseteq \mathbf{Q}$, identificando cada $a \in R$ com $[R, a_l] \in \mathbf{Q}$.

Lema 0.2.8 *Seja $(\mathcal{U}, f) \in \mathbf{T}$. Então para qualquer $u \in \mathcal{U}$, temos $f \circ u_l = (f(u))_l$. Em particular, $[\mathcal{U}, f][R, u_l] = [R, (f(u))_l]$.*

prova : Como $f : \mathcal{U}_R \to R_R$, então para cada $u \in \mathcal{U}$ e $x \in R$ obtemos

$$f \circ u_l(x) = f(u_l(x)) = f(ux) = (f(u))x = (f(u))_l(x).$$

Assim, $f \circ u_l = (f(u))_l$. Agora,

$$[\mathcal{U}, f][R, u_l] = [R\mathcal{U}, f \circ u_l] = [\mathcal{U}, f \circ u_l] = [\mathcal{U}, (f(u))_l] = [R, (f(u))_l]. \ \square$$

Lema 0.2.9 *Seja $q \in \mathbf{Q}$ e seja $(\mathcal{U}, f) \in \mathbf{T}$ tal que $q = [\mathcal{U}, f]$. Então, $qu = f(u)$, para todo $u \in \mathcal{U}$.*

prova : Se $u \in \mathcal{U}$, temos que $qu = qu_l = [\mathcal{U}, f][R, u_l] = [R, (f(u))_l] = (f(u))_l$, para todo $u \in \mathcal{U}$. □

O lema acima poderia ter sido enunciado da seguinte forma:

Lema 0.2.10 *Seja $\mathcal{U} \in \mu$ e seja $f : \mathcal{U} \to R$ um homomorfismo de R-módulos à direita. Então $\exists q \in \mathbf{Q}$ tal que $qu = f(u)$ para qualquer $u \in \mathcal{U}$.*

prova : Tomemos $q = [\mathcal{U}, f] \in \mathbf{Q}$. Logo, como na prova do lema 0.2.9, $qu = (f(u))_l$ para todo $u \in \mathcal{U}$. □

O próximo corolário nos mostra uma propriedade importante de $\boldsymbol{Q}$, que será doravante muito utilizada.

Corolário 0.2.11 *Seja $q \in \mathbf{Q}$ e seja $(\mathcal{U}, f) \in \mathbf{T}$ tal que $q = [\mathcal{U}, f]$. Então, $q\mathcal{U} \subseteq R$. Em particular, para qualquer $q \in \mathbf{Q}$ existe $\mathcal{U} \in \mu$ tal que $q\mathcal{U} \subseteq R$.*

prova : É claro do lema 0.2.9. □

Corolário 0.2.12 *Para quaisquer $q_1, \cdots, q_n \in \mathbf{Q}$, existe $\mathcal{U} \in \mu$ tal que $q_i\mathcal{U} \subseteq R$ para cada $i \in \{1, \cdots, n\}$.*

prova : Para cada $i \in \{1, \ldots, n\}$ consideramos $\mathcal{U}_i \in \mu$ tal que $q_i\mathcal{U}_i \subseteq R$. Então $\mathcal{U} = \bigcap_{i=1}^{n} \mathcal{U}_i$ satisfaz a condição do corolário. □

Lema 0.2.13 *Seja $q \in \mathbf{Q}$ e $\mathcal{U} \in \mu$. Se $q\mathcal{U} = 0$, então $q = 0$.*

prova : Seja $q = [\mathcal{V}, f] \in \mathbf{Q}$. Por hipótese, $q(\mathcal{U} \cap \mathcal{V}) = 0$. Logo, pelo lema 0.2.8, $f \mid_{\mathcal{U}\cap\mathcal{V}} = 0$. Conseqüentemente,

$$q = [\mathcal{V}, f] = [\mathcal{U} \cap \mathcal{V}, f \mid_{\mathcal{U}\cap\mathcal{V}}] = [\mathcal{U} \cap \mathcal{V}, 0] = [R, 0] = 0. \ \square$$

Consideremos agora um subanel $\mathbf{M}$ de Q que contém R (R primo) e vejamos que M é também um anel primo.

Proposição 0.2.14 *Se $\mathbf{Q} \supseteq \mathbf{M} \supseteq R$, então M é primo. Em particular, $\mathbf{Q}$ é um anel primo.*

prova : Suponhamos que existam $q \neq 0$ e $p \neq 0$ em M tais que $q\mathbf{M}p = 0$. Do corolário 0.2.11, existem $\mathcal{U}, \mathcal{V} \in \mu$ satisfazendo $q\mathcal{U} \subseteq R$ e $p\mathcal{V} \subseteq R$, pois $\mathbf{M} \subseteq \mathbf{Q}$. Do fato de q e p serem não-nulos, existem $u \in \mathcal{U}$ e $v \in \mathcal{V}$, com $qu \neq 0$ e $pv \neq 0$. Como R é primo, temos $0 \neq (qu)R(pv) \subseteq (qRp)v = 0$, uma contradição. Logo, $\mathbf{M}$ é um anel primo. □

Definição 0.2.15 *O conjunto* $V_{\mathbf{Q}}(R) = \{q \in \mathbf{Q} \mid qr = rq, \ \forall r \in R\}$ *formado pelos elementos* $q \in \mathbf{Q}$ *que comutam com todo* $r \in R$ *é denominado* CENTRALIZADOR DE R EM $\mathbf{Q}$.

Denotamos por $\mathbf{C}$ *o* CENTRO DE $\mathbf{Q}$.

Vejamos o

Lema 0.2.16 *Seja* $q = [\mathcal{U}, f] \in \mathbf{Q}$. *As seguintes condições são equivalentes:*
(i) $q \in \mathbf{C}$;
(ii) $f : \mathcal{U} \to R$ *é um homomorfismo de* R- *bimódulos;*
(iii) $q \in V_{\mathbf{Q}}(R)$.

prova : $(i) \to (iii)$ Imediato.

$(iii) \to (ii)$ Seja $q = [\mathcal{U}, f] \in V_{\mathbf{Q}}(R)$. Sabemos que $f(u) = qu$ para todo $u \in \mathcal{U}$, pelo lema 0.2.10. Como $\mathcal{U} \lhd R$ bilátero, segue que $ru \in \mathcal{U}$ para todo $r \in R$. Visto que $q \in V_{\mathbf{Q}}(R)$, $f(ru) = q(ru) = (qr)u = (rq)u = r(qu) = rf(u)$. Logo, f é também homomorfismo de R-bimódulos à esquerda e segue o resultado.

$(ii) \to (i)$ Seja f é um homomorfismo de R-bimódulos. Então $f(ru) = rf(u)$ para todos $r \in R$ e $u \in \mathcal{U}$. Mas, como vimos acima, $f(ru) = qru$ e $rf(u) = rqu$, donde $qru = f(ru) = rf(u) = rqu$. Ou seja, $(qr - rq)u = 0$ para todo $u \in \mathcal{U}$. Pelo lema 0.2.13, segue que $qr - rq = 0$ para todo $r \in R$. Portanto, $q \in V_{\mathbf{Q}}(R)$.

Seja agora $p \in \mathbf{Q}$ não-nulo. Temos que $\exists\, 0 \neq \mathcal{V} \lhd R$ tal que $p\mathcal{V} \subseteq R$. Seja $v \in \mathcal{V}$ de modo que $0 \neq pv \in R$. Como $pv \in R$ e $q \in V_{\mathbf{Q}}(R)$, segue que $q(pv) = (pv)q = p(vq) = p(qv)$, pois $v \in R$. Logo, $(qp)v = (pq)v$, donde $(qp - pq)v = 0$ para todo $v \in \mathcal{V}$. Conseqüentemente, $pq - qp = 0$, ou seja, $q \in \mathbf{C}$. □

Mostremos a seguir que $\mathbf{C}$ é um **corpo**.

Sejam $0 \neq a \in \mathbf{C}$ e $b \in \mathbf{Q}$. Suponhamos que $ab = 0$. Então $0 = \mathbf{Q}ab = a\mathbf{Q}b$. Como $\mathbf{Q}$ é primo, $b = 0$. Logo, nenhum elemento de $\mathbf{C}$ é um divisor de zero em $\mathbf{Q}$. Em particular, $\mathbf{C}$ é um domínio de integridade comutativo.

Observamos que se, $c = [\mathcal{U}, f] \in \mathbf{C}$, então pelo lema 0.2.16, podemos considerar f um homomorfismo de R-bimódulos.

Proposição 0.2.17 $\mathbf{C}$ *é um corpo.*

prova : Basta verificar que todo $0 \neq c \in \mathbf{C}$ tem inverso multiplicativo em $\mathbf{C}$. Sabemos que existe $(0) \neq \mathcal{U} \lhd R$ tal que $c\mathcal{U} \subseteq R$ (corolário 0.2.11). Assim, pelo lema 0.2.13, $0 \neq c\mathcal{U} \lhd R$ e a função $g : cu \rightsquigarrow u$ de $c\mathcal{U}$ em R induz um elemento $d = [c\mathcal{U}, g] \in \mathbf{Q}$. Pelo lema 0.2.9, temos $d(ca) = g(ca) = a$ para todo $ca \in c\mathcal{U}$. Portanto $d(cu) = u$ para cada $u \in \mathcal{U}$. Logo, $(dc-1)\mathcal{U} = 0$. Pelo lema 0.2.13, $dc = 1$, o que completa a prova. □

Definição 0.2.18 *O corpo* $\mathbf{C}$ *é chamado de* CENTRÓIDE ESTENDIDO DE R. *O subanel* S *de* $\mathbf{Q}$ *gerado por* R *e* $\mathbf{C}$, *isto é,* $S = R\mathbf{C}$, *é dito a* CLAUSURA CENTRAL DE R.

A proposição a seguir nos mostra que todo anel contido em $\mathbf{Q}$ e que contenha a clausura central de R, tem como centro exatamente o centro de $\mathbf{Q}$.

Proposição 0.2.19 *Seja* $\mathbf{M}$ *um subanel de* $\mathbf{Q}$ *contendo* S. *Então* $Z(\mathbf{M}) = \mathbf{C}$.

prova : Seja $c \in Z(\mathbf{M})$. Portanto $cm = mc$ para todo $m \in \mathbf{M}$. Como $R \subseteq \mathbf{M}$, $cr = rc$ para todo $r \in R$. Logo $c \in V_{\mathbf{Q}}(R)$ e, pelo lema 0.2.16, $c \in \mathbf{C}$. Assim, $Z(\mathbf{M}) \subseteq \mathbf{C}$.

A outra inclusão é óbvia, desde que $1 \in R$ e portanto $Z(\mathbf{M}) = \mathbf{C}$. □

Lema 0.2.20 *Se* $0 \neq a \in \mathbf{Q}$, *então* $aRaR \cap R \neq 0$.

prova : Sendo $a \neq 0$, $aR \neq 0$. Como R é primo, segue que $aRaR \neq 0$. Logo basta provar que se $\mathcal{J}_r$ é um ideal à direita não-nulo de R, $\mathcal{J}_r \cap R \neq 0$. De fato, tome $0 \neq q \in \mathcal{J}_r$ e $0 \neq \mathcal{U} \lhd R$ tal que $q\mathcal{U} \subseteq R$. □

Lema 0.2.21 *Se* $a, b \in \mathbf{Q}$ *são tais que* $aRb = 0$, *então* $a = 0$ *ou* $b = 0$.

prova : Pelo corolário 0.2.11 exitem $\mathcal{U}$, $\mathcal{V} \in \mu$ tais que $a\mathcal{U} \subseteq R$ e $b\mathcal{V} \subseteq R$. Se $aRb = 0$, então $a\mathcal{U}Rb\mathcal{V} = 0$. Como R é primo, segue que $a\mathcal{U} = 0$ ou $b\mathcal{V} = 0$. Assim, $a = 0$ ou $b = 0$ (lema 0.2.13). □

Lema 0.2.22 *Se a_i, b_i, $1 \leq i \leq m$, são elementos não-nulos de* $\mathbf{Q}$ *tais que* $\sum_{i=1}^{m} a_i x b_i = 0$ *para todo* $x \in R$, *então os* a_i*'s e os* b_i*'s são linearmente dependentes sobre* $\mathbf{C}$.

prova : Mostraremos que os a_i's são linearmente dependentes sobre $\mathbf{C}$. Caso contrário, existem um n minimal e elementos $a_1, \cdots, a_n \in R$ linearmente independentes sobre $\mathbf{C}$ tais que $\sum_{i=1}^{n} a_i x b_i = 0$ para todo $x \in R$ e para alguns b_i's, onde os b_i's são elementos não-nulos de R. Visto que R é primo, $n > 1$. Suponhamos que x_j, $y_j \in R$ são tais que $\sum x_j b_1 y_j = 0$.

Se $r \in R$, então $0 = \sum_j a_1 r x_j b_1 y_j = -\sum_{i=2}^{n} a_i r \left(\sum_j x_j b_i y_j\right)$, uma vez que $\sum_{i=1}^{n} a_i r x_j b_i = 0$. Como temos uma relação mais curta do que n, concluimos que $\sum_j x_j b_i y_j = 0$ para todo i. Por conseguinte, a aplicação

$$\gamma_i : Rb_1R \to R$$

$$\sum_j u_j b_1 v_j \rightsquigarrow \sum_j u_j b_i y_j \text{ é bem definida.}$$

Pode-se mostrar que γ_i é um homomorfismo de R-módulos do ideal Rb_1R em R, donde γ_i define um elemento – que denotaremos ainda por γ_i – pertencente a $\mathbf{Q}$. Não é difícil mostrar que γ_i pertence a $\mathbf{C}$, pois é um homomorfismo de R-bimódulos. Ademais, por esta definição, $\gamma_i b_1 = b_i$. Então, para todo $x \in R$,

$$0 = \sum_i a_i x b_i = \sum_i a_i x \gamma_i b_1 = \left(\sum_i \gamma_i a_i\right) x b_i.$$

Como $\mathbf{R}$ é primo, segue que $\sum \gamma_i a_i = 0$ (lema 0.2.21). Visto que os a_i's são linearmente independentes sobre $\mathbf{C}$, resulta que $\gamma_i = 0$. Neste caso, $Rb_iR = 0$ pela definição de γ_i, donde $b_i = 0$, contradição. Isto prova o lema. □

Lema 0.2.23 *Seja* $0 \neq q \in \mathbf{Q}$ *tal que* $qR = Rq$ *(globalmente). Então* q *é um elemento inversível.*

prova : Pelo corolário 0.2.11 existe $0 \neq \mathcal{I} \lhd R$ tal que $q\mathcal{I} \subseteq R$.

Afirmação : $q\mathcal{I}$ é um ideal bilátero ($q\mathcal{I}_R \lhd R_R$ é um subgrupo abeliano de R).

Dados $i \in \mathcal{I}$ e $r \in R$, temos $q(i) \cdot r = q(ir) \in q\mathcal{I}$ e então $q\mathcal{I}$ é um ideal à direita. Por hipótese, $qR = Rq$, donde $rq\mathcal{I} \subseteq qR\mathcal{I} \subseteq q\mathcal{I}$, desde que $\mathcal{I}$ é um ideal bilátero de R. Logo $q\mathcal{I}$ também é ideal de R à esquerda. Como $q\mathcal{I}$ é ideal bilátero, podemos utilizá-lo como domínio de definição de uma aplicação $\varphi : q\mathcal{I} \to R$ tal que $\varphi(q.i) = i$.

Note que φ é um homomorfismo à direita bem definido.

De fato, se $qi = qi'$ para i, $i' \in \mathcal{I}$, então $q(i - i') = 0$ e $Rq(i - i') = 0$. Pela hipótese podemos concluir que $qR(i - i') = 0$. Assim, via lema 0.2.21, segue que $i - i' = 0$, donde $i = i'$.

Podemos verificar facilmente que $\varphi \circ q_l = id_{\mathcal{I}}$ e $q_l \circ \varphi = id_{q\mathcal{I}}$. Logo a aplicação φ define um elemento q' tal que $qq' = q'q = 1$. □

0.3 Derivações em Anéis

Definição 0.3.1 *Seja R um anel. Uma aplicação $d : R \to R$ é dita uma* DERIVAÇÃO *se, para quaisquer a e b de R, tivermos:*
1. $d(a + b) = d(a) + d(b)$;
2. $d(ab) = d(a)b + ad(b)$.

A condição 1. nos diz que d é uma aplicação aditiva em R.

Proposição 0.3.2 *Sejam $n \in \mathbf{N}$ e $d : R \to R$ uma derivação em R. Então $d^n(yx) = \sum_{i=0}^{n} \binom{n}{i} d^i(y)d^{n-i}(x)$ para todo x, $y \in R$.*

prova : Procederemos por indução sobre n.

Para $\underline{n = 1}$, como d é uma derivação segue que $d(yx) = yd(x) + d(y)x$ para todo x, $y \in R$. Aplicando d a esta expressão, obtemos

$$\begin{aligned} d^2(yx) &= d(d(yx)) = d(yd(x) + d(y)x) = d(yd(x)) + d(d(y)x) = \\ &= yd^2(x) + d(y)d(x) + d(y)d(x) + d^2(y)x = \\ &= yd^2(x) + 2d(y)d(x) + d^2(y)x \text{ para todo } x, y \in R. \end{aligned}$$

Suponhamos agora que, para todo x, $y \in R$ e para todo $m < n$, vale

$$d^m(yx) = \sum_{i=0}^{m} \binom{m}{i} d^i(y)d^{m-i}(x). \text{ Então,}$$

$$\begin{aligned} d^{m+1}(yx) &= d(d^m(yx) = d\left(\textstyle\sum_{i=0}^{m} \binom{m}{i} d^i(y)d^{m-i}(x)\right) = \\ &= \textstyle\sum_{i=0}^{m} \binom{m}{i} d^i(y)d^{m-i+1}(x) + \sum_{i=0}^{m} \binom{m}{i} d^{i+1}(y)d^{m-i}(x) = \\ &= \textstyle\sum_{i=0}^{m} \binom{m}{i} d^i(y)d^{m-i+1}(x) + \sum_{i=1}^{m+1} \binom{m}{i-1} d^i(y)d^{m-i+1}(x) = \\ &= yd^{m+1}(x) + \textstyle\sum_{i=1}^{m} \binom{m}{i} d^i(y)d^{m-i+1}(x) + \sum_{i=1}^{m} \binom{m}{i-1} d^i(y)d^{m-i+1}(x) + d^{m+1}(y)x. \end{aligned}$$

Lembrando a *relação de Stiffel*: $\binom{m+1}{i} = \binom{m}{i-1} + \binom{m}{i}$, temos

$$\begin{aligned} d^{m+1}(yx) &= yd^{m+1}(x) + \sum_{i=1}^{m}\binom{m+1}{i}d^i(y)d^{m-i+1}(x) + d^{m+1}(y)x = \\ &= \sum_{i=0}^{m+1}\binom{m+1}{i}d^i(y)d^{m+1-i}(x). \end{aligned}$$

Logo, por indução, segue que $d^n(yx) = \sum_{i=0}^{n}\binom{n}{i}d^i(y)d^{n-i}(x)$ para todo $n \in \mathbf{N}$ e quaisquer x, $y \in R$. $\square$

Capítulo 1

Derivações de Jordan

Uma derivação de Jordan definida num anel R é uma aplicação aditiva que satisfaz a propriedade $d(a^2) = d(a)a + ad(a)$ para todo elemento $a \in R$. Toda derivação é obviamente uma derivação de Jordan. A recíproca é falsa, em geral (ver exemplo 1.1.11). É natural, então, perguntarmo-nos sob quais condições uma derivação de Jordan é uma derivação usual. Esta foi a questão considerada por I.N.Herstein. Em 1957, provou em seu trabalho [8] que, quando o anel é primo e livre de 2-torção, o resultado é válido.

Mais tarde, já em 1988, M.Bresăr e J.Vukman [4] publicaram uma versão mais simplificada da prova de Herstein. No primeiro parágrafo deste capítulo apresentaremos esta prova para o resultado mencionado.

No mesmo ano, M.Bresăr [5] mostrou a validade da questão de Herstein para anéis semiprimos livres de 2-torção. Esta prova constitui nosso segundo parágrafo. Naturalmente, esta segunda prova é também uma prova do resultado para anéis primos, uma vez que todo anel primo é semiprimo. Ponderamos apresentar as duas por razões históricas, e além disso pelo fato da primeira ser mais simples que a segunda.

1.1 Derivações de Jordan em Anéis Primos

Definição 1.1.1 *Seja R um anel. Uma aplicação aditiva $d : R \to R$ é dita uma* DERIVAÇÃO DE JORDAN *se $d(a^2) = d(a)a + ad(a)$ para todo $a \in R$.*

Obviamente, toda derivação é uma derivação de Jordan. Neste parágrafo demonstraremos o seguinte

Teorema 1.1.2 *Sejam R um anel primo livre de 2-torção e d: $R \to R$ uma derivação de Jordan em R. Então d é uma derivação.*

Convém chamar a atenção para o fato de que a definição de derivação de Jordan apresentada no trabalho de Herstein [8], não é a dada acima. De fato, Herstein constrói, a partir do anel R, um novo anel, o *ANEL DE JORDAN DE R*, definindo o produto neste como sendo $a \circ b = ab + ba$ para quaisquer a e b em R (ab significa o produto de a por b no anel R). Claramente este novo produto é bem definido e pode-se verificar facilmente que $(R, +, \circ)$ é um anel. Assim sendo, uma aplicação aditiva d, do anel de Jordan nele próprio, é dita por Herstein uma derivação de Jordan, se $d(a \circ b) = d(a) \circ b + a \circ d(b)$.

Para anéis livres de 2-torção as duas definições são equivalentes. De fato,

Proposição 1.1.3 *Sejam R um anel livre de 2-torção e d: $R \to R$ uma aplicação aditiva. Então*

$$d(a \circ b) = d(a) \circ b + a \circ d(b),\ \forall\ a,\ b \in R \Leftrightarrow d(a^2) = d(a)a + ad(a),\ \forall\ a \in R.$$

prova : ($\Rightarrow$) Dado a em R e tomando como derivação de Jordan a definição de Herstein,

$$\begin{aligned} d(a \circ a) &= d(a) \circ a + a \circ d(a) = \\ &= d(a)a + ad(a) + ad(a) + d(a)a = \\ &= 2(d(a)a + ad(a)). \end{aligned}$$

Mas, $a \circ a = aa + aa = 2aa = 2a^2$. Portanto $2d(a^2) = d(a \circ a) = 2(d(a)a + ad(a))$ e, por ser R livre de 2-torção, segue que $d(a^2) = d(a)a + ad(a)$. Logo, d é uma derivação de Jordan, conforme a definição 1.1.1.

($\Leftarrow$) Reciprocamente, tomando como derivação de Jordan a definição 1.1.1, como $(a+b)^2 = a^2 + ab + ba + b^2$, temos que, para quaisquer a e b em R,
$d((a+b)^2) = d(a)a + ad(a) + d(ab+ba) + d(b)b + bd(b)$. Todavia,

$$\begin{aligned} d((a+b)^2) &= d(a+b)(a+b) + (a+b)d(a+b) = \\ &= d(a)a + d(a)b + d(b)a + d(b)b \ + ad(a) + ad(b) + bd(a) + bd(b). \end{aligned}$$

Por conseguinte,

$$\begin{aligned} d(a \circ b) &= d(ab+ba) = \\ &= d(a)b + bd(a) + ad(b) + d(b)a = \\ &= d(a) \circ b + a \circ d(b) \end{aligned}$$

e d é uma derivação de Jordan no sentido de Herstein. $\square$

Para a prova do teorema, necessitamos previamente de alguns resultados. Comecemos pela seguinte

Proposição 1.1.4 *Sejam R um anel e $d : R \to R$ uma derivação de Jordan. Então, para quaisquer a, b e c em R:*
(i) $d(ab+ba) = d(a)b + ad(b) + d(b)a + bd(a)$.
Se o anel R for livre de 2-torção, valem ainda:
(ii) $d(aba) = d(a)ba + ad(b)a + abd(a)$;
(iii) $d(abc+cba) = d(a)bc + ad(b)c + abd(c) + d(c)ba + cd(b)a + cbd(a)$.

prova : (i) Sendo d uma derivação de Jordan, temos que $d(x^2) = d(x)x + xd(x)$ para todo x de R.

Tomando $x = a + b$, com a e b em R, $x^2 = (a+b)(a+b) = a^2 + ab + ba + b^2$. Aplicando d nesta igualdade e calculando como acima, segue que

$$d(ab+ba) = d(a)b + ad(b) + d(b)a + bd(a).$$

Seja agora R livre de 2-torção.

(ii) Sejam a, b em R. Consideremos o elemento $\omega = d(a(ab+ba)+(ab+ba)a)$. Como ω é do tipo $d(ac+ca)$, com $c = ab+ba$, podemos utilizar (i). Temos que

$$\begin{aligned}
\omega &= d(a)(ab+ba) + ad(ab+ba) + (ab+ba)d(a) + d(ab+ba)a = \\
&= d(a)ab + d(a)ba + a(d(a)b + ad(b) + d(b)a + bd(a)) + \\
&\quad + abd(a) + bad(a) + (d(a)b + ad(b) + d(b)a + bd(a))a = \\
&= d(a)ab + 2d(a)ba + ad(a)b + a^2d(b) + 2ad(b)a + \\
&\quad + 2abd(a) + bad(a) + d(b)a^2 + bd(a)a.
\end{aligned}$$

Mas, por outro lado, também temos

$$\begin{aligned}
\omega &= d((a^2b + ba^2) + 2aba) = \\
&= d(a^2b + ba^2) + 2d(aba) = \\
&= d(a^2)b + a^2d(b) + d(b)a^2 + bd(a^2) + 2d(aba) = \\
&= (d(a)a + ad(a))b + a^2d(b) + d(b)a^2 + b(d(a)a + ad(a)) + 2d(aba) = \\
&= d(a)ab + ad(a)b + a^2d(b) + d(b)a^2 + bd(a)a + bad(a) + 2d(aba).
\end{aligned}$$

Assim, $2d(aba) = 2(d(a)ba + ad(b)a + abd(a))$ e, visto que R é livre de 2-torção, segue que $d(aba) = d(a)ba + ad(b)a + abd(a)$.

(iii) Seja $\nu = d((a+c)b(a+c))$ com $a, b, c \in R$. Aplicando (ii), temos:

$$\begin{aligned}
\nu &= d(a+c)b(a+c) + (a+c)d(b)(a+c) + (a+c)bd(a+c) = \\
&= d(a)ba + d(a)bc + d(c)ba + d(c)bc + ad(b)a + ad(b)c + \\
&\quad + cd(b)a + cd(b)c + abd(a) + abd(c) + cbd(a) + cbd(c) = \\
&= d(a)ba + ad(b)a + abd(a) + d(c)bc + cd(b)c + cbd(c) + \\
&\quad + d(a)bc + d(c)ba + ad(b)c + cd(b)a + abd(c) + cbd(a) = \\
&= d(aba) + d(cbc) + d(a)bc + d(c)ba + ad(b)c + cd(b)a + abd(c) + cbd(a).
\end{aligned}$$

Por outro lado,

$$\begin{aligned}
\nu &= d(aba + abc + cba + cbc) = \\
&= d(aba) + d(cbc) + d(abc + cba).
\end{aligned}$$

Comparando as expressões, chegamos à igualdade procurada. □

Observação 1.1.5 Na prova da proposição acima, parte (iii), temos aplicado um mecanismo que será usual no que segue. Para desenvolver a expressão de ν utilizamos a fórmula de (ii), mas substituindo a por $a+c$. Tal processo denomina-se linearização da fórmula de (ii) com respeito a a.

É conveniente introduzir a seguinte notação: sejam $a, b \in R$. Denotaremos por $[a, b]$ a diferença $ab - ba$, isto é,

$$[a, b] \doteq ab - ba.$$

Por outra parte, para qualquer derivação de Jordan d, denotaremos por a^b o elemento $d(ab) - d(a)b - ad(b)$, isto é,

$$a^b \doteq d(ab) - d(a)b - ad(b).$$

Note que $a^b = 0$ para quaisquer $a, b \in R$ equivale a d ser uma derivação usual.
A seguir, destacamos algumas propriedades deste novo símbolo, através do

Lema 1.1.6 *Sejam R um anel e d uma derivação de Jordan em R. Então para quaisquer que sejam $a, b, c \in R$, valem:*
(i) $a^{b+c} = a^b + a^c$;
(ii) $(a + b)^c = a^c + b^c$;
(iii) $a^b = -b^a$.

prova : (i) Para $a, b, c \in R$ temos

$$\begin{aligned} a^{b+c} &= d(a(b+c)) - d(a)(b+c) - ad(b+c) = \\ &= d(ab+ac) - d(a)b - d(a)c - ad(b) - ad(c) = \\ &= d(ab) - d(a)b - ad(b) + d(ac) - d(a)c - ad(c) = a^b + a^c. \end{aligned}$$

(ii) Novamente para a, b, $c \in R$, temos

$$\begin{aligned} (a+b)^c &= d((a+b)c) - d(a+b)c - (a+b)d(c) = \\ &= d(ac) + d(bc) - d(a)c - d(b)c - ad(c) - bd(c) = \\ &= d(ac) - d(a)c - ad(c) + d(bc) - d(b)c - bd(c) = a^c + b^c. \end{aligned}$$

(iii) Para $a, b, c \in R$ temos, pela proposição 1.1.4,

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

ou seja, $a^b = d(ab) - d(a)b - ad(b) = -(d(ba) - d(b)a - bd(a)) = -b^a$. □

Observação 1.1.7 O símbolo $[a,b]$ satisfaz as mesmas propriedades acima, como se pode verificar por cálculos diretos. Isto é, para quaisquer $a, b, c \in R$, valem*:*
(i) $[a, b+c] = [a,b] + [a,c]$*;*
(ii) $[a+b, c] = [a,c] + [b,c]$*;*
(iii) $[a,b] = -[b,a]$.

Lema 1.1.8 *Sejam R um anel livre de 2-torção e $d : R \to R$ uma derivação de Jordan. Então, para quaisquer a, $b \in R$, $a^b[a,b] = 0$.*

prova : Substituindo c por ab na fórmula (iii) da proposição 1.1.4, obtemos:

$$d(ab \cdot ab + ab \cdot ba) = d(a)b \cdot ab + ad(b) \cdot ab + abd(ab) + d(ab)ba + abd(b)a + abbd(a).$$

Entretanto, $ab \cdot ab + ab \cdot ba = (ab)^2 + ab^2a$. Logo, pelo item (ii) da mesma,

$$\begin{aligned} d((ab)^2) + d(ab^2a) &= abd(ab) + d(ab)ab + d(a)b^2a + ad(b^2)a + ab^2d(a) = \\ &= abd(ab) + d(ab)ab + d(a)b^2a + abd(b)a + ad(b)ba + ab^2d(a). \end{aligned}$$

Das duas expressões, $ad(b)ab + d(a)bab + d(ab)ba = d(ab)ab + d(a)b^2a + ad(b)ba$, ou seja, $(d(ab) - d(a)b - ad(b))(ab - ba) = 0$. □

Passemos à

Proposição 1.1.9 *Sejam R um anel livre de 2-torção e $d : R \to R$ uma derivação de Jordan. Para quaisquer $a, b, r \in R$, temos $a^b r[a,b] + [a,b]ra^b = 0$.*

prova : Consideremos o elemento $\mu = abrba + barab$, com a, b, $r \in R$.

Pela proposição 1.1.4 parte (ii),

$$\begin{aligned} d(\mu) &= d(a(brb)a + b(ara)b) = \\ &= d(a(brb)a) + d(b(ara)b) = \\ &= d(a)brba + ad(brb)a + abrbd(a) + d(b)arab + bd(ara)b + barad(b) = \\ &= d(a)brba + ad(b)rba + abd(r)ba + abrd(b)a + abrbd(a) + \\ &\quad + d(b)arab + bd(a)rab + bad(r)ab + bard(a)b + barad(b). \end{aligned}$$

Utilizando agora o item (iii) da mesma,

$$\begin{aligned} d(\mu) &= d((ab)r(ba) + (ba)r(ab)) = \\ &= d(ab)rba + abd(r)ba + abrd(ba) + d(ba)rab + bad(r)ab + bard(ab). \end{aligned}$$

Comparando as expressões obtidas, temos

$$\begin{aligned} (d(ab)rba - d(a)brba - ad(b)rba) &+ (d(ba)rab - d(b)arab - bd(a)rab) + \\ +(abrd(ba) - abrd(b)a - abrbd(a)) &+ (bard(ab) - bard(a)b - barad(b)) = 0. \end{aligned}$$

Em outras palavras, $a^b rba + b^a rab + abrb^a + bara^b = 0$. Como $b^a = -a^b$, segue que $a^b rba - a^b rab - abra^b + bara^b = 0$, ou seja, $a^b r[b,a] + [b,a]ra^b = 0$. Conseqüentemente, $a^b r[a,b] + [a,b]ra^b = 0$. □

Estamos agora em condições de demonstrar o teorema 1.1.2, que é uma conseqüência da proposição 1.1.9 e do lema 0.1.9:

Demonstração do teorema 1.1.2: Sejam a e b elementos fixos de R.

Primeiramente, se $ab \neq ba$, então $a^b = 0$. De fato, como $a^b x[a,b] + [a,b]xa^b = 0$ para todo $x \in R$ e R é primo (em particular semiprimo), segue que $a^b x[a,b] = 0$ para todo $x \in R$, pelo lema 0.1.9. Mas, $[a,b] \neq 0$ e portanto $a^b = 0$.

Agora, sejam a e b pertencentes a $Z(R)$. Da proposição 1.1.4 (i), temos: $2d(ab) = d(ab + ba) = d(a)b + ad(b) + d(b)a + bd(a) = 2(d(a)b + ad(b))$. Como R é livre de 2-torção, segue que $a^b = d(ab) - d(a)b - ad(b) = 0$.

Finalmente, suponhamos que $a \notin Z(R)$ ou $b \notin Z(R)$. Sem perda de generalidade, tomemos $b \notin Z(R)$ e $[a,b] = 0$, sendo que se $[a,b] \neq 0$, já foi provado acima. Linearizando a fórmula do lema 1.1.3 com respeito a a $(a = a + c)$ verifica-se, via cálculos elementares que, para quaisquer a, b, $c \in R$, $a^b[c,b] + c^b[a,b] = 0$. Como $[a,b] = 0$, segue que $a^b[c,b] = 0$ para todo $c \in R$. Portanto, $a^b \in T(b)$ (ver definição 0.1.13). Como $b \notin Z(R)$, pelo lema 0.1.15, $T(b) = 0$ e isto implica $a^b = 0$. □

Derivações de Jordan nem sempre são derivações ordinárias:

Seja $h : R \to R$ uma aplicação aditiva definida num anel R, satisfazendo a propriedade $h(ab) = h(b)a + bh(a)$ para todo $a, b \in R$. Tal aplicação é dita uma *DERIVAÇÃO REVERSA EM R.*

Obviamente h é uma derivação de Jordan.Mas, em geral, h não será uma derivação ordinária (p.e., se R não for comutativo ou se $[a,h(b)] \neq 0$ e $[b,h(a)] \neq 0$).

O que mostraremos é a seguinte

Proposição 1.1.10 *Se Ré um anel primo e h é uma derivação reversa não-nula em R, então R é um anel comutativo sem divisores de zero (próprios) e h é uma derivação ordinária em R.*

prova : Sejam a, b e $c \in R$. Então, $h(a(bc)) = h(bc)a + bch(a) = h(c)ba + ch(b)a + bch(a)$. Igualmente, $h((ab)c) = h(c)ab + ch(ab) = h(c)ab + ch(b)a + cbh(a)$. Entretanto, $a(bc) = (ab)c$. Assim os últimos membros acima precisam ser iguais. Portanto, comparando-os, obtemos $h(c)[a,b] = [b,c]h(a)$ para todo a, b, $c \in R$.

No caso particular em que $c = b$, $h(b)[a,b] = 0$ para todo $a \in R$. Então, $h(b) \in T(b)$. Conseqüentemente, se $h(b) \neq 0$, quer dizer que $T(b) \neq (0)$. Neste caso, pelo lema 0.1.15, temos que $b \in Z(R)$. Isto é, se $b \in R$ é tal que $h(b) \neq 0$, então $b \in Z(R)$.

Suponhamos agora que $b \in R$ e que $h(b) = 0$. Visto que h não é a aplicação identicamente nula, existe algum $a \in R$ tal que $h(a) \neq 0$. Pelo raciocínio acima, $a \in Z(R)$. Como $h(a+b) = h(a) + h(b) = h(a) \neq 0$, novamente $a + b \in Z(R)$. Por conseguinte, $b \in Z(R)$.

Portanto, b pertence a $Z(R)$ em todos os casos. Logo $R = Z(R)$, e assim R é comutativo. Como R é primo, segue que R é um anel comutativo sem divisores de zero (próprios). Sendo assim, $h(ab) = h(b)a + bh(a) = ah(b) + h(a)b$ e h é de fato uma derivação ordinária em R. □

A proposição acima mostra que derivações reversas não-nulas não podem, jamais, ocorrer em anéis primos não comutativos.

Exemplo 1.1.11 Consideremos a aplicação aditiva $\psi : \mathbf{Z}_2[X,Y] \to \mathbf{Z}_2[X,Y]$ no anel de polinômios a duas indeterminadas com coeficientes em $\mathbf{Z}_2$, definida por:

$$\begin{cases} \psi(Y) = \overline{1} \\ \psi(X^iY^j) = \overline{0}, \ \forall \ (i,j) \neq (0,1) \text{ com } i,j \in \mathbf{N}. \end{cases}$$

Então ψ é uma derivação de Jordan, pois dado um polinômio arbitrário $p(XY) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij}X^iY^j$, onde a_{ij} vale $\overline{0}$ ou $\overline{1}$, temos pela definição de ψ que

$$\psi(p^2) = \psi\left(\sum_{i=0}^{n}\sum_{j=0}^{m}\sum_{k=0}^{n}\sum_{s=0}^{m} a_{ij}a_{ks}X^{i+k}Y^{j+s}\right) = a_{00}a_{01} + a_{01}a_{00} =$$

$$= 2a_{00}a_{01} = \overline{0},$$

porque $\mathbf{Z}_2$ tem característica 2.

Como $\mathbf{Z}_2[X,Y]$ é comutativo, $\psi(p)p + p\psi(p) = 2p\psi(p) = \overline{0}$. Logo $\psi(p^2) = \psi(p)p + p\psi(p)$ e ψ é uma derivação de Jordan. Entretanto ψ não é uma derivação usual, uma vez que $\overline{0} = \psi(XY) \neq \psi(X)Y + X\psi(Y) = X$.

1.2 Derivações de Jordan em Anéis Semiprimos

Como mencionamos anteriormente, o propósito deste parágrafo é provar o seguinte resultado:

Teorema 1.2.1 *Sejam R um anel semiprimo livre de 2-torção e $d : R \to R$ uma derivação de Jordan em R. Então d é uma derivação.*

demonstração : Nosso objetivo é mostrar que $a^b = 0$ para quaisquer a e $b \in R$. Da proposições 1.1.9 e do lema 0.1.9, segue que

(1) $\quad a^b x[a,b] = 0$ para quaisquer a, b, $x \in R$.

Linearizando este resultado com respeito a b (substituindo b por $b+c$, com $c \in R$), vem $a^{b+c}x[a,b+c] = 0$.

Utilizando o lema 1.1.6 e a observação 1.1.7,

$$\begin{aligned} 0 &= a^{b+c}x[a,b+c] = a^b x[a,b+c] + a^c x[a,b+c] = \\ &= a^b x[a,b] + a^b x[a,c] + a^c x[a,b] + a^c x[a,c] = a^b x[a,c] + a^c x[a,b], \end{aligned}$$

donde $a^b x[a,c] = -a^c x[a,b]$. Com esta relação e (1), obtemos $(a^b x[a,c])y(a^b x[a,c]) = -a^b(x[a,c]ya^c x)[a,b] = 0$ para todo $y \in R$ e, por ser R semiprimo, segue que

(2) $\quad a^b x[a,c] = 0$ para quaisquer a, b, c, $x \in R$.

Linearizando (2) com respeito a a (substituindo a por $a+d$, com $d \in R$) e calculando como acima, chegamos a $a^b x[d,c] + d^b x[a,c] = 0$, ou seja, $a^b x[d,c] = -d^b x[a,c]$. Conseqüentemente, por (2), $(a^b x[d,c])y(a^b x[d,c]) = -a^b(x[d,c]yd^b x)[a,c] = 0$ para todo $y \in R$. Novamente, sendo R semiprimo, segue que

(3) $\quad a^b x[d,c] = 0$ para quaisquer a, b, c, d, $x \in R$.

Em particular, $[a^b,c]x[a^b,c] = (a^b c - ca^b)x[a^b,c] = a^b(cx)[a^b,c] - ca^b x[a^b,c] = 0$ para todo $x \in R$. Outra vez, sendo R semiprimo, segue que $[a^b,c] = 0$ para todo a, b, $c \in R$, isto é, $a^b c = ca^b$ para todo $c \in R$. Em outras palavras, provamos que a^b pertence ao centro $Z(R)$ de R para quaisquer a, $b \in R$.

Usando (3), obtemos $(a^b[d,c])x(a^b[d,c]) = 0$ para todo $x \in R$. Conseqüentemente,

(4) $\quad a^b[d,c] = 0$ para todo a, b, c, $d \in R$.

Agora, lembrando que $a^b = -b^a$, temos

$$\begin{aligned} 2(a^b)^2 &= a^b a^b + a^b a^b = a^b a^b + a^b(-b^a) = a^b(a^b - b^a) = \\ &= a^b(d(ab) - d(ba) + [d(b),a] + [b,d(a)]). \end{aligned}$$

Por (4), $a^b[d(b), a] = 0$ e $a^b[b, d(a)] = 0$, de modo que a relação acima se reduz a

(5) $\qquad 2(a^b)^2 = a^b d([a, b]).$

Por (4), e visto que $a^b \in Z(R)$, temos

$$\begin{aligned} 0 &= 2a^b[a, b] = \\ &= a^b[a, b] + a^b[a, b] = \\ &= a^b[a, b] + [a, b]a^b. \end{aligned}$$

Conseqüentemente, aplicando d a esta igualdade e usando a proposição 1.1.4 (i), obtemos

$$\begin{aligned} 0 &= d(a^b)[a, b] + a^b d([a, b]) + d([a, b])a^b + [a, b]d(a^b) = \\ &= d(a^b)[a, b] + 2a^b d([a, b]) + [a, b]d(a^b). \end{aligned}$$

Logo, por (5),

(6) $\qquad 4(a^b)^2 + d(a^b)[a, b] + [a, b]d(a^b) = 0$

para a e b elementos arbitrários de R.

Multiplicando (6) por a^b (à direita ou à esquerda, não importa pois $a^b \in Z(R)$) e usando (4), obtemos

$$\begin{aligned} 0 &= 4(a^b)^3 + d(a^b)[a, b]a^b + [a, b]d(a^b)a^b = \\ &= 4(a^b)^3 + d(a^b)a^b[a, b] + a^b[a, b]d(a^b) = \\ &= 4(a^b)^3. \end{aligned}$$

Agora, como R é livre de 2-torção, segue que $(a^b)^3 = 0$. Mas, $a^b \in Z(R)$ e R é semiprimo, logo, pelo lema 0.1.12, podemos concluir que $a^b = 0$.

Isto completa a demonstração do teorema. □

Capítulo 2

Derivações de Hasse-Schmidt-Jordan

Neste capítulo generalizaremos os resultados obtidos no capítulo anterior. Estes resultados não aparecem na literatura, e foram obtidos pelo autor, seguindo sugestões do prof. M.Ferrero.

Uma família $D = (d_n)_{n\in\mathbf{N}}$ de aplicações aditivas $d_n : R \to R$ é dita uma derivação de Hasse-Schmidt (HS-derivação) no anel R, se $d_0 = id_R$ e, para quaisquer elementos a e b em R e qualquer natural n, $d_n(ab) = \sum_{i+j=n} d_i(a)d_j(b)$.

Por outro lado, D é dita uma derivação de Hasse-Schmidt-Jordan em R (HSJ--derivação), se $d_0 = id_R$ e, para qualquer $a \in R$ e n natural, $d_n(a^2) = \sum_{i+j=n} d_i(a)d_j(a)$.

Visto que toda HS-derivação é uma HSJ-derivação e que a recíproca nem sempre é verdadeira (ver exemplo 2.1.4), faz sentido novamente perguntar sob quais condições uma HSJ-derivação é uma HS-derivação.

Seguindo a linha de raciocínio do capítulo 1 conseguimos mostrar, no § 2 que, se o anel R é semiprimo e livre de 2-torção, então $D = (d_n)_{n\in\mathbf{N}}$ é uma HS-derivação se, e somente se, $D = (d_n)_{n\in\mathbf{N}}$ é uma HSJ-derivação. Contudo, a exemplo do capítulo anterior, iniciaremos mostrando o resultado num caso particular em que o anel R é livre de 2-torção e primo.

2.1 HSJ-Derivações em Anéis Primos

Definição 2.1.1 *Uma família* $D = (d_n)_{n\in\mathbf{N}}$ *de aplicações* d_n*:* $R \to R$ *é dita uma* DERIVAÇÃO DE HASSE-SCHMIDT (HS-derivação)*, se satisfaz, para todo* $a, b \in R$ *e para todo* $n \in \mathbf{N}$*:*

1. $d_0 = id_R$;
2. $d_n(a+b) = d_n(a) + d_n(b)$;
3. $d_n(ab) = \sum_{i+j=n} d_i(a)d_j(b)$.

Definição 2.1.2 *Uma família* $D = (d_n)_{n\in\mathbf{N}}$ *de aplicações* d_n*:* $R \to R$ *é dita uma* DERIVAÇÃO DE HASSE-SCHMIDT-JORDAN (HSJ-derivação)*, se satisfaz, para todo* $a, b \in R$ *e para todo* $n \in \mathbf{N}$*:*

1. $d_0 = id_R$;
2. $d_n(a+b) = d_n(a) + d_n(b)$;
3′. $d_n(a^2) = \sum_{i+j=n} d_i(a)d_j(a)$.

Exemplo 2.1.3 Seja $\delta : R \to R$ uma derivação usual sobre uma $\mathbb{Q}$-álgebra R (álgebra sobre os racionais). Definindo $d_i = \frac{\delta^i}{i!}$ para todo $i \in N$, temos que a seqüência $(d_i)_{i\in\mathbf{N}}$ é uma HS-derivação em R.

De fato, para a e b pertencentes a R,

$d_0(ab) = \frac{\delta^0(ab)}{0!} = ab$;

$d_1(ab) = \delta(ab) = a\delta(b) + \delta(a)b = ad_1(b) + d_1(a)b$;

$$d_2(ab) = \frac{\delta^2(ab)}{2} = \frac{\delta}{2}(\delta(ab)) = \frac{\delta}{2}(a\delta(b) + \delta(a)b) = a\frac{\delta^2(b)}{2} + \frac{\delta(a)\delta(b)}{2} + \frac{\delta(a)\delta(b)}{2} + \frac{\delta^2(a)b}{2} =$$

$$= a\frac{\delta^2(b)}{2!} + \delta(a)\delta(b) + \frac{\delta^2(a)b}{2!} = ad_2(b) + d_1(a)d_1(b) + d_2(a)b.$$

Suponhamos, agora, que $d_i = \frac{\delta^i}{i!}$ define uma HS-derivação em R para todo $i < n$. Então, $d_n(ab) = \frac{\delta^n(ab)}{n!} = \frac{1}{n}\delta\left(\frac{\delta^{n-1}(ab)}{(n-1)!}\right) = \frac{1}{n}\delta(d_{n-1}(ab))$.

Aplicando a hipótese de indução a d_{n-1} no lado direito desta igualdade, obtemos

$$\begin{aligned}
d_n(ab) &= \tfrac{1}{n}\delta\left(\textstyle\sum_{j=0}^{n-1} d_j(a)d_{n-1-j}(b)\right) = \tfrac{1}{n}\delta\left(\textstyle\sum_{j=0}^{n-1} \frac{\delta^j(a)}{j!}\frac{\delta^{n-1-j}(b)}{(n-1-j)!}\right) = \\
&= \tfrac{1}{n}\left(\textstyle\sum_{j=0}^{n-1}\left(\frac{\delta^j(a)}{j!}\frac{\delta^{n-j}(b)}{(n-1-j)!} + \frac{\delta^{j+1}(a)}{j!}\frac{\delta^{n-1-j}(b)}{(n-1-j)!}\right)\right) = \\
&= \tfrac{1}{n}\textstyle\sum_{j=0}^{n-1} d_j(a)d_{n-j}(b)(n-j) + \frac{1}{n}\sum_{j=0}^{n-1} d_{j+1}(a)(j+1)d_{n-1-j}(b) = \\
&= \textstyle\sum_{j=0}^{n-1} d_j(a)d_{n-j}(b) - \frac{1}{n}\sum_{j=1}^{n-1} d_j(a)d_{n-j}(b)j + \\
&\quad + \tfrac{1}{n}\textstyle\sum_{j=1}^{n-1} d_{j+1}(a)d_{n-1-j}(b)j + \frac{1}{n}\sum_{j=0}^{n-1} d_{j+1}(a)d_{n-1-j}(b) = \\
&= \textstyle\sum_{j=0}^{n-1} d_j(a)d_{n-j}(b) - \frac{1}{n}\sum_{j=1}^{n-2} d_j(a)d_{n-j}(b)j - \frac{1}{n}d_{n-1}(a)d_1(b)n + \\
&\quad + \tfrac{1}{n}d_{n-1}(a)d_1(b) + \frac{1}{n}\sum_{l=2}^{n} d_l(a)d_{n-l}(b)(l-1) + \frac{1}{n}\sum_{l=1}^{n} d_l(a)d_{n-l}(b),
\end{aligned}$$

por uma mudança de variável.

Desenvolvendo um pouco mais esta última igualdade e simplificando os termos comuns, temos

$$\begin{aligned}
d_n(ab) &= \textstyle\sum_{j=0}^{n-1} d_j(a)d_{n-j}(b) - \frac{1}{n}d_1(a)d_{n-1}(b) - \frac{1}{n}\sum_{j=2}^{n-2} d_j(a)d_{n-j}(b)j - \\
&\quad - d_{n-1}(a)d_1(b) + \tfrac{1}{n}d_{n-1}(a)d_1(b) + \frac{1}{n}\sum_{l=2}^{n-2} d_l(a)d_{n-l}(b)l + \\
&\quad + \tfrac{1}{n}d_{n-1}(a)d_1(b)n - \frac{1}{n}d_{n-1}(a)d_1(b) + d_n(a)b - \frac{1}{n}\sum_{l=2}^{n} d_l(a)d_{n-l}(b) + \\
&\quad + \tfrac{1}{n}d_1(a)d_{n-1}(b) + \frac{1}{n}\sum_{l=2}^{n} d_l(a)d_{n-l}(b) = \\
&= \textstyle\sum_{j=0}^{n} d_j(a)d_{n-j}(b).
\end{aligned}$$

Portanto, a família $(d_i)_{i\in\mathbf{N}}$, com $d_i = \frac{\delta^i}{i!}$, define uma HS-derivação em R. Por outra parte, se $D = (d_i)_{i\in\mathbf{N}}$ é uma HS-derivação em R, então d_1 é uma derivação.

Exemplo 2.1.4 Consideremos a família $\Psi = (\psi_i)_{i\in\mathbf{N}}$,

$$\psi_i : \mathbf{Z}_2[X,Y] \to \mathbf{Z}_2[X,Y] \text{ para todo } i \in \mathbf{N},$$

no anel de polinômios a duas indeterminadas com coeficientes em $\mathbf{Z}_2$.

Suponhamos ψ_i aditiva para todo $i \in \mathbf{N}$ e satisfazendo as seguintes condições:

$$* \quad \psi_0 = id_R$$

$$* \quad \psi_1 = \begin{cases} \psi_1(Y) = \overline{1} \\ \psi_1(X^iY^j) = \overline{0},\ \forall\ (\mathrm{i},\mathrm{j}) \neq (0,1),\ \mathrm{com\ i,\ j} \in \mathbf{N} \end{cases}$$
(ver exemplo 1.1.11)

$$* \quad \psi_2 = \begin{cases} \psi_2(Y) = \overline{0} \\ \psi_2(Y^i) = \psi_1(Y^{i-1}) + \psi_2(Y^{i-1})Y = Y^{i-2}, \forall\ \mathrm{i} \geq 2 \\ \psi_2(X^iY^j) = \overline{0},\ \forall\ \mathrm{i,\ j} \in \mathbf{N},\ \mathrm{i} \neq 0 \end{cases}$$

$$* \quad \psi_3 = \begin{cases} \psi_3(Y) = \overline{0} \\ \psi_3(Y^2) = \overline{0} \\ \psi_3(Y^i) = \psi_2(Y^{i-1}) + \psi_3(Y^{i-1})Y = \begin{cases} \overline{0}, se\ i = par \\ Y^{i-3}, se\ i = \acute{i}mpar \geq 3 \end{cases} \\ \psi_3(X^iY^j) = \overline{0},\ \forall\, \mathrm{i,\ j} \in \mathbf{N},\ \mathrm{i} \neq 0 \end{cases}$$

$$\vdots$$

$$* \quad \psi_n = \begin{cases} \psi_n(Y^I) = \overline{0},\ \forall\, \mathrm{i} \leq \mathrm{n}-1,\ \mathrm{n} \geq 2 \\ \psi_n(Y^i) = \psi_{n-1}(Y^{i-1}) + \psi_n(Y^{i-1})Y, \forall\ \mathrm{i} \geq \mathrm{n} \geq 2 \\ \psi_n(X^iY^j) = \overline{0}, \forall\ \mathrm{i,\ j} \in \mathbf{N},\ \mathrm{i} \neq 0 \end{cases}$$

A prova de que esta seqüência constitui uma HSJ-derivação é fácil, contudo extremamente enfadonha, fugindo assim dos nossos propósitos. Entretanto Ψ não é uma HS-derivação, uma vez que

$$\overline{0} = \psi_2(XY^2) \neq X\psi_2(Y^2) + \psi_1(X)\psi_1(Y^2) + \psi_2(X)Y^2 = X.$$

Os seguintes resultados são generalizações naturais dos resultados obtidos na proposição 1.1.4, na observação 1.1.7, no lema 1.1.6 e na proposição 1.1.9.

Proposição 2.1.5 *Sejam R um anel e $D = (d_n)_{n\in\mathbf{N}}$ uma HSJ-derivação. Então, para quaisquer $a, b, c \in R, n \in \mathbf{N}$:*
(i) $d_n(ab + ba) = \sum_{i+j=n} (d_i(a)d_j(b) + d_i(b)d_j(a))$.
Se o anel R for livre de 2-torção, valem ainda:
(ii) $d_n(aba) = \sum_{\mathrm{i+j+k=n}} d_i(a)d_j(b)d_k(a)$;
(iii) $d_n(abc + cba) = \sum_{\mathrm{i+j+k=n}}(d_i(a)d_j(b)d_k(c) + d_i(c)d_j(b)d_k(a))$.

prova : *(i)* Sejam $a, b \in R$, $n \in \mathbf{N}$. Dado que $d_n(a^2) = \sum_{i+j=n} d_i(a)d_j(b)$, ao linearizarmos esta relação substituindo a por $a + b$, obtemos

$$\begin{aligned} d_n((a+b)^2) &= \textstyle\sum_{t+u=n} d_t(a+b)d_u(a+b) = \sum_{t+u=n}(d_t(a)+d_t(b))(d_u(a)+d_u(b)) = \\ &= \textstyle\sum_{t+u=n} d_t(a)d_u(a) + \sum_{t+u=n} d_t(a)d_u(b) + \\ &\quad + \textstyle\sum_{t+u=n} d_t(b)d_u(a) + \sum_{t+u=n} d_t(b)d_u(b). \end{aligned}$$

Porém,

$$\begin{aligned} d_n((a+b)^2) &= d_n(a^2 + ab + ba + b^2) = d_n(a^2) + d_n(ab+ba) + d_n(b^2) = \\ &= d_n(ab+ba) + \textstyle\sum_{i+j=n} d_i(a)d_j(a) + \sum_{r+s=n} d_r(b)d_s(b). \end{aligned}$$

Comparando as duas expressões e reordenando os índices, chegamos ao resultado procurado.

(ii) Sejam $a, b \in R$, $n \in \mathbf{N}$ e seja $\omega = d_n(a(ab + ba) + (ab + ba)a)$. Usando *(i)* com $ab + ba$ no lugar de b, vemos que

$$\begin{aligned} \omega &= \sum_{i+j=n} d_i(a)d_j(ab+ba) + \sum_{i+j=n} d_i(ab+ba)d_j(a) = \\ &= \sum_{i+j=n} d_i(a)\left(\sum_{r+s=j} d_r(a)d_s(b) + \sum_{r+s=j} d_r(b)d_s(a)\right) + \\ &\quad + \sum_{i+j=n}\left(\sum_{k+l=i} d_k(a)d_l(b) + \sum_{k+l=i} d_k(b)d_l(a)\right) d_j(a) = \end{aligned}$$

$$= \sum_{i+j=n} d_i(a) \sum_{r+s=j} d_r(a)d_s(b) + \sum_{i+j=n} d_i(a) \sum_{r+s=j} d_r(b)d_s(a) +$$

$$+ \sum_{i+j=n} \sum_{k+l=i} d_k(a)d_l(b)d_j(a) + \sum_{i+j=n} \sum_{k+l=i} d_k(b)d_l(a)d_j(a) =$$

$$= \sum_{\mathrm{i+j=n}} \sum_{\mathrm{r+s=j}} d_i(a)d_r(a)d_s(b) + 2 \sum_{\mathrm{i+j+k=n}} d_i(a)d_j(b)d_k(a) +$$

$$+ \sum_{i+j=n} \sum_{k+l=i} d_k(b)d_l(a)d_j(a).$$

Note que na última igualdade utilizamos

$$\sum_{\mathrm{i+j=n}} d_i(a) \sum_{\mathrm{r+s=j}} d_r(b)d_s(a) + \sum_{\mathrm{i+j=n}} \sum_{\mathrm{k+l=i}} d_k(a)d_l(b)d_j(a) = 2 \sum_{\mathrm{i+j+k=n}} d_i(a)d_j(b)d_k(a),$$

o que é de fácil verificação, pois uma vez fixado n e dado i, o índice j do lado esquerdo da igualdade fica determinado por $j = n - i$. Portanto, no somatório da primeira parcela, $r + s = j = n - i$. Donde, $r + s + i = n$. Do mesmo modo, no somatório da segunda parcela, $j = n - i = n - (k + l)$. Donde, $i + k + l = n$. A igualdade segue agora facilmente.

Por outro lado, $\omega = d_n((a^2b + ba^2) + 2aba) = d_n(a^2b + ba^2) + 2d_n(aba)$.

Agora, por (i) e utilizando o fato que D é uma HSJ-derivação:

$$\omega = 2d_n(aba) + \sum_{i+j=n} \sum_{r+s=i} d_r(a)d_s(a)d_j(b) + \sum_{i+j=n} d_i(b) \sum_{k+l=j} d_k(a)d_l(a).$$

Portanto, comparando as duas expressões e reordenando os índices, encontramos $2d_n(aba) = 2\sum_{\mathrm{i+j+k=n}} d_i(a)d_j(b)d_k(a)$. Como R é livre de 2-torção, segue que $d_n(aba) = \sum_{\mathrm{i+j+k=n}} d_i(a)d_j(b)d_k(a)$.

(iii) Sejam a, b, $c \in R$, $n \in \mathbf{N}$. Começamos linearizando o resultado anterior, substituindo a por $a + c$, ou seja, considerando $\gamma = d_n((a + c)b(a + c))$.

Temos $\gamma = d_n(aba) + d_n(cbc) + d_n(abc + cba)$. Contudo, pela parte (ii),

$$\gamma = \sum_{\text{i+j+k=n}} d_i(a+c)d_j(b)d_k(a+c) =$$

$$= \sum_{i+j+k=n} d_i(a)d_j(b)d_k(a) + \sum_{i+j+k=n} d_i(a)d_j(b)d_k(c) +$$

$$+ \sum_{i+j+k=n} d_i(c)d_j(b)d_k(a) + \sum_{i+j+k=n} d_i(c)d_j(b)d_k(c) =$$

$$= d_n(aba) + \sum_{i+j+k=n} d_i(a)d_j(b)d_k(c) + \sum_{i+j+k=n} d_i(c)d_j(b)d_k(a) + d_n(cbc).$$

Logo, $d_n(abc + cba) = \sum_{i+j+k=n}(d_i(a)d_j(b)d_k(c) + d_i(c)d_j(b)d_k(a))$. □

Para qualquer HSJ-derivação e quaisquer a, $b \in R$, $n \in \mathbf{N}$, denotaremos por $\varphi_n(a,b)$ o elemento

$$\varphi_n(a,b) \doteq d_n(ab) - \textstyle\sum_{i+j=n} d_i(a)d_j(b).$$

Note que dizer que $\varphi_n(a,b) = 0$ para todo n natural e para todo a, $b \in R$ equivale a dizer que D é uma HS-derivação.

Lema 2.1.6 *Sejam R um anel e $D = (d_n)_{n\in\mathbf{N}}$ uma HSJ-derivação em R. Então, para quaisquer a, b, $c \in R$ e $n \in \mathbf{N}$, temos:*
(i) $\varphi_n(b,a) = -\varphi_n(a,b)$;
(ii) $\varphi_n(a,b+c) = \varphi_n(a,b) + \varphi_n(a,c)$;
(iii) $\varphi_n(a+b,c) = \varphi_n(a,c) + \varphi_n(b,c)$.

prova : (i) Sejam a, $b \in R$, $n \in \mathbf{N}$. Da proposição 2.1.5 (i), vemos que $d_n(ab) + d_n(ba) = d_n(ab+ba) = \sum_{i+j=n} d_i(a)d_j(b) + \sum_{i+j=n} d_i(b)d_j(a)$, donde $d_n(ab) - \sum_{i+j=n} d_i(a)d_j(b) = -\left(d_n(ba) - \sum_{i+j=n} d_i(b)d_j(a)\right)$, ou seja, $\varphi_n(a,b) = -\varphi_n(b,a)$.

(ii) e (iii) Sejam agora a, b, $c \in R$, $n \in \mathbf{N}$. Então,

$$\varphi_n(a, b+c) = d_n(a(b+c)) - \sum_{i+j=n} d_i(a)d_j(b+c) =$$

$$= d_n(ab) - \sum_{i+j=n} d_i(a)d_j(b) + d_n(ac) - \sum_{i+j=n} d_i(a)d_j(c) =$$

$$= \varphi_n(a, b) + \varphi_n(a, c).$$

Analogamente mostra-se que $\varphi_n(a+b, c) = \varphi_n(a, c) + \varphi_n(b, c)$. □

Proposição 2.1.7 *Sejam R um anel livre de 2-torção, n um número natural e $D = (d_i)_{i\in\mathbf{N}}$ uma HSJ-derivação. Se $\varphi_m(a, b) = 0$ para todo $m < n$ e para quaisquer a, $b \in R$, então $\varphi_n(a, b)r[a, b] + [a, b]r\varphi_n(a, b) = 0$ para todo r, a, $b \in R$.*

prova : Sejam a, $b \in R$. Por hipótese, $\varphi_m(a, b) = 0$ para todo $m < n$. Portanto, $\varphi_m(a, b)r[a, b] + [a, b]r\varphi_m(a, b) = 0$ para todo $r \in R$ e para todo $m < n$.

Seja $\vartheta = abrba + barab$, com $a, b, r \in R$. Por um lado, pela parte (ii) da proposição 2.1.5,

$$d_n(\vartheta) = d_n(a(brb)a+b(ara)b) =$$

$$= \sum_{i+j+k=n} (d_i(a)d_j(brb)d_k(a) + d_i(b)d_j(ara)d_k(b)) =$$

$$= \sum_{i+j+k=n} \left(d_i(a) \sum_{l+t+u=j} d_l(b)d_t(r)d_u(b)d_k(a) + d_i(b) \sum_{l+t+u=j} d_l(a)d_t(r)d_u(a)d_k(b) \right) =$$

$$= \sum_{\mathrm{i+l+t+u+k=n}} (d_i(a)d_l(b)d_t(r)d_u(b)d_k(a) + d_i(b)d_l(a)d_t(r)d_u(a)d_k(b)) .$$

No entanto, pela proposição 2.1.5 parte (iii),

$$d_n(\vartheta) = d_n((ab)r(ba)+(ba)r(ab)) =$$

$$= \sum_{\alpha+\beta+\gamma=n} (d_\alpha(ab)d_\beta(r)d_\gamma(ba) + d_\alpha(ba)d_\beta(r)d_\gamma(ab)) .$$

Igualando-se as duas expressões, obtemos

$$(1) \qquad \sum_{\alpha+\beta+\gamma=n} d_\alpha(ab)d_\beta(r)d_\gamma(ba) - \sum_{i+l+t+u+k=n} d_i(a)d_l(b)d_t(r)d_u(b)d_k(a) +$$

$$+ \sum_{\alpha+\beta+\gamma=\mathrm{n}} d_\alpha(ba)d_\beta(r)d_\gamma(ab) - \sum_{\mathrm{i+l+t+u+k=n}} d_i(b)d_l(a)d_t(r)d_u(a)d_k(b) = 0.$$

Calculemos inicialmente a primeira parcela:

$$\sum_{\alpha+\beta+\gamma=\mathrm{n}} d_\alpha(ab)d_\beta(r)d_\gamma(ba) = \sum_{\alpha+\gamma=n} d_\alpha(ab)rd_\gamma(ba) + \sum_{\alpha+\gamma=n-1} d_\alpha(ab)d_1(r)d_\gamma(ba) +$$

$$+ \sum_{\alpha+\gamma=n-2} d_\alpha(ab)d_2(r)d_\gamma(ba) + \ldots + \sum_{\alpha+\gamma=2} d_\alpha(ab)d_{n-2}(r)d_\gamma(ba) +$$

$$+ \sum_{\alpha+\gamma=1} d_\alpha(ab)d_{n-1}(r)d_\gamma(ba) + abd_n(r)ba =$$

$$= abrd_n(ba) + d_n(ab)rba + \sum_{\substack{\alpha+\gamma=n \\ \alpha,\gamma\leq n-1}} d_\alpha(ab)rd_\gamma(ba) + \sum_{\alpha+\gamma=n-1} d_\alpha(ab)d_1(r)d_\gamma(ba) +$$

$$+ \sum_{\alpha+\gamma=n-2} d_\alpha(ab)d_2(r)d_\gamma(ba) + \ldots + \sum_{\alpha+\gamma=2} d_\alpha(ab)d_{n-2}(r)d_\gamma(ba) +$$

$$+ abd_{n-1}(r)d_1(ba) + d_1(ab)d_{n-1}(r)ba + abd_n(r)ba.$$

Agora, pela hipótese inicial ($\varphi_m(a,b) = 0, \forall m < n$) aplicada a cada somatório, a soma acima é igual a

$$abrd_n(ba) + d_n(ab)rba + \sum_{\substack{\alpha+\gamma=n \\ \alpha,\gamma\leq n-1}} \sum_{i+j=\alpha} d_i(a)d_j(b)r \sum_{u+k=\gamma} d_u(b)d_k(a) +$$

$$+ \sum_{\alpha+\gamma=n-1} \sum_{i+j=\alpha} d_i(a)d_j(b)d_1(r) \sum_{u+k=\gamma} d_u(b)d_k(a) + \ldots$$

$$\ldots + \sum_{\alpha+\gamma=2} \sum_{i+j=\alpha} d_i(a)d_j(b)d_{n-2}(r) \sum_{u+k=\gamma} d_u(b)d_k(a) +$$

$$+ abd_{n-1}(r)d_1(b)a + abd_{n-1}(r)bd_1(a) + d_1(a)bd_{n-1}(r)ba +$$

$$+ ad_1(b)d_{n-1}(r)ba + abd_n(r)ba.$$

Observe também que podemos escrever a segunda parcela em (1) como

$$\sum_{i+l+t+u+k=n} d_i(a)d_l(b)d_t(r)d_u(b)d_k(a) = \sum_{i+l+u+k=n} d_i(a)d_l(b)rd_u(b)d_k(a) +$$

$$+ \sum_{i+l+u+k=n-1} d_i(a)d_l(b)d_1(r)d_u(b)d_k(a) + \ldots$$

$$\ldots + \sum_{i+l+u+k=1} d_i(a)d_l(b)d_{n-1}(r)d_u(b)d_k(a) + abd_n(r)ba =$$

$$= abr \sum_{u+k=n} d_u(b)d_k(a) + \sum_{i+l=n} d_i(a)d_l(b)rba +$$

$$+ \sum_{\substack{i+l+u+k=n \\ 1\leq i+l\leq n-1 \\ 1\leq u+k\leq n-1}} d_i(a)d_l(b)rd_u(b)d_k(a) +$$

$$+ \sum_{i+l+u+k=n-1} d_i(a)d_l(b)d_1(r)d_u(b)d_k(a) + \ldots$$

$$\ldots + \sum_{i+l+u+k=2} d_i(a)d_l(b)d_{n-2}(r)d_u(b)d_k(a) +$$

$$+ d_1(a)bd_{n-1}(r)ba + ad_1(b)d_{n-1}(r)ba + abd_{n-1}(r)d_1(b)a +$$

$$+ abd_{n-1}(r)bd_1(a) + abd_n(r)ba.$$

Calculando a diferença entre as duas primeiras parcelas de (1) através das respectivas expressões obtidas, notamos que as únicas parcelas que não se cancelam são $\varphi_n(a,b)rba + abr\varphi_n(b,a)$, isto é,

$$\sum_{\alpha+\beta+\gamma=n} d_\alpha(ab)d_\beta(r)d_\gamma(ba) - \sum_{i+l+t+u+k=n} d_i(a)d_l(b)d_t(r)d_u(b)d_k(a) =$$

$$= \varphi_n(a,b)rba + abr\varphi_n(b,a).$$

Com raciocínio inteiramente análogo, verifica-se que

$$\sum_{\alpha+\beta+\gamma=n} d_\alpha(ba)d_\beta(r)d_\gamma(ab) - \sum_{i+l+t+u+k=n} d_i(b)d_l(a)d_t(r)d_u(b)d_k(a) =$$

$$= \varphi_n(b,a)rab + bar\varphi_n(a,b).$$

Portanto, segue de (1) que $\varphi_n(a,b)rba + abr\varphi_n(b,a) + \varphi_n(b,a)rab + bar\varphi_n(a,b) = 0$. Utilizando o lema 2.1.6 (i), temos

$$\begin{aligned} 0 &= \varphi_n(a,b)rba - abr\varphi_n(a,b) - \varphi_n(a,b)rab + bar\varphi_n(a,b) = \\ &= \varphi_n(a,b)r(ba-ab) + (ba-ab)r\varphi_n(a,b) = \\ &= \varphi_n(a,b)r[b,a] + [b,a]r\varphi_n(a,b) = \\ &= -(\varphi_n(a,b)r[a,b] + [a,b]r\varphi_n(a,b)), \text{ que é o resultado procurado. } \square \end{aligned}$$

Lema 2.1.8 *Seja $D = (d_n)_{n\in\mathbf{N}}$ uma HS-derivação em um anel R. Então*

$$d_i(Z(R)) \subseteq Z(R) \text{ para todo } i \in \mathbf{N}.$$

prova : Procederemos por indução sobre n. Seja $a \in Z(R)$. Então $ab = ba$ para todo $b \in R$ e portanto $d_n(ab) = d_n(ba)$ para todo $n \in \mathbf{N}$.

Para $n = 0$ o resultado é óbvio.

Agora, $d_1(ab) = d_1(ba)$ e, assim, $ad_1(b) + d_1(a)b = bd_1(a) + d_1(b)a$. Como $ad_1(b) = d_1(b)a$, visto que $a \in Z(R)$, segue que $d_1(a)b = bd_1(a)$ para todo $b \in R$ e para todo $a \in Z(R)$. Logo $d_1(Z(R)) \subseteq Z(R)$.

Suponhamos, por hipótese de indução, que $d_m(Z(R)) \subseteq Z(R)$ para todo $m < n$. Temos $d_n(ab) = d_n(ba)$ para todo $b \in R$, isto é,

$$\sum_{i+j=n} d_i(a)d_j(b) = \sum_{i+j=n} d_i(b)d_j(a).$$

Portanto,

$$\begin{aligned} &ad_n(b) + d_1(a)d_{n-1}(b) + d_2(a)d_{n-2}(b) + d_3(a)d_{n-3}(b) + \ldots \\ &\quad \ldots + d_{n-2}(a)d_2(b) + d_{n-1}(a)d_1(b) + d_n(a)b = \\ &= bd_n(a) + d_1(b)d_{n-1}(a) + d_2(b)d_{n-2}(a) + \ldots \\ &\quad \ldots + d_{n-3}(b)d_3(a) + d_{n-2}(b)d_2(a) + d_{n-1}(b)d_1(a) + d_n(b)a. \end{aligned}$$

Logo $d_n(a)b = bd_n(a)$ pois, pela hipótese de indução, $d_i(a)d_{n-i}(b) = d_{n-i}(b)d_i(a)$ para todo $0 \leq i \leq n-1$. Assim, $d_n(Z(R)) \subseteq Z(R)$ para todo $n \in \mathbf{N}$. □

Lema 2.1.9 *Sejam R um anel semiprimo livre de 2-torção e $D = (d_n)_{n\in\mathbf{N}}$ uma HSJ-derivação em R. Se $\varphi_m(a,b) = 0$ para todo $m < n$ e para todo $a, b \in R$, então:*
(i) $\varphi_n(a,b) \in Z(R)$;
(ii) $\varphi_n(a,b)[d,c] = 0$ *para quaisquer* $a, b, c, d \in R$, $n \in \mathbf{N}$.

prova : *(i)* Da hipótese, pela proposição 2.1.7 e pelo lema 0.1.9, segue que

$$\varphi_n(a,b)x[a,b] = 0 \text{ para todo } a,\ b,\ x \in R. \tag{2}$$

Linearizando esta expressão com respeito a b e utilizando o lema 2.1.6 *(ii)*, temos

$$\begin{aligned} 0 &= \varphi_n(a,b+c)x[a,b+c] = \\ &= \varphi_n(a,b)x[a,b] + \varphi_n(a,b)x[a,c] + \varphi_n(a,c)x[a,b] + \varphi_n(a,c)x[a,c] = \\ &= \varphi_n(a,b)x[a,c] + \varphi_n(a,c)x[a,b]. \end{aligned}$$

Portanto, $\varphi_n(a,b)x[a,c] = -\varphi_n(a,c)x[a,b]$.

Sendo assim, por (2),

$$\begin{aligned}(\varphi_n(a,b)x[a,c])y(\varphi_n(a,b)x[a,c]) &= (\varphi_n(a,b)x[a,c])y(-\varphi_n(a,c)x[a,b]) = \\ &= -\varphi_n(a,b)(x[a,c]y\varphi_n(a,c)x)[a,b] = \\ &= 0 \text{ para todo } a,b,c,x,y \in R.\end{aligned}$$

Visto que R é semiprimo, segue que

(3) $\varphi_n(a,b)x[a,c] = 0$ para todo $a,b,c,x \in R$.

Linearizando (3) com respeito a a,

$$\begin{aligned}0 &= \varphi_n(a+d,b)x[a+d,c] = \\ &= \varphi_n(a,b)x[a,c] + \varphi_n(a,b)x[d,c] + \varphi_n(d,b)x[a,c] + \varphi_n(d,b)x[d,c] = \\ &= \varphi_n(a,b)x[d,c] + \varphi_n(d,b)x[a,c].\end{aligned}$$

Portanto, $\varphi_n(a,b)x[d,c] = -\varphi_n(d,b)x[a,c]$.

Agora,

$$\begin{aligned}(\varphi_n(a,b)x[d,c])y(\varphi_n(a,b)x[d,c]) &= (\varphi_n(a,b)x[d,c])y(-\varphi_n(d,b)x[a,c]) = \\ &= -\varphi_n(a,b)(x[d,c]y\varphi_n(d,b)x)[a,c] = \\ &= 0.\end{aligned}$$

Logo,

(4) $\varphi_n(a,b)x[d,c] = 0$ para todo $a,b,c,x \in R$.

Em particular,

$$\begin{aligned}[\varphi_n(a,b),c]x[\varphi_n(a,b),c] &= (\varphi_n(a,b)c - c\varphi_n(a,b))x[\varphi_n(a,b),c] = \\ &= \varphi_n(a,b)(cx)[\varphi_n(a,b),c] - c\varphi_n(a,b)x[\varphi_n(a,b),c] = \\ &= 0 \text{ para todo } a,b,c,x \in R.\end{aligned}$$

Portanto $[\varphi_n(a,b),c] = 0$ para todo a, b, $c \in R$, isto é, $\varphi_n(a,b)c - c\varphi_n(a,b) = 0$. Logo $\varphi_n(a,b) \in Z(R)$ para todo $a,b \in R, n \in \mathbf{N}$, concluindo a prova de (i).

(ii) Como $\varphi_n(a,b)x[d,c] = 0$ para todo $x \in R$ (por (4)) e $\varphi_n(a,b) \in Z(R)$ (por (i)), segue que $\varphi_n(a,b)[d,c]x\varphi_n(a,b)[d,c] = 0$. Por R ser semiprimo, podemos concluir que $\varphi_n(a,b)[d,c] = 0$ para todo a, b, c, $d \in R$, $n \in \mathbf{N}$. □

Teorema 2.1.10 *Sejam R um anel primo livre de 2-torção e $D = (d_n)_{n\in\mathbf{N}}$ uma HSJ-derivação em R. Então D é uma HS-derivação.*

demonstração : Sejam a, $b \in R$, $n \in \mathbf{N}$. Vamos mostrar que $\varphi_n(a,b) = 0$ para todo $n \in \mathbf{N}$. Procederemos por indução sobre n. Já sabemos que $\varphi_0(a,b) = 0$. Suponhamos, por hipótese de indução, que $\varphi_m(a,b) = 0$ para todo $m < n$. Então $d_i(ab) = \sum_{l+k=i} d_l(a)d_k(b)$ e podemos usar o lema 2.1.8 para todo $i \leq m$,.

Caso 1 : Se a e b pertencem a $Z(R)$, então $ab = ba$ e $d_n(ab) = d_n(ba)$. Pelos lemas 2.1.5 (i) e 2.1.8, $2d_n(ab) = 2\sum_{i+j=n} d_i(a)d_j(b)$. Logo $d_n(ab) = \sum_{i+j=n} d_i(a)d_j(b)$ e D é uma HS-derivação.

Caso 2 : Se $a \notin Z(R)$ ou $b \notin Z(R)$, sem perda de generalidade, podemos supor que $b \notin Z(R)$. Lembrando que R é, em particular, um anel semiprimo, utilizemos o lema 2.1.9 (ii). Segue que $\varphi_n(a,b)[d,c] = 0$ para todo a, b, $c \in R$. Em particular, $\varphi_n(a,b)[b,c] = 0$ para todo $c \in R$. Conseqüentemente, $\varphi_n(a,b) \in T(b)$ (ver definição 0.1.13). Como R é primo e $b \notin Z(R)$, pelo lema 0.1.15, temos $\varphi_n(a,b) = 0$. □

2.2 HSJ-Derivações em Anéis Semiprimos

Nosso objetivo aqui é provar que num anel semiprimo R livre de 2-torção toda HSJ-derivação é uma HS-derivação. No parágrafo anterior já deduzimos todos os preliminares necessários para demonstrar o seguinte

Teorema 2.2.1 *Sejam R um anel semiprimo livre de 2-torção e $D = (d_n)_{n\in\mathbf{N}}$ uma HSJ-derivação em R. Então D é uma HS-derivação em R.*

demonstração : Queremos mostrar que $\varphi_n(a,b) = 0$ para todo a, $b \in R$, $n \in \mathbf{N}$. Suponhamos, por hipótese de indução, que $\varphi_m(a,b) = 0$ para todo $m < n$. Sabemos que $\varphi_n(a,b) = -\varphi_n(b,a)$, portanto

$$\begin{aligned}
2(\varphi_n(a,b))^2 &= \varphi_n(a,b)\varphi_n(a,b) + \varphi_n(a,b)\varphi_n(a,b) = \\
&= \varphi_n(a,b)\varphi_n(a,b) + \varphi_n(a,b)(-\varphi_n(b,a)) = \\
&= \varphi_n(a,b)(\varphi_n(a,b) - \varphi_n(b,a)) = \\
&= \varphi_n(a,b)\left(d_n(ab) - d_n(ba) + \textstyle\sum_{i+j=n}\left(d_i(a)d_j(b) - d_i(b)d_j(a)\right)\right) = \\
&= \varphi_n(a,b)\left(d_n(ab) - d_n(ba) + \textstyle\sum_{i+j=n}\left[d_i(a), d_j(b)\right]\right).
\end{aligned}$$

Porém, pelo lema 2.1.9 (ii), $\varphi_n(a,b)\sum_{i+j=n}[d_i(a),d_j(b)]=0$. Assim, a expressão se reduz a

$$2(\varphi_n(a,b))^2=\varphi_n(a,b)d_n([a,b]). \tag{5}$$

Visto que $\varphi_n(a,b)\in Z(R)$ (lema 2.1.9 (i)), temos
$0=2\varphi_n(a,b)[a,b]=\varphi_n(a,b)[a,b]+\varphi_n(a,b)[a,b]=\varphi_n(a,b)[a,b]+[a,b]\varphi_n(a,b)$ (que é uma expressão do tipo $cd+dc$). Apliquemos d_n a ela:

$$\begin{aligned}0 &= d_n\left(\varphi_n(a,b)[a,b]+[a,b]\varphi_n(a,b)\right)=\\
&=\sum_{i+j=n}\left(d_i(\varphi_n(a,b))d_j([a,b])+d_i([a,b])d_j(\varphi_n(a,b))\right)=\\
&=\varphi_n(a,b)d_n([a,b])+d_n([a,b])\varphi_n(a,b)+\\
&\quad+\sum_{\substack{i+j=n\\1\le i\le n-1}}\left(d_i(\varphi_n(a,b))d_j([a,b])+d_j([a,b])d_i(\varphi_n(a,b))\right)+\\
&\quad+\ d_n(\varphi_n(a,b))[a,b]\ +\ [a,b]d_n(\varphi_n(a,b)).\end{aligned}$$

Como $\varphi_n(a,b)\in Z(R)$, segue que

$$\begin{aligned}&2\varphi_n(a,b)d_n([a,b])+\sum_{\substack{i+j=n\\1\le i\le n-1}}\left(d_i(\varphi_n(a,b))d_j([a,b])+d_j([a,b])d_i(\varphi_n(a,b))\right)+\\
&\quad+\ d_n(\varphi_n(a,b))[a,b]+[a,b]d_n(\varphi_n(a,b))=0.\end{aligned}$$

Utilizando (5), obtemos

$$\begin{aligned}&4(\varphi_n(a,b))^2+\sum_{\substack{i+j=n\\1\le i\le n-1}}\left(d_i(\varphi_n(a,b))d_j([a,b])+d_j([a,b])d_i(\varphi_n(a,b))\right)+\\
&\quad+d_n(\varphi_n(a,b))[a,b]+[a,b]d_n(\varphi_n(a,b))=0.\end{aligned} \tag{6}$$

Por hipótese de indução, temos que $\varphi_m(a,b)=0$ para todo $m<n$. Passemos a mostrar que, nestas condições, $\varphi_n(a,b)d_k([a,b])=0$ para todo $k\le m$.

De fato, para $k=0$ o resultado é válido pelo lema 2.1.9 (ii).

Suponhamos $\varphi_n(a,b)d_l([a,b]) = 0$ para todo $l < k$. Então,

$$\varphi_n(a,b)d_k([a,b]) = \varphi_n(a,b)d_k(ab-ba) = \varphi_n(a,b)d_k(ab) - \varphi_n(a,b)d_k(ba).$$

Mas, $\varphi_k(a,b) = 0$, pois $k < n$ e, portanto, $d_k(ab) = \sum_{i+j=k} d_i(a)d_j(b)$. Por conseguinte,

$$\varphi_n(a,b)d_k([a,b]) = \varphi_n(a,b)\left(\sum_{i+j=k} d_i(a)d_j(b) - d_i(b)d_j(a)\right) =$$

$$= \varphi_n(a,b)\sum_{i+j=k}[d_i(a), d_j(b)] =$$

$$= 0, \text{ pelo lema2.1.9 } (ii).$$

Logo, $\varphi_n(a,b)d_k([a,b]) = 0$ para todo $k \leq m$.

Multipliquemos agora (6) por $\varphi_n(a,b) \in Z(R)$. Segue que $4(\varphi_n(a,b))^3 = 0$, donde $(\varphi_n(a,b))^3 = 0$, por R ser livre de 2-torção. Lembrando que anéis semiprimos não possuem elementos centrais nilpotentes não-nulos (lema 0.1.12), concluimos, finalmente, que $\varphi_n(a,b) = 0$, completando a prova do teorema. □

Capítulo 3

Derivações Algébricas

Neste capítulo, R é um anel primo (com unidade) não necessariamente comutativo e d uma derivação usual definida no anel R. $\mathbf{Q}$ denotará o anel de quocientes (à direita) de Martindale de R construído no capítulo 0 e $\mathbf{C}$ denotará o centróide estendido de R. O capítulo segue do trabalho de A.Leroy e J.Matczuk [16].

A derivação d pode ser estendida a uma única derivação $d^\star : Q \to Q$ de modo que $d^\star|_R = d$. Diremos que $d : R \to R$ é T-algébrica (sobre R) (onde T é um subanel de Q estável por $d^\star$), se existir um polinômio não-nulo $f(t)$ pertencente ao "skew" anel de polinômios $T[t; d^\star|_T]$ tal que $f(d)(R) = 0$ (ver definição 3.2.1). Ademais, d será dita X-interna, se existir um elemento $q \in \mathbf{Q}$ tal que $d(x) = qx - xq$ para todo $x \in R$.

V.K.Kharchenko em seu trabalho [13] mostrou que se d é R-algébrica e R é de característica zero, então d é X-interna. Apresentaremos uma prova simplificada deste resultado, devida a A.Leroy e J.Matczuk [16]. Além disto, demonstraremos o teorema 3.2.13, o qual afirma que $d^\star$ é R-algébrica $\Leftrightarrow$ $d^\star$ é $\mathbf{Q}$-algébrica $\Leftrightarrow$ d é $\mathbf{Q}$-algébrica $\Leftrightarrow$ d é R-algébrica $\Leftrightarrow$ $d^\star$ é $\mathbf{C}$-algébrica $\Leftrightarrow$ d é $\mathbf{C}$-algébrica.

3.1 Preliminares

Neste parágrafo apresentaremos algumas definições e resultados fundamentais para a compreensão do restante do capítulo. Iniciamos lembrando alguns relativos ao anel Q de quocientes (à direita) de Martindale de R que, embora tenham sido apresentados no capítulo 0, serão doravante utilizados com certa freqüência. Agrupamo-los no seguinte lema:

Lema 3.1.1 *Sejam R um anel primo (com unidade) e Q o anel de quocientes (à direita) de Martindale de R. Então:*
(i) $R \subseteq Q$;
(ii) se $a \in Q$, então existe um ideal bilátero não-nulo $\mathcal{I}$ de R tal que $a\mathcal{I} \subseteq R$;
(iii) se $a \in Q$ é tal que $a\mathcal{I} = 0$ ou $\mathcal{I}a = 0$ para algum $0 \neq \mathcal{I} \lhd R$, então $a = 0$;
(iv) se $(0) \neq \mathcal{I} \lhd R$ e $f : \mathcal{I} \to R$ é um homomorfismo de R-módulos à direita, então existe um elemento $a \in Q$ tal que $f(i) = ai$ para todo $i \in \mathcal{I}$;
(v) o centro $\mathbf{C}$ de Q é um corpo, chamado de centróide estendido de R.

Definição 3.1.2 Sejam R um anel (não necessariamente comutativo) e α um automorfismo de R. Uma aplicação $D : R \to R$ é dita uma α-DERIVAÇÃO, se para quaisquer elementos a, b de R tem-se
1. $D(a+b) = D(a) + D(b)$;
2. $D(ab) = D(a)\alpha(b) + aD(b)$.

Seja D uma α-derivação de R e X uma indeterminada sobre R. Se no conjunto $\mathbf{S} = \{\sum_{i=0}^{n} X^i a_i : a_i \in R\}$ consideramos a soma usual

$$\left(\sum_{i=0}^{n} X^i a_i\right) + \left(\sum_{i=0}^{n} X^i b_i\right) = \sum_{i=0}^{n} X^i (a_i + b_i)$$

e definimos o produto

$$\left(\sum_{i=0}^{n} X^i a_i\right)\left(\sum_{j=0}^{m} X^j b_j\right)$$

por distributividade e mediante a relação $aX = X\alpha(a) + D(a)$ para todo $a \in R$, obtemos o anel chamado "SKEW" ANEL DE POLINÔMIOS ou EXTENSÃO DE ÖRE de R, que denotamos por $\mathbf{S} = R[X; \alpha, D]$.

Se em particular $D = 0$, então $aX = X\alpha(a)$ para todo $a \in R$ e $\mathbf{S}$ será dito de TIPO AUTOMORFISMO. Neste caso, denotamos $\mathbf{S} = R[X; \alpha]$.

Se $\alpha = id_R$, D é uma derivação usual e então $aX = Xa + D(a)$ para todo $a \in R$. Neste caso $\mathbf{S}$ será dito de TIPO DERIVAÇÃO e denotado por $\mathbf{S} = R[X; D]$.

Proposição 3.1.3 *Sejam R um anel primo e $d : R \to R$ uma derivação. Então existe uma única derivação $d^\star : Q \to Q$ que é extensão de d (i.e., tal que $d^\star|_R = d$).*

prova : Seja $q \in Q$. Pelo lema 3.1.1 (ii), existe um ideal bilátero não-nulo $\mathcal{I}$ de R tal que $q\mathcal{I} \subseteq R$. Nosso propósito é definir $d^\star(q)$.

Dados $q \in Q$ e $i \in \mathcal{I}$, temos que $qi = r \in R$. Então, $d(qi) = d(r)$.

Para que $d^\star$ seja extensão de d e ainda continue sendo uma derivação, deve satisfazer $d(r) = d(qi) = d^\star(q)i + qd^\star(i)$.

Note que se $d(i) \in \mathcal{I}^2$, então $qd^\star(i) \in \mathcal{I} \subseteq R$ e também $d^\star(q)i \in R$. Por conseguinte, tomamos $i \in \mathcal{I}^3$, pois sendo d uma derivação e $\mathcal{I}$ um ideal bilátero, segue que $d(\mathcal{I}^3) \subseteq \mathcal{I}^2$ conforme desejado. Definimos então $d^\star(q) \in Q$ como sendo a aplicação $d^\star(q) : \mathcal{I}^3 \to R$ tal que

$$(1) \qquad d^\star(q)i = d(qi) - qd(i) \text{ para todo } i \in \mathcal{I}^3.$$

A própria expressão de $d^\star(q)$ nos mostra que $d^\star$ é bem definida, visto que independe da escolha do representante da classe de equivalência, uma vez que d já é bem definida. Vejamos agora que $d^\star$ é de fato uma derivação.

Sejam $q, q' \in Q$ e $i \in \mathcal{I}^3$. Sem perda de generalidade, suponhamos que $i = jl$, com $j \in \mathcal{I}^2$, $l \in \mathcal{I}$. Portanto,

$$\begin{aligned} d^\star(qq')i &= d(qq'i) - qq'd(i) = \\ &= d(q(q'j)l) - qq'd(jl). \end{aligned}$$

Note que $q'j \in \mathcal{I}$ e então $q(q'j) \in q\mathcal{I} \subseteq R$. Conseqüentemente, podemos computar $d((qq'j)l)$. Assim sendo,

$$\begin{aligned} d^\star(qq')i &= d((qq'j)l) - qq'd(jl) = \\ &= qq'jd(l) + d(qq'j)l - qq'jd(l) - qq'd(j)l = \\ &= d(qq'j)l - qq'd(j)l. \end{aligned}$$

Por outro lado,

$$\begin{aligned} qd^\star(q')i &= qd(q'i) - qq'd(i) = \\ &= qd((q'j)l) - qq'd(jl) = \\ &= qq'jd(l) + qd(q'j)l - qq'jd(l) - qq'd(j)l = \\ &= qd(q'j)l - qq'd(j)l \end{aligned}$$

e

$$\begin{aligned} d^\star(q)q'i &= d^\star(q)q'jl = \\ &= d(qq'jl) - qd(q'jl) = \\ &= qq'jd(l) + d(qq'j)l - qq'jd(l) - qd(q'j)l = \\ &= d(qq'j)l - qd(q'j)l. \end{aligned}$$

Comparando as expressões obtidas, $d^\star(qq')i = (qd^\star(q') + d^\star(q)q')i$ para todo $i \in \mathcal{I}^2$. Assim, $d^\star(qq') = qd^\star(q') + d^\star(q)q'$ e segue que $d^\star$ é uma derivação.

Observemos ainda que $d^\star$ estende d. De fato, sejam $r \in R$ e $i \in \mathcal{I}^2$. Como $d(ri) = rd(i) + d(r)i$, segue que $d^\star(r)i = d(ri) - rd(i) = d(r)i$. Assim sendo $(d^\star(r) - d(r))\mathcal{I} = 0$ donde $d^\star(r) = d(r)$.

A unicidade segue facilmente de (1) com um raciocínio semelhante ao do último parágrafo. □

Definição 3.1.4 Seja $d : R \to R$ uma derivação. Diremos que d é uma derivação INTERNA, se existir um elemento $a \in R$ tal que $d(x) = ax - xa$ para todo $x \in R$. Neste caso, d_a denotará esta derivação interna definida por a.

Por outro lado, diremos que $d : R \to R$ é X-INTERNA se existir um elemento $q \in Q$ tal que $d(x) = qx - xq$ para todo $x \in R$.

Observação 3.1.5 Kharchenko [13] provou que toda derivação algébrica sobre um anel primo de característica zero (no sentido da definição 3.2.1) é X-interna. Esta denominação tem sido dada justamente como homenagem a ele.

A seguir, mostraremos que vale o algoritmo da divisão à direita em $Q[t; d^\star]$, quando o divisor é um polinômio mônico não-nulo. O símbolo ∂ indicará o grau do polinômio.

Proposição 3.1.6 *Sejam $f(t)$, $g(t) \in Q[t; d^\star]$. Se $g(t)$ é um polinômio mônico, então existem únicos $q(t)$, $r(t) \in Q[t; d^\star]$ tais que $f(t) = q(t)g(t)+r(t)$, onde $r(t) = 0$ ou $\partial r(t) < \partial g(t)$.*

prova : Antes de iniciarmos é conveniente salientar que a prova é semelhante à conhecida no caso usual. Sejam

$$f(t) = t^m a_m + t^{m-1}a_{m-1} + \ \ldots \ + ta_1 + a_0, \ \ a_i \in Q \ \text{ e}$$

$$g(t) = t^n + t^{n-1}b_{n-1} + \ \ldots \ + tb_1 + b_0, \ \ b_i \in Q.$$

Existência: Se $f(t) = 0$, basta tomar $q(t) = r(t) = 0$. Suponhamos $f(t) \neq 0$. Assim, $\partial f(t) = m$. Se $m < n$, basta tomar $q(t) = 0$ e $r(t) = f(t)$. Portanto, podemos assumir $m \geq n$ e que o resultado é válido para todo polinômio de grau menor que $\partial f(t)$.

Agora seja $f_1(t)$ o polinômio definido por: $f(t) = t^{m-n}a_m g(t) + f_1(t)$. É fácil observarmos que $\partial f_1(t) < \partial f(t)$.

Pela hipótese de indução, existem $q_1(t), r_1(t)$ tais que: $f_1(t) = q_1(t)g(t) + r_1(t)$, onde $r_1(t) = 0$ ou $\partial r_1(t) < \partial g(t)$. Daí segue imediatamente que $f(t) = (q_1(t) + t^{m-n}a_m)g(t) + r_1(t)$. Portanto, tomando $q(t) = q_1(t) + t^{m-n}a_m$ e $r_1(t) = r(t)$, fica provada a existência.

Unicidade: A prova da unicidade é inteiramente análoga à do caso usual. □

Observação 3.1.7 No parágrafo seguinte trabalharemos com polinômios $f(t)$ e precisaremos computar $f(d)$, onde d é uma derivação.

Para fazer sentido calcular $f(d)$, devemos ter um homomorfismo*:* $R[t] \to End(R)$. No entanto, a aplicação acima será homomorfismo, somente se partirmos de $R[t; d]$. Isto é o que afirma o próximo lema, que apresentaremos sem demonstração.

Lema 3.1.8 *Considere φ a seguinte aplicação:*

$$\begin{array}{rcccl} \varphi & : & Q[t;d^\star] & \to & End(\mathbf{Q}) \\ & & \sum_{i=0}^n t^i q_i & \rightsquigarrow & \sum_{i=0}^n d^{\star i} q_i \quad : \quad \mathbf{Q} \to \mathbf{Q} \\ & & & & \qquad\qquad x \rightsquigarrow \sum_{i=0}^n d^{\star i}(x) q_i. \end{array}$$

Então φ é um homomorfismo de anéis, onde o produto em $End(\mathbf{Q})$ é a composição. Denotamos $f(d) \doteq \varphi(f)$.

3.2 Derivações Algébricas

Sejam d uma derivação definida num anel primo R e T um subanel de $\mathbf{Q}$ estável por $d^\star$ (i.e., $d^\star(T) \subseteq T$).

No nosso estudo de derivações algébricas vamos considerar os polinômios em d onde os coeficientes não são necessariamente constantes sob d (i.e., não necessariamente se anulam sob d); será prático tratá-los como elementos do "skew" anel de polinômios.

Definição 3.2.1 *Diremos que d é T-algébrica sobre um ideal não-nulo $\mathcal{I}$ de R, se existir um polinômio não-nulo $f(t) \in T[t; d^\star\,|_T]$ tal que $f(d)(\mathcal{I}) = 0$ (conforme lema 3.1.8).*

Se $\mathcal{I} = R$, diremos simplesmente que d é T-algébrica.

Por grau da derivação algébrica entendemos o mínimo grau de um polinômio $f(t)$ nas condições acima e o denotamos por $\partial f(t)$.

Lembramos que derivações aplicam o centro do anel nele próprio (lema 2.1.8): assim, $d^\star|_{\mathbf{C}}$ é derivação em $\mathbf{C}$.

Lema 3.2.2 *Se d é $\mathbf{C}$-algébrica, então d é R-algébrica.*

prova : De fato, existe um polinômio não-nulo
$f(t) = t^n c_n + t^{n-1}c_{n-1} + \cdots + c_0 \in \mathbf{C}[t; d^\star|_{\mathbf{C}}]$ tal que $f(d)(R) = 0$. Pelo lema 3.1.1 (i) e (ii), existe $0 \neq \mathcal{J} \lhd R$ tal que $c_i\mathcal{J} \subseteq R$ para todo i e $c_i\mathcal{J} \neq 0$ para algum i. Seja $j \in \mathcal{J}$ tal que $0 \neq c_i j \in R$ (temos $c_i j \neq 0$ para algum i por (iii) do lema 3.1.1). Portanto, $\sum_{i=0}^{n} d^i(r)(c_i j) = 0$ para todo $r \in R$, e d é R-algébrica. □

O teorema 3.2.12 que demonstraremos logo mais nos dá uma recíproca deste fato.

Lema 3.2.3 *Seja d uma derivação R-algébrica de grau n. Então d satisfaz um polinômio mônico $g(t) \in Q[t; d^\star]$ de grau n. Ademais, se a característica de R for maior do que n, então d é X-interna.*

prova : Seja

$$\mathcal{A} = \{r \in R \mid \exists (r_{n-1}, r_{n-2}, ..., r_1, r_0) \in R^n \; tq. \; d^n(x)r + d^{n-1}(x)r_{n-1} + ... + xr_0 = 0, \forall x \in R\}.$$

Sejam $x \in R, r \in \mathcal{A}$ e $r_{n-1}, r_{n-2}, ..., r_1, r_0 \in R$ elementos como aparecem na definição de $\mathcal{A}$. Vemos que $\mathcal{A}$ é um ideal à direita de R e, como d é R-algébrica de grau n, $\mathcal{A} \neq 0$. Sabemos, pela proposição 0.3.2 que, para todo $m \leq n$ e para qualquer $y \in R$, $d^m(yx) = \sum_{i=0}^{n} \binom{m}{i} d^i(y)d^{m-i}(x)$. Portanto,

$$0 = d^n(yx)r + d^{n-1}(yx)r_{n-1} + \; \ldots \; + d(yx)r_1 + yxr_0 =$$

$$= \sum_{i=0}^{n} \binom{n}{i} d^i(y)d^{n-i}(x)r + \sum_{i=0}^{n-1} \binom{n-1}{i} d^i(y)d^{n-1-i}(x)r_{n-1} + \ldots + yd(x)r_1 + d(y)xr_1 + yxr_0 =$$

$$= y\left(d^n(x)r + d^{n-1}(x)r_{n-1} + \ldots + d(x)r_1 + xr_0\right) +$$
$$+ \; d(y)\left(nd^{n-1}(x)r + (n-1)d^{n-2}(x)r_{n-1} + \ldots + xr_1\right) + \; \ldots$$
$$\ldots \; + d^{n-1}(y)\left(nd(x)r + xr_{n-1}\right) + d^n(y)xr =$$
$$= d^n(y)xr + d^{n-1}(y)\left(nd(x)r + xr_{n-1}\right) + \; \ldots$$
$$\ldots \; + d(y)\left(nd^{n-1}(x)r + (n-1)d^{n-2}(x)r_{n-1} + \ldots + xr_1\right) +$$
$$+ \; y\left(d^n(x)r + d^{n-1}(x)r_{n-1} + \ldots + d(x)r_1 + xr_0\right).$$

Isto é, para $r \in \mathcal{A}$ e $x \in R$, existe um polinômio com termo dominante xr que se anula em y para todo $y \in R$, ou seja, $\mathcal{A}$ é ideal à esquerda também. Logo, é um ideal bilátero não-nulo de R.

Definamos, para cada $i = 0,\ 1,\ \cdots,\ n$, as aplicações $\varphi_i : \mathcal{A} \to R$ tais que $\varphi_i(r) = r_i$, onde $r_n = r$ e $(r_{n-1}, ..., r_0)$ é uma upla associada a r como na definição de $\mathcal{A}$. Como d é R-algébrica de grau n, todas as aplicações φ_i são bem definidas. De fato, sejam $r,\ r' \in \mathcal{A}$ tais que $r = r'$. Então, para $r \in \mathcal{A}$, existem $r_{n-1}, ..., r_0$ como na definição de $\mathcal{A}$. Analogamente para $r' \in \mathcal{A}$, ambos satisfazendo um polinômio de grau n, isto é,

$$\begin{aligned} d^n(x)r + d^{n-1}(x)r_{n-1} + \cdots + xr_0 &= 0 \text{ e} \\ d^n(x)r' + d^{n-1}(x)r'_{n-1} + \cdots + xr'_0 &= 0,\ \forall\ x \in R. \end{aligned}$$

Como $r = r'$, as expressões acima nos dão

$$d^{n-1}(x)(r_{n-1} - r'_{n-1}) + d^{n-2}(x)(r_{n-2} - r'_{n-2}) + \cdots + x(r_0 - r'_0) = 0 \text{ para todo } x \in R.$$

O polinômio encontrado acima é de grau estritamente menor do que n e é anulado por todo $x \in R$, contrariando a minimalidade de n. Logo $r_i - r'_i = 0$ e as φ_i's estão bem definidas para todo $i \in \{0, 1, ..., n\}$.

Para $r,\ r' \in \mathcal{A}$ e $s \in R$, podemos verificar facilmente que $\varphi_i(rs) = \varphi_i(r)s$ e $\varphi_i(r+r') = \varphi_i(r)+\varphi_i(r')$ para todo $i \in \{0, 1, \cdots, n\}$. Logo as φ_i's são homomorfismos de R-módulos à direita. Então, pelo item (iv) do lema 3.1.1, existem $q_0,\ q_1,\ \cdots,\ q_{n-1},\ q_n = 1$ em Q tais que $\varphi_i(r) = q_i r$ para todo $r \in \mathcal{A}$ e para todo $i \in \{0, 1, \cdots, n\}$. Por conseguinte,

$$0 = d^n(x)r + d^{n-1}(x)r_{n-1} + \ \ldots\ + xr_0 = \left(d^n(x) + d^{n-1}(x)q_{n-1} + \ldots + xq_0\right) r$$

para cada $r \in \mathcal{A}$ e para qualquer $x \in R$, onde o fator entre parênteses na expressão acima é um elemento de Q. Como $r \in \mathcal{A}$ é arbitrário, o item (iii) do lema 3.1.1 mostra que $g(d)(x) = 0$ para todo $x \in R$, onde

$$g(t) = t^n + t^{n-1}q_{n-1} + \ \ldots\ + tq_1 + q_0 \in Q[t; d^\star].$$

Suponhamos agora que $n <$ característica R (note então que neste caso n é um inversível em Q, pelo lema 0.2.23). Sejam $x,\ y \in R$. Então

$$\begin{aligned} 0 = g(d)(xy) = \\ &= x\left(d^n(y) + d^{n-1}(y)q_{n-1} + \ldots + d(y)q_1 + yq_0\right) + \\ &+ d(x)\left(nd^{n-1}(y) + (n-1)d^{n-2}(y)q_{n-1} + \ldots + yq_1\right) + \ \ldots \\ &\ldots\ + d^{n-1}(x)\left(nd(y) + yq_{n-1}\right) + d^n(x)y. \end{aligned}$$

Temos ainda que

$$0 = g(d)(x)y = d^n(x)y + d^{n-1}(x)q_{n-1}y + \ \ldots\ + d(x)q_1y + xq_0y.$$

Dado que $\partial d = n$ e que x é arbitrário, ao subtrairmos as duas expressões acima e compararmos os coeficientes, resulta que $nd(y) + yq_{n-1} = q_{n-1}y$ para todo $y \in R$. Pela hipótese sobre a característica de R, podemos escrever $d^\star(y) = \frac{q_{n-1}}{n}y - y\frac{q_{n-1}}{n} = = \left[\frac{q_{n-1}}{n}, y\right]$ para todo $y \in R$. Logo, d é X-interna. □

Exemplo 3.2.4 É conveniente destacar o fato de que a hipótese sobre a característica de R é essencial para a validade da última afirmação do lema 3.2.3. De fato, se d é a derivação "standart" de $\mathcal{F}(t)$, o corpo das funções racionais sobre um corpo $\mathcal{F}$ de característica $p < \infty$, então é fácil verificar que $d^p = 0$.

Ademais, num anel comutativo toda derivação interna é a derivação identicamente nula. Como $\mathcal{F}(t)$ é comutativo e d é uma derivação não-trivial, segue que d não é interna.

Observação 3.2.5 Podemos estender $d^\star : Q \to Q$ *a* $Q[t; d^\star]$, bastando para isto definir para um elemento $f(t) = \sum_{i=0}^{n} t^i q_i \in Q[t; d^\star]$, $d^\star(f(t)) = \sum_{i=0}^{n} t^i d^\star(q_i)$.

Uma indução fácil mostra que $qt^l = \sum_{i=0}^{l} \binom{l}{i} t^i d^{\star l-i}(q)$ para todo $q \in Q$. De fato, se vale a fórmula acima, pela lei de comutação $qt = tq + d^\star(q)$ em $\mathbf{Q}[t; d^\star]$, temos:

$$qt^{l+1} = qt^l t = \sum_{i=0}^{l} \binom{l}{i} t^i d^{\star l-i}(q)t = \sum_{i=0}^{l} \binom{l}{i} t^i t d^{\star l-i}(q) + \sum_{i=0}^{l} \binom{l}{i} t^i d^{\star l-i+1}(q) =$$

$$= t^{l+1}q + \sum_{i=1}^{l} \binom{l}{i-1} t^i d^{\star l+1-i}(q) + \sum_{i=1}^{l} \binom{l}{i} t^i d^{\star l=1-i}(q) + d^{\star l=1}(q) =$$

$$= \sum_{i=1}^{l} \binom{l+1}{i} t^i d^{\star l+1-i}(q) \ + \ t^{l+1}q \ + \ d^{\star l+1}(q) =$$

$$= \sum_{i=0}^{l+1} \binom{l+1}{i} t^i d^{\star l+1-i}(q).$$

Agora é fácil verificar que $d^\star$ resulta também uma derivação em $\mathbf{Q}[t; d^\star]$.

No próximo lema utilizaremos a notação $f(d) = 0$ indicando que, para o polinômio $f(t)$ acima, $f(d)(x) = \sum_{i-0}^{n} d^i(x)q_i = 0$ para todo $x \in R$. Do mesmo modo, $d^\star(f(d)) = 0$ indicará que $\sum_{i=0}^{n} d^i(x)d^\star(q_i) = 0$ para todo $x \in R$.

Lema 3.2.6 *Sejam $d : R \to R$ uma derivação e $d^\star : Q[t; d^\star] \to Q[t; d^\star]$ a sua extensão a $Q[t; d^\star]$. Se existir um polinômio mônico $f(t) \in Q[t; d^\star]$ de grau n tal que $f(d) = 0$, então $d^\star(f(d)) = 0$.*

prova : Suponhamos que $f(d) = 0$, ou seja, $\sum_{i=0}^{n} d^i(x)q_i = 0$ para todo $x \in R$, com $q_i \in \mathbf{Q}$, $q_n = 1$. Aplicando $d^\star$ a esta expressão, temos $\sum_{i=0}^{n} d^{i+1}(x)q_i + \sum_{i=0}^{n} d^i(x)d^\star(q_i) = 0$ para todo $x \in R$. Mas, $\sum_{i=0}^{n} d^{i+1}(x)q_i = \sum_{i=0}^{n} d^i(d(x))q_i$. Como por hipótese $\sum_{i=0}^{n} d^i(x)q_i = 0$ para todo $x \in R$, vale também no caso particular em que $d(x) \in R$ é tomado no lugar de x. Portanto, $\sum_{i=0}^{n} d^i(d(x))q_i = 0$. Logo, $\sum_{i=0}^{n} d^i(x)d^\star(q_i) = 0$ para todo $x \in R$. Conseqüentemente, $d^\star(f(d)) = 0$. □

Corolário 3.2.7 *Se $g(t) = t^n + t^{n-1}q_{n-1} + \cdots + tq_1 + q_0 \in \mathbf{Q}[t; d^\star]$ é um polinômio mônico de grau n anulado por d, então $g(t)$ satisfaz as seguintes propriedades:*
(i) $d^\star(q_i) = 0$ para $i = 0, 1, \cdots, n-1$, isto é, $g(t)$ tem coeficientes constantes;
(ii) $\sum_{i=j+1}^{n} \binom{i}{j} d^{i-j}(x)q_i = q_j x - xq_j$ para todo $x \in R$ e qualquer $j = 0, 1, \cdots, n-1$;
(iii) o polinômio $g(t)$ pertence ao centro de $Q[t; d^\star]$;
(iv) $[q_i, q_j] = 0$ para $0 \leq i \leq j \leq n-1$;
(v) $q_0 = 0$.
Em particular, valem para o polinômio construído no lema 3.2.3.

prova : (i) Sabemos que $g(d) = 0$ ($g(t)$ existe pelo lema 3.2.3). Portanto, pelo lema 3.2.6, $d^\star(g(t))$ anula d e como $q_n = 1$ e $d^\star(1) = 0$, ele é um polinômio de grau menor que $\partial g(t)$ que anula d. Logo $d^\star(g(t)) = 0$ é o polinômio identicamente nulo, donde os coeficientes $d^\star(q_i)$, $i = 0, 1, \cdots, n-1$, são todos nulos.

(ii) Como na prova do lema 3.2.3, a identidade $g(d)(xy) - g(d)(x)y = 0$ para $x, y \in R$, fornece um polinômio de grau menor do que n e que anula d. Então os coeficientes deste polinômio devem ser todos nulos e disto resultam as igualdades desejadas.

(iii) Da lei de comutação $qt = tq + d^\star(q)$ em $Q[t; d^\star]$ e da parte (i) provada acima, resulta claramente que $tg(t) = g(t)t$ em $Q[t; d^\star]$.

Por outro lado, vimos na observação 3.2.5 que $qt^l = \sum_{i=0}^{l} \binom{l}{i} t^i d^{\star l-i}(q)$ para todo $q \in Q$. Utilizando esta fórmula e a parte (ii), obtemos $g(t)a = ag(t)$ para todo $a \in R$. De fato,

$$\begin{aligned}
ag(t) - g(t)a = t^n a + \sum_{i=0}^{n-1} \binom{n}{i} t^i d^{\star n-i}(a) + t^{n-1} a q_{n-1} + \sum_{i=0}^{n-2} \binom{n-1}{i} t^i d^{\star n-1-i}(a) q_{n-1} + \\
+ t^{n-2} a q_{n-2} + \sum_{i=0}^{n-3} \binom{n-2}{i} t^i d^{\star n-2-i}(a) q_{n-2} + \ \ldots \ + t^2 a q_2 + \\
+ 2td^{\star}(a)q_2 + d^{\star 2}(a)q_2 + d^{\star}(a)q_1 + taq_1 + aq_0 - t^n a - \\
- t^{n-1} q_{n-1} a - t^{n-2} q_{n-2} a - \ \ldots \ - t^2 q_2 a - t q_1 a - q_0 a = \\
= -t^{n-1}(q_{n-1}a - aq_{n-1}) - t^{n-2}(q_{n-2}a - aq_{n-2}) - \ \ldots \\
\ldots \ - t^2(q_2 a - aq_2) - t(q_1 a - aq_1) - (q_0 q - aq_0) + \\
+ \sum_{i=0}^{n-1} \binom{n}{i} t^i d^{\star n-i}(a) + \sum_{i=0}^{n-2} \binom{n-1}{i} t^i d^{\star n-1-i}(a) q_{n-1} + \\
+ \sum_{i=0}^{n-3} \binom{n-2}{i} t^i d^{\star n-2-i}(a) q_{n-2} + 2td^{\star}(a)q_2 + \\
+ d^{\star 2}(a)q_2 + \ d^{\star}(a)q_1 = \\
= -t^{n-1} n d(a) - t^{n-2} \sum_{i=n-1}^{n} \binom{i}{n-2} d^{i-(n-2)}(a) q_i - \ \ldots \\
\ldots \ - t \sum_{i=2}^{n} \binom{i}{1} d^{i-1}(a) q_i - \sum_{i=1}^{n} d^i(a) q_i + \\
+ \sum_{i=0}^{n-1} \binom{n}{i} t^i d^{\star n-1}(a) + \sum_{i=0}^{n-2} \binom{n-1}{i} t^i d^{\star n-1-i}(a) q_{n-1} + \ \ldots \\
\ldots \ + 2td^{\star}(a)q_2 + d^{\star 2}(a)q_2 + d^{\star}(a)q_1 = 0.
\end{aligned}$$

Logo, $ag(t) = g(t)a$ para todo $a \in R$.

Sejam agora $q \in Q$ e $(0) \neq \mathcal{I} \lhd R$ tais que $q\mathcal{I} \subseteq R$. Portanto, para todo $a \in \mathcal{I}$, em $Q[t; d^{\star}]$ temos $g(t)qa = qag(t)$, pois $qa \in R$. Do mesmo modo, $qag(t) = qg(t)a$, pois $a \in R$. Então, $(g(t)q - qg(t))a = 0$ para todo $a \in \mathcal{I}$.

Segue que $g(t)q - qg(t) = 0$ para todo $q \in \mathbf{Q}$. Esta relação junto com $tg(t) = g(t)t$ prova que $g(t)$ pertence ao centro de $Q[t; d^\star]$.

(iv) Por (i), temos $d^\star(q_i) = 0$ para todo $0 \leq i \leq n-1$. Sabemos que $q_i t^l = \sum_{j=0}^{l} \binom{l}{j} t^j d^{\star l-j}(q_i)$ e, por (iii), $q_i g(t) = g(t)q_i$. Comparando os coeficientes, concluimos que $q_i q_j = q_j q_i$ para $0 \leq i \leq j \leq n-1$.

(v) Temos $g(d)(x) = 0$ para todo $x \in R$. Ou seja,

$$0 = d^n(x) + d^{n-1}(x)q_{n-1} + \cdots + d(x)q_1 + xq_0 = \sum_{i=1}^{n} d^i(x)q_i + xq_0.$$

No entanto, pela parte (ii) com $j = 0$, temos $\sum_{i=1}^{n} d^i(x)q_i = q_0 x - xq_0$. Portanto, segue que $q_0 x = 0$ para todo $x \in R$. Logo, $q_0 = 0$. □

Corolário 3.2.8 *Se d é uma derivação algébrica sobre um anel primo R, então o centro de $Q[t; d^\star]$ não está contido em Q.*

prova : Vimos que $g(t)$ como acima possui grau positivo e pertence ao centro de $Q[t; d^\star]$. Logo o centro de $Q[t; d^\star]$ é não-trivial, i.e., $Z(Q[t; d^\star]) \not\subseteq Q$. □

Lema 3.2.9 *Seja d uma derivação X-interna em R, definida por um elemento $a \in Q$. Então as seguintes afirmações são equivalentes:*
(i) a é algébrico sobre $\mathbf{C}$;
(ii) d é $\mathbf{C}$-algébrica;
(iii) d é R-algébrica;
(iv) $d^\star$ é $\mathbf{C}$-algébrica;
(v) $d^\star$ é R-algébrica.

Ademais, se uma destas afirmações é verificada, então o grau de a sobre $\mathbf{C}$ é igual ao grau de d sobre R.

prova : $(i) \to (ii)$ Suponhamos que $a \in Q$ seja algébrico de grau n sobre $\mathbf{C}$. Seja $\sum_{i=0}^{n} t^i c_i \in \mathbf{C}[t; d^\star|_{\mathbf{C}}]$ com $c_n = 1$ um polinômio minimal de a sobre $\mathbf{C}$.

Como $d(x) = ax - xa$ para todo $x \in R$, temos que $(d-a)(x) = (-1)xa$ para todo $x \in R$. Isto é, aplicar $(d-a)$ ao elemento $x \in R$ significa multiplicá-lo por (-1) à esquerda e por a à direita. Portanto,

$$(d-a)^2(x) = (d-a)((d-a)(x)) = (-1)(-1)xaa = xa^2.$$

Utilizando uma indução trivial, chega-se a $(d-a)^i(x) = (-1)^i xa^i$ para todo $0 \leq i \leq n$ e para qualquer $x \in R$. Então,

$$0 = \sum_{i=0}^{n} a^i c_i = x \sum_{i=0}^{n} a^i c_i = \sum_{i=0}^{n} xa^i c_i = \sum_{i=0}^{n} (-1)^i (d-a)^i(x) c_i.$$

Isto significa que d satisfaz um polinômio mônico de grau n sobre $\mathbf{C}[a]$, ou seja, d é $\mathbf{C}[a]$-algébrica. Visto que $\mathbf{C}[a][d]$ é finito-dimensional sobre $\mathbf{C}[a]$ e $\mathbf{C}[a]$ é finito-dimensional sobre $\mathbf{C}$, por transitividade temos que $\mathbf{C}[a][d]$ é finito-dimensional sobre $\mathbf{C}$, digamos de grau $m < \infty$. Então 1, d, d^2, $\cdots$, d^m ($m+1$ elementos) são linearmente dependentes sobre $\mathbf{C}$. Portanto existem elementos b_0, b_1, $\cdots$, $b_m \in \mathbf{C}$ não todos nulos tais que $\sum_{i=0}^{m} d^i b_i = 0$ e isto nos diz que d é $\mathbf{C}$-algébrica.

$(ii) \to (iii)$ É justamente o lema 3.2.2.

$(iii) \to (i)$ Suponhamos d R-algébrica de grau n e seja $f(t) = \sum_{i=0}^{n} t^i r_i \in R[t;d]$ um polinômio minimal para d sobre R. Como $d(x) = ax - xa$ para todo $x \in R$, segue que $d^2(x) = d(d(x)) = d(ax) - d(xa) = a^2x - 2axa + xa^2$ para todo $x \in R$. Por indução, podemos provar facilmente que $d^i(x) = \sum_{j=0}^{i} (-1)^{i+j} \binom{i}{j} a^j x a^{i-j}$ para todo $0 \leq i \leq n$ e qualquer $x \in R$. Portanto,

$$0 = f(d)(x) = \sum_{i=0}^{n} \left(\sum_{j=0}^{i} (-1)^{i+j} \binom{i}{j} a^j x a^{i-j} \right) r_i \text{ para todo } x \in R.$$

Trocando a ordem das parcelas, obtemos $0 = \sum_{j=0}^{n} a^j x f_j(a)$ para todo $x \in R$, onde $f_j(a) = \sum_{i=j}^{n} a^{i-j} (-1)^{i+j} \binom{i}{j} r_i$.

Por ser R um anel primo, o lema 0.2.22 nos diz que a é algébrico sobre $\mathbf{C}$ de grau inferior ou igual a n.

Para provarmos $(i) \leftrightarrow (iv) \leftrightarrow (v)$ valemo-nos de raciocínios inteiramente análogos aos acima:

$(i) \to (iv)$ É análogo ao argumento utilizado para mostrar que $(i) \to (ii)$.

$(iv) \to (v) \to (i)$ É imediato, tendo em vista a prova de $(ii) \to (iii) \to (i)$.

$(v) \to (ii)$ Utiliza-se o mesmo argumento de $(iii) \to (i) \to (ii)$. □

Teorema 3.2.10 *Seja n menor do que a característica de R. Se d é R-algébrica de grau n, então:*
(i) d é X-interna;
(ii) $d^\star$ satisfaz o mesmo polinômio minimal com coeficientes em R que d;
(iii) $d^\star$ é $\mathbf{C}$-algébrica;
(iv) $d^\star$ satisfaz o mesmo polinômio minimal com coeficientes em $\mathbf{C}$ que d.

demonstração : (i) É exatamente a afirmação do lema 3.2.3.

(ii) Sabemos que d satisfaz um polinômio mônico $g(t) \in Q[t; d^\star]$ de grau n, pelo lema 3.2.3.

Basta mostrar que $g(d^\star)(x) = 0$ para qualquer $\mathbf{x} \in \mathbf{Q}$. De fato, seja $f(t)$ um polinômio minimal para d com coeficientes em R. Pela proposição 3.1.6, podemos dividir $f(t)$ por $g(t)$ à direita em $Q[t; d^\star]$, encontrando polinômios $p(t)$ e $r(t)$ tais que $f(t) = p(t)g(t) + r(t)$, com $r(t) = 0$ ou $\partial r(t) < \partial g(t)$. Assim, $f(d^\star) = p(d^\star)g(d^\star) + r(d^\star)$. Para $\mathbf{x} \in \mathbf{R}$, temos $0 = f(d^\star)(x) = p(d^\star)(g(d^\star(x)) + r(d^\star)(x) = r(d^\star)(x)$. Ou seja, $r(d^\star)(x) = 0$ para todo $x \in R$. O fato de que o grau de $g(t)$ é igual ao grau de d sobre R (conforme lema 3.2.3) implica que $r(t) = 0$. Logo, $f(t) = p(t)g(t)$ em $\mathbf{Q}[t; d^\star]$. Se provarmos que $g(d^\star(x)) = 0$ para todo $\mathbf{x} \in \mathbf{Q}$, teremos que $0 = p(d^\star)(g(d^\star(x))) = f(d^\star(x))$ para todo $x \in \mathbf{Q}$. Portanto, $d^\star$ satisfaz o mesmo polinômio minimal com coeficientes em R que d.

Passemos então a mostrar que $g(d^\star)(x) = 0$ para qualquer $\mathbf{x} \in \mathbf{Q}$.

Como d é X-interna, seja $a \in Q$ tal que $d^\star$ é a derivação interna induzida por a, isto é, $d^\star(x) = ax - xa$ para todo $\mathbf{x} \in \mathbf{Q}$. Pelo lema 3.2.9, $d^\star$ é R-algébrica. Obviamente o grau de algebricidade de $d^\star$ segue sendo n. Agora, aplicando o lema 3.2.3 a $d^\star$, temos que $d^\star$ satisfaz um polinômio mônico $f(t) \in Q[t; d^\star]$ de grau n. Então é evidente que $f(d)(x) = 0$ para todo $\mathbf{x} \in \mathbf{R}$. Como $\partial g(t) = n = \partial f(t)$, os polinômios $f(t)$ e $g(t)$ são iguais. Por conseguinte, $g(d^\star) = 0$.

(iii) Pelo item (i), $d^\star$ é interna definida por um elemento $a \in Q$ e, por (ii), $d^\star$ é R-algébrica de grau n. O lema 3.2.9 mostra que $d^\star$ é $\mathbf{C}$-algébrica.

(*iv*) Sejam $f(t)$ um polinômio minimal para d com coeficientes em $\mathbf{C}$ e $g(t)$ o polinômio mônico para d com coeficientes em Q introduzido no lema 3.2.3. O mesmo raciocínio utilizado no item (*ii*) mostra que $f(t) = p(t)g(t)$ em $\mathbf{Q}[t; d^\star]$ para algum $p(t) \in \mathbf{Q}[t; d^\star]$. Por (*ii*), $g(d^\star) = 0$, donde $f(d^\star) = 0$. □

Observação 3.2.11 A primeira afirmação do teorema no caso em que a característica de R é infinita também foi obtida por Kharchenko [13] em seu estudo sobre a teoria das identidades diferenciais.

Lema 3.2.12 *Seja d uma derivação R-algébrica. Se característica $R = p < \infty$, então existem elementos c_0, c_1, $\cdots$, c_n de $\mathbf{C}_{d^\star} = \{c \in \mathbf{C} \mid d^\star(c) = 0\}$ tais que $\delta = \sum_{i=1}^{m} d^{\star p^i} c_i$ é uma derivação interna de Q induzida por um elemento algébrico sobre $\mathbf{C}$.*

prova : O corolário 3.2.7 nos permite escolher um polinômio $f(t) = \sum_{i=0}^{l>0} t^i a_i$ de grau mínimo no centro de $Q[t; d^\star]$. Mostraremos inicialmente que os polinômios $f_j(t) = \sum_{i=j}^{l>0} t^{i-j} \binom{i}{j} a_i$ são centrais.

Igualando os coeficientes dos monômios de mesmo grau em $tf(t) = f(t)t$ e lembrando que $qt = tq + d^\star(q)$ para todo $q \in Q$, obtemos:

$$\sum_{i=0}^{l>0} t^{i+1} a_i = tf(t) = f(t)t = \sum_{i=0}^{l>0} t^i a_i t = \sum_{i=0}^{l>0} t^{i+1} a_i + \sum_{i=0}^{l>0} t^i d^\star(a_i),$$

donde segue que $d^\star(a_0) = 0$ (termo independente).

Comparando os coeficientes dos termos de grau 1, temos $a_0 = a_0 + d^\star(a_1)$, donde $d^\star(a_1) = 0$. Sucessivamente, encontramos $d^\star(a_i) = 0$ para todo $0 \leq i \leq l$. Portanto, $f_j(t) = tf_j(t) + \sum_{i=j}^{l>0} t^{i-j} d^\star(a_i) \binom{i}{j} = tf_j(t)$ para todo $j = 0, 1, \cdots, l$. Como para cada $x \in Q$, $xf(t) = f(t)x$ e já sabemos que $xt^u = \sum_{i=0}^{u} t^i \binom{u}{i} d^{\star u-i}(x)$ para todo $x \in Q$ e para todo $u \in \mathbf{N}$, segue que

$$\sum_{i=0}^{l} \sum_{j=0}^{i} t^j \binom{i}{j} d^{\star i-j}(x) a_i = \sum_{i=0}^{l} x t^i a_i = x \sum_{i=0}^{l} t^i a_i = xf(t) = f(t)x = \sum_{i=0}^{l} t^i a_i x.$$

Logo,

$$\sum_{i-0}^{l} \left(t^i a_i x - \sum_{j=0}^{i} t^j d^{\star i-j}(x) \binom{i}{j} a_i \right) = 0.$$

Comparando os coeficientes de t^k para todo $k \in \{0, 1, \ \ldots \ , l\}$, segue que

$$b_k \doteq a_k x - \sum_{i=k}^{l} d^{\star^{i-k}}(x)\tbinom{i}{k} a_i = 0$$

para todo $x \in Q$ e qualquer $k \in \{0, 1, \cdots, l\}$. Calculando $f_j(t)x - x f_j(t)$ para todo $x \in Q$ e qualquer $j \in \{1, \cdots, l\}$ (tomamos $j \geq 1$ para que os f_j tenham grau menor do que ∂f), obtemos

$$f_j(t)x - x f_j(t) = \sum_{k=j}^{l} t^{k-j}\tbinom{k}{j} a_k x - x \sum_{i=j}^{l} t^{i-j}\tbinom{i}{j} a_i = \sum_{k=j}^{l} t^{k-j}\tbinom{k}{j} a_k x - x \sum_{i=0}^{l-j} t^i \tbinom{i+j}{j} a_{i+j} =$$

$$= \sum_{k=j}^{l} t^{k-j}\tbinom{k}{j} a_k x - \sum_{i=0}^{l-j}\sum_{r=0}^{i} t^r d^{\star^{i-r}}(x)\tbinom{i}{r}\tbinom{i+j}{j} a_{i+j} =$$

$$= \sum_{k=j}^{l} t^{k-j}\tbinom{k}{j} a_k x - \sum_{r=0}^{l-j}\sum_{i=r}^{l-j} t^r d^{\star^{i-r}}(x)\tbinom{i}{r}\tbinom{i+j}{j} a_{i+j} =$$

$$= \sum_{k=j}^{l} t^{k-j}\tbinom{k}{j} a_k x - \sum_{r=j}^{l}\sum_{i=r-j}^{l-j} t^{r-j} d^{\star^{i+j-r}}(x)\tbinom{i}{r-j}\tbinom{i+j}{j} a_{i+j} = \sum_{k=j}^{l} t^{k-j} s_k,$$

onde s_k é dado por

$$s_k = \tbinom{k}{j} a_k x - \sum_{i=k-j}^{l-j} d^{\star^{i+j-k}}(x)\tbinom{i}{k-j}\tbinom{i+j}{j} a_{i+j} = \tbinom{k}{j} a_k x - \sum_{i=k}^{l} d^{\star^{i-k}}(x)\tbinom{i-j}{k-j}\tbinom{i}{j} a_i$$

para cada $k \in \{j, \cdots, l\}$. Mas, $\binom{i}{j}\binom{i-j}{k-j} = \binom{k}{j}\binom{i}{i-k}$, donde,

$$s_k = \tbinom{k}{j}\left(a_k x - \sum_{i=k}^{l} d^{\star^{i-k}}(x)\tbinom{i}{i-k} a_i\right) =$$

$$= \tbinom{k}{j}\left(a_k x - \sum_{i=k}^{l} d^{\star^{i-k}}(x)\tbinom{i}{k} a_i\right) =$$

$$= \tbinom{k}{j} b_k =$$

$$= 0 \ \text{ para } \ k \in \{j, \ \ldots \ , l\}.$$

Portanto, $f_j(t)x - xf_j(t) = \sum_{k=j}^{l} t^{k-j}\binom{k}{j}b_k = 0$ para todo $x \in Q$ e qualquer $k \in \{j, \cdots, l\}$. Isto conclui a prova de que os $f_j(t)$'s pertencem ao centro de $Q[t; d^\star]$.

A minimalidade do grau de $f(t)$ em relação ao centro de $Q[t; d^\star]$ implica que $\partial f_j(t) = 0$ para $j \in \{1, \ldots, l\}$. Isto significa que $f_j(t) = a_j \in Q$. Por conseguinte $xa_j = a_j x$ para todo $x \in Q$, o que quer dizer que $a_j \in \mathbf{C}$.

Do mesmo modo $ta_j = a_j t$, o que mostra que $d^\star(a_j) = 0$. Ou seja, $a_j \in \mathbf{C}_{d^\star}$.

Ademais, dada a definição de $f_j(t)$ e visto que $f_j(t)$ tem grau zero, segue que $\binom{i}{j}a_i = 0$ para todo i, j tais que $1 \leq j < i \leq l$.

Utilizemos agora a hipótese sobre a característica de R. Supondo que característica de $R = p < \infty$, os inteiros i para os quais $\binom{i}{j} \equiv 0(mod\ p)$ para todo $0 < j < i$ são $i = p, p^2, \ldots$. De modo que $a_i = 0$, se i não for zero nem potência de p. Então, tomando $c_i = a_{p^i}$, obtemos $f(t) = \sum_{i=0}^{m} t^{p^i}c_i + a_0$, onde $c_i \in \mathbf{C}_{d^\star}$ e $d^\star(a_0) = 0$.

Tomando a expressão de b_k acima, com $k = 0$, temos:

$$0 = b_0 = a_0 x - \sum_{i=0}^{l} d^{\star^i}(x)a_i = a_0 x - xa_0 - \sum_{i=1}^{l} d^{\star^i}(x)a_i$$

para todo $x \in Q$. Isto é equivalente a dizer que $\sum_{i=0}^{m} d^{\star^{p^i}}(x)c_i = a_0 x - xa_0$ para todo $x \in Q$. Então $\delta(x) \doteq \sum_{i=0}^{m} d^{\star^{p^i}}(x)c_i$ define uma derivação interna em Q induzida por $b = a_0$.

Resta-nos mostrar que b é algébrico sobre $\mathbf{C}$.

Seja T o subanel de Q gerado sobre $\mathbf{C}_{d^\star}$ por $q_1, \cdots, q_{n-1}$, onde os q_i são os coeficientes do polinômio mônico $g(t)$ definido no lema 3.2.3 (pelo corolário 3.2.7, $q_0 = 0$, $d^\star(q_i) = 0$ e $[q_i, q_j] = 0$ para todo $0 \leq i \leq j \leq n-1$). Como estes q_i comutam entre si e com os elementos de $\mathbf{C}_{d^\star}$, segue que $T = \mathbf{C}_{d^\star}[q_1, \cdots, q_{n-1}]$ é um subanel comutativo de Q.

Seja E o subanel de Q gerado por T e R. Tomemos $d' \doteq d^\star|_E$. Note que $d^\star$ se restringe bem a E, pois d' leva R em R e T em zero. Se considerarmos $End(E, +)$ como um T-módulo à direita ($t \cdot r = tr \in E$, $t \in T$, $r \in R$), então T está contido em $End(E, +)$.

Definamos por M o T-submódulo de $End(E, +)$ gerado por $\{1, d', d'^2, \cdots\}$. Utilizando o corolário 3.2.7 ítens (i), (iv) e (ii), chegamos a $\sum_{i=1}^{n} d'^i(x)q_i = 0$ para todo $x \in E$.

De fato, o resultado vale para todo $x \in R$, pois $g(d)(R) = 0$. Pelo lema 3.2.3, segue válido para todo $\mathbf{x} \in \mathbf{Q}$. Pela definição de $\mathbf{C}_{d^\star}$, continua valendo para $\mathbf{x} \in \mathbf{C_{d^\star}}$. Portanto, vale para todo elemento de $T = \mathbf{C}_{d^\star}[q_1, \cdots, q_{n-1}]$.

Note que d é T-linear. Então para qualquer $j = 0,\ 1,\ \cdots,\ n-1$ temos $d(q_j r) = q_j d(r)$ com $q_j \in \mathbf{Q}$, $r \in R$. Fixemos $j \in \{0, 1, \cdots, n-1\}$ e seja $r \in R$. Pela T-linearidade de d e pelo corolário 3.2.7 item (i), segue que

$$\sum_{i=1}^{n} d'^i(q_j r)q_i = \sum_{i=1}^{n} q_j d'^i(r)q_i = q_j \sum_{i=1}^{n} d'^i(r)q_i = 0.$$

Pelo item (iv) do mesmo corolário e lembrando que q_j é central, temos

$$\sum_{i=1}^{n} d'^i(rq_j)q_i = \left(\sum_{i=1}^{n} d'^i(r)q_i\right) q_j = 0.$$

O mesmo raciocínio vale para $x = q_j r q_k$.

Vejamos o que acontece com os elementos de E do tipo $x = rq_j r'$, com r e $r' \in R$. Pelo corolário 3.2.7 (ii), concluimos que

$$q_j r = \sum_{i=j+1}^{n} \left(d^{i-j}(r)q_i\binom{i}{j} + rq_j\right).$$

Por este motivo, dado $q_i r \in E$ existem r_s, q_{j_s} tais que $q_i r = \sum_s r_s q_{j_s}$. Logo E é gerado por produtos da forma rq_j. Então $rq_j r' = \sum_s (u)q_{j_r} = u'q_l$, onde u, $u' \in R$. Portanto, $\sum_{i=1}^{n} d'^i(x)q_i = 0$ para todo $x \in E$.

Uma vez feito isto, podemos concluir que M é, portanto, um T-módulo finitamente gerado por $\{1, d', d'^2, \cdots, d'^{n-1}\}$. Sendo T um subanel finitamente gerado sobre um corpo, T é noetheriano. Por conseguinte, M é noetheriano.

Chamando $\delta' = \sum_{i=0}^{m} (d')^{p^i} c_i$ e considerando os T-submódulos de M gerados por

$$\{\delta'\} \subseteq \{\delta', \delta'^2\} \subseteq \{\delta', \delta'^2, \delta'^3\} \subseteq \ \ldots\ ,$$

obtemos uma cadeia ascendente de T-submódulos de M. Logo, tal cadeia é estacionária. Concluimos que δ' é algébrica com coeficientes em T. Sendo assim, δ' é Q-algébrica sobre $E \supseteq R$.

Isto nos diz que a derivação interna induzida por b é Q-algébrica sobre R e o lema 3.2.9 afirma então que b é $\mathbf{C}$-algébrico. □

Teorema 3.2.13 *As seguintes afirmações são equivalentes:*
(i) $d^\star$ *é* R*-algébrica;*
(ii) $d^\star$ *é* Q*-algébrica;*
(iii) d *é* Q*-algébrica;*
(iv) d *é* R*-algébrica;*
(v) $d^\star$ *é* $\mathbf{C}$*-algébrica;*
(vi) d *é* $\mathbf{C}$*-algébrica.*

demonstração : As implicações $(v) \to (i) \to (iv)$, $(v) \to (vi)$ e $(vi) \to (iv)$ seguem do lema 3.2.9.

A implicação $(i) \to (ii) \to (iii)$ é imediata.

$(iii) \to (iv)$ Se d é Q-algébrica, então existe um polinômio $f(t) = \sum_{i=1}^{n} t^i q_i \in Q[t]$ tal que $f(d) = 0$. Pelo lema 3.1.1 (ii), existe $(0) \neq \mathcal{I} \lhd R$ tal que $0 \neq q_i\mathcal{I} \subseteq R$. Tomando $\alpha \in \mathcal{I}$ tal que, para algum i, $0 \neq q_i\alpha \in R$, temos $\sum_{i=0}^{n} d^i(x)(q_i\alpha) = 0$ para todo $x \in R$. Logo d é R-algébrica.

Para provar o teorema, é suficiente agora mostrar que $(iv) \to (v)$.

$(iv) \to (v)$ Se a característica de $R > n =$ grau de d sobre R, então o teorema 3.2.10 nos fornece o resultado.

Caso característica de $R = p \leq n = grau\ d$, o lema 3.2.12 mostra que para todo $x \in Q$, $\delta(x) = \sum_{i=0}^{m} d^{\star^{p^i}}(x)c_i = bx - xb$, onde b é um elemento algébrico de Q e $c_i \in \mathbf{C}_{d^\star}$. O lema 3.2.9 mostra que $\delta = \sum_{i=0}^{m} d^{\star^{p^i}} c_i$ é uma derivação $\mathbf{C}$-algébrica. Utilizando o fato de que os c_i pertencem a $\mathbf{C}_{d^\star}$, obtemos assim uma equação para $d^\star$ com coeficientes em $\mathbf{C}$. □

Observemos ainda que o polinômio minimal para d com coeficientes em $\mathbf{C}$ pode ser suposto mônico e que, como no corolário 3.2.7 (i), os coeficientes deste polinômio estão na realidade em $\mathbf{C}_{d^\star}$.

Em [6], Chung e Luh mostraram que se $d^n(\mathcal{I}) = 0$ para um certo ideal não-nulo $\mathcal{I}$ de R, então $d^n(R) = 0$.

Podemos supor, sem perda de generalidade, que $d(\mathcal{I}) \subseteq \mathcal{I}$, como em [6]. De fato, se $d^n(\mathcal{I}) = 0$, então $\mathcal{J} = \mathcal{I} + d(\mathcal{I}) + d^2(\mathcal{I}) + \cdots + d^{n-1}(\mathcal{I})$ é um ideal bilátero não-nulo de R tal que $d^n(\mathcal{J}) = 0$ e $d(\mathcal{J}) \subseteq \mathcal{J}$. Logo, basta substituir $\mathcal{I}$ por $\mathcal{J}$.

Pode-se verificar que o polinômio mônico minimal para $d|_{\mathcal{I}}$ com coeficientes em $\mathbf{C}$ é na realidade um polinômio com coeficientes em $\mathbf{C}_{d^\star}$ e que se d é nilpotente sobre $\mathcal{I}$ de índice n, então t^n é um polinômio minimal para d sobre $\mathcal{I}$ com coeficientes em $\mathbf{C}$. O teorema de Chung e Luh pode, portanto, se exprimir dizendo que se t^n é um polinômio minimal com coeficientes em $\mathbf{C}$ para $d\,|_{\mathcal{I}}$, então t^n é minimal com coeficientes em $\mathbf{C}$ para d.

O teorema seguinte generaliza este resultado.

Teorema 3.2.14 *Se d é uma derivação $\mathbf{C}$-algébrica (respectivamente R- algébrica) sobre um ideal não-nulo $\mathcal{I}$ de R, então d é $\mathbf{C}$-algébrica (respectivamente R-algébrica) sobre R e satisfaz o mesmo polinômio minimal com coeficientes em $\mathbf{C}$ (respectivamente R) que $d\,|_{\mathcal{I}}$.*

demonstração : Para provar o teorema, é suficiente mostrar que se h é um polinômio com coeficientes em Q tal que $h(d)(\mathcal{I}) = 0$, então $h(d)(R) = 0$.

Suponhamos que d seja R-algébrica sobre $\mathcal{I}$. Seja

$$f(t) = t^n r + t^{n-1} r_{n-1} + \ \ldots \ + r_0 \in R[t; d]$$

o polinômio minimal para $d\,|_{\mathcal{I}}$. Por R ser primo, existe $i \in \mathcal{I}$ tal que $ir \neq 0$ e

$$d^n(xi)r + d^{n-1}(xi)r_{n-1} + \ \ldots \ + xir_0 = 0 \text{ para todo } x \in R.$$

Logo, $d^n(x)ir + \sum_{j=0}^{n-1} d^j(x)a_j = 0$ para todo $x \in R$, onde $a_j \in R$. Como $ir \neq 0$, d é R-algébrica de grau n.

Pelo lema 3.2.3, d satisfaz um polinômio mônico $g(t) \in Q[t; d^\star]$ de grau n. Dividindo $h(t)$ por $g(t)$ à direita em $Q[t; d^\star]$, obtemos $h(t) = p(t)g(t) + r(t)$, com $\partial r(t) < n$. O que mostra que $p(d^\star)\,(g(d^\star)(x)) + r(d^\star)(x) = h\,((d^\star)(x)) = 0$ para todo $x \in \mathcal{I}$. Logo $r(d^\star)(\mathcal{I}) = 0$ e $\partial r(t) < n$.

Sendo n o grau de d sobre $\mathcal{I}$, temos que $r(t) = 0$, donde $h(t) = p(t)g(t)$. Deduzimos então que $h(d^\star) = p(g(d^\star))$ e para todo $x \in R$, $h(d^\star)(x) = p(d)(g(d)(x)) = 0$, ou seja, $h(d)(R) = 0$. □

Encerraremos este capítulo com uma observação suplementar concernente às derivações nilpotentes. Sendo R primo, é fácil verificar que se $d \cdot r = 0$ para um certo elemento não-nulo r de R, então $d = 0$. De fato, para quaisquer x, $y \in R$,

$$0 = d(xy)r = d(x)yr + xd(y)r = d(x)yr.$$

Como $r \neq 0$ e $d(x)yr = 0$ para todo $y \in R$, segue que $d(x) = 0$ para todo $x \in R$, donde $d = 0$.

Ademais, uma indução fácil (e que já vimos anteriormente) mostra que se d é uma derivação interna definida por um elemento $a \in R$, então $d^n = \sum_{i=0}^{n}(-1)^i\binom{n}{i}a^{n-i}xa^i$, para todo $n \in \mathbf{N}$. Nestas condições, se a for um elemento nilpotente de índice n, d satisfaz $d^{2n-1} = 0$ e $d^n a^{n-1} = 0$. Mais geralmente, temos a

Proposição 3.2.15 *Seja $r \in R \setminus \{0\}$ tal que $d^n \cdot r = 0$. Então $d^{2n-1} = 0$.*

prova : Para todo x, $y \in R$, pela proposição 0.3.2,

$$(2) \qquad 0 = d^n(xy)r = \sum_{i=0}^{n}\binom{n}{i}d^i(x)d^{n-i}(y)r = \sum_{i=0}^{n}\binom{n}{i}d^{n-i}(x)d^i(y)r.$$

Mostraremos, por indução que, para todo $k \in \{0, 1, \ \ldots \ , n-1, n\}$,

$$(3) \qquad d^{n+k-1}(x)d^{n-k}(y)r = 0 \ \text{ para todo } \ x, y \in R.$$

Se $k = 0$, então $d^{n-1}(x)d^n(y)r = 0$, pois $d^n \cdot r = 0$.

Suponhamos agora $k < n$ e $d^{n+l-1}(x)d^{n-l}(y)r = 0$ para todo x, $y \in R$ e qualquer $l \leq k$. Substituindo x e y, respectivamente, por $d^k(x)$ e $d^{n-(k+1)}(y)$ em (2), obtemos:

$$0 = \sum_{i=0}^{n}\binom{n}{i}d^{n-i}\left(d^k(x)\right)d^i\left(d^{n-(k+1)}(y)\right)r = \sum_{i=0}^{n}\binom{n}{i}d^{n+k-i}(x)d^{n+i-(k+1)}(y)r =$$

$$= \sum_{i=0}^{k+1}\binom{n}{i}d^{n+k-i}(x)d^{n+i-(k+1)}(y)r + \sum_{i=k+2}^{n}\binom{n}{i}d^{n+k-i}(x)d^{n+i-(k+1)}(y)r =$$

$$= \sum_{i=0}^{k+1}\binom{n}{i}d^{n+k-i}(x)d^{n+i-(k+1)}(y)r.$$

A hipótese de indução nos permite concluir que

$$0 = d^{n+(k+1)-1}(x)d^{n-(k+1)}(y)r, \ \text{ o que prova } (3).$$

Em particular, para $k = n$, a expressão (3) se escreve como $d^{2n-1}(x)yr = 0$ para todo $y \in R$. Por ser R primo e $r \neq 0$, segue que $d^{2n-1}(x) = 0$ para todo $x \in R$. Logo, $d^{2n-1} = 0$. $\square$

Capítulo 4

Bibliografia

Bibliografia

[1] S. A. AMITSUR, "Derivations in simple rings", Proc. London Math. Soc. (3)7 (1957), pp. 87–112

[2] M. F. ATIYAH, I. G. MACDONALD, "Introduction to commutative algebra", Reading, Addison-Wesley, 1969

[3] N. BOURBAKI, " Élements de mathématique", Algèbre, Structures Algébriques, Algèbre Lineaire, chapitres 1 et 2, Herman, editeurs des sciences et des arts à Paris, 1970

[4] M. BRESĂR, J. VUKMAN, "Jordan derivations on prime rings", Bull. Austral. Math. Soc., vol. 37 (1988), pp. 321–322

[5] M. BRESĂR, "Jordan derivations on semiprime rings", Proc. Amer. Math. Soc., vol. 104, n. 4 (1988), pp. 1003–1006

[6] L. O. CHUNG, J. LUH, "Nilpotency of derivations on an ideal", Proc. American Math. Soc., vol. 90, n. 2 (1984), pp. 211–214

[7] F. DUMAS, R. VIDAL, "Dérivations, et hautes dérivations, dans certains corps gauches de series de Laurent", Pacific Journal of Mathematics, vol. 153, n. 2 (1992), pp. 277–280

[8] I. N .HERSTEIN, "Jordan derivations of prime rings", Proc. Amer. Math. Soc., 8 (1957), pp. 1104–1110

[9] _____, "Topics in Algebra", Waltham, Blaisdell, 1964

[10] _____, "Topics in ring theory", Chicago Lectures in Mathematics, 1969

[11] _____, "Rings with involutions", The University of Chicago Press, 1976

[12] A. JONES, "Notas de álgebra", São Paulo, IME-USP, 1979

[13] V. K. KARCHENKO, "Differential identities of prime rings", Algebra i Logika, vol 17, n. 2(1978), pp. 220–238 = Algebra and Logic 17(1978), pp. 155–168

[14] J. KREMPA, J. MATCZUK, "On algebraic derivations of prime rings", Methods in Ring Theory *edited by F.Van Oystaeyen*, 1984, pp. 211–229

[15] J. LAMBEK, "Lectures on rings and modules, N.York, Chelsea, 1976

[16] A. LEROY, J. MATCZUK, "Derivations et automorphismes algebriques d'anneux premiers", Communications in Algebra, 13(6) (1985), pp. 1245–1266

[17] W. MARTINDALE, "Prime rings satysfying a generalized polynomial identity", Journal of Algebra, 12 (1969), pp. 576–584

[18] N. H. McCOY, "the theory of rings", N. York, Macmillan, 1969

[19] A. NOWICKI, "Inner derivations of higher orders", Tsukuba J. Math., vol. 8, n. 2 (1984), pp. 219–225

[20] A. A. SANT'ANA, "Ideais primos e fechados em extensões de anéis", Universidade Federal do Rio Grande do Sul, *dissertação orientada por M.FERRERO*, Porto Alegre, 1992

Capítulo 5

Índice Remissivo

Índice Remissivo

Terminologia

Notações