DERIVAÇÕES
EM
ANÉIS NÃO COMUTATIVOS

Deborah Martins Raphael

DISSERTAÇÃO APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO

PARA OBTENÇÃO DO GRAU DE MESTRE
EM
MATEMÁTICA

ÁREA DE CONCENTRAÇÃO: ÁLGEBRA

ORIENTADOR:
Prof. Dr. Francisco César Polcino Milies

- SÃO PAULO, NOVEMBRO DE 1985 -

A meus pais:
Thereza e Zadok.

PREFÁCIO

As derivações fornecem uma ferramenta que pode ser usada para abordar problemas em Teoria de Anéis. Neste trabalho, apresentamos alguns resultados bastante recentes que nos dão uma idéia de como, estudando as derivações em um anel não comutativo, podemos deduzir propriedades intrínsecas do anel.

No capítulo 0, listamos alguns resultados que serão utilizados ao longo deste trabalho, introduzimos a definição de derivação, citando alguns exemplos e dando dois resultados importantes.

No capítulo I, estudamos a imagem e compostas de derivações. Os resultados aqui apresentados foram introduzidos por I.N.Hersteins e generalizados por J.Bergen. A idéia é mostrar que a imagem de uma derivação é "grande o suficiente" para permitir obter informações sobre o anel.

Os capítulos 2, 3 e 4 abordam o caso de uma derivação cujos valores são, de alguma forma, especiais.

No capítulo 2, relacionamos nilpotência e derivações. Numa primeira parte, apresentamos um resultado de B.Felzenswalb e A.Giambruno que caracteriza um anel primo R , sem ideais nil não nulos, que tem uma derivação d , tal que $d(x^{n(x)})=0$ para todo elemento x de R . Conclui-se, neste caso, que R é um domínio comutativo infinito de característica $p>0$. Em seguida, apresentamos uma prova de que um trabalho anterior de B.Felzenswalb é, na verdade, uma consequência do resultado acima. Numa segunda parte, demonstra

mos o seguinte resultado de B.Felzenszwalb e C.Lanski: se um anel R sem ideais à direita nil não nulos tem uma derivação que é nil em um ideal não nulo I de R , então $d(I)=0$. Este é o resultado central do capítulo 2 e uma introdução ao problema que é abordado no capítulo seguinte.

O capítulo 3 pode ser considerado a parte central do presente trabalho. Nele, estudamos um anel com uma derivação cujos valores, elevados a alguma potência, são centrais. Esta é uma introdução natural ao estudo de derivações cujos valores são algébricos sobre o centro do anel. Apresentamos uma nova demonstração de dois resultados - um de I.N.Herstein e outro de C.Lanski - que permite enunciar-los de forma mais geral. Em ambos os trabalhos, procura-se concluir que um anel com uma derivação, com a propriedade acima, é uma ordem numa álgebra simples de dimensão no máximo 4 sobre seu centro. Herstein conclui que este é o caso se o anel é primo e os valores da derivação elevados a uma potência fixada são centrais. Lanski, por sua vez, conclui o mesmo no caso em que o anel é primo, sem ideal à direita nil não nulo e com centro não enumerável. Nossa generalização permite supormos apenas que R é semiprimo no resultado de Herstein (contando que os valores da derivação sejam regulares ou nulos) e mostra que a hipótese de R ser primo no teorema de Lanski é supérflua. Conseguimos também provar um resultado que, até onde sabemos, não havia sido demonstrado: o teorema de Lanski vale para todo anel de característica $p>0$, sem ideais à direita nil, sem restrição sobre a cardinalidade do centro.

No capítulo 4 apresentamos um trabalho de J. Bergen, I.N.Herstein e C.Lanski que estuda um anel com uma

derivação cujos valores são nulos ou inversíveis. A hipótese é restritiva, mas a classificação é completa: o anel é D ou $M_2(D)$ ou $D[X]/(X^2)$ onde D é um anel com divisão; se for $D[X]/(X^2)$ então $\text{car} D = 2$. Retomamos, ainda, dois resultados do capítulo anterior, que podem ter interesse independente. Um deles, provamos ser uma generalização de um resultado de Bergen; o outro é o instrumento que nos permitiu generalizar os teoremas de Herstein e Lanski apresentados no capítulo 3.

Gostaria de agradecer a todas as pessoas que colaboraram na realização deste trabalho; em particular, ao Prof. Dr. Francisco César Polcino Milies pela sugestão do tema e pela dedicada orientação, e à Profa. Dra. Sônia Pitta Coelho pela paciência e interesse com que acompanhou boa parte deste trabalho.

Quero agradecer especialmente à Profa. Heloísa Daruiz Borsari e ao Prof. Dr. Francisco Miraglia pelas sugestões e pela paciência e incentivos constantes.

À Nadia Vicentini e Aparecida Conceta Pompeu T. de Souza, agradeço o rápido e eficiente trabalho de datilografia.

Finalmente, um abraço e um beijo a meus colegas do IME, amigos de tanto tempo: Jacques, Jorge, Chico Mi, Helô, Lindito, Toninho, Daci, Bel, Lucinha, Cris, Zara, Ana Cá, Saulo, Angela, Guilherme, Lucília, Baixinho, Inês, Walter, Salvitti, Bianconi, Pê Boulos, Sussu, Iole, Panza, Carrião, Cordaro, Zé Carlos, Bete, Maria Angela e Rosinha.

ÍNDICE

PREFÁCIO	iii
NOTAÇÃO	vii
CAPÍTULO 0	01
CAPÍTULO I	24
CAPÍTULO II	72
CAPÍTULO III	109
CAPÍTULO IV	173
BIBLIOGRAFIA	210

NOTAÇÃO

Dado R um anel, usaremos a seguinte convenção:

- $Z(R)$ é o centro de R ;
- $J(R)$ é o ideal de Jacobson de R ;
- $N(R)$ é a soma dos ideais nil de R ;
- R_Z é o localizado de R em $Z(R)^*$.

Se $A \subset R$ então:

- $C_R(A)$ é o centralizador de A em R ;
- $Anl_e(A)$ é o anulador à esquerda de A em R ;
- $Anl_d(A)$ é o anulador à direita de A em R .

Se I e J são ideais de R , frequentemente usaremos a expressão "ideal IJ " nos referindo ao ideal gerado por IJ (isto é, o subgrupo aditivo gerado por IJ). Com o mesmo espírito, se $A \subset R$, diremos "ideal à esquerda IA " e "ideal à direita AI ".

CAPÍTULO 0

Apresentamos neste capítulo alguns resultados de Teoria de Anéis que utilizaremos neste trabalho. Nos limitaremos a enunciar aqui aqueles que não são facilmente encontrados na bibliografia. De resto, os conceitos e resultados de Teoria de Anéis que serão requisitados ao longo deste trabalho encontram-se, na sua maioria, em [H.6].

Também introduziremos, neste capítulo, a noção de derivação em um anel, que é nosso objeto de estudo. Mostraremos algumas propriedades básicas que decorrem imediatamente da definição e alguns exemplos elucidativos. Apresentaremos, em seguida, dois resultados interessantes, um dos quais usaremos ao longo deste trabalho.

Iniciamos, portanto, com os seguintes resultados:

0.1 - TEOREMA. Sejam R um anel primo e $L \neq 0$ um ideal lateral de R . São verdadeiras as seguintes afirmações:

(i) os elementos não nulos de $Z(R)$ são regulares.

(ii) $C_R(L) = Z(R)$.

(iii) se $L \subset Z(R)$ então R é comutativo.

(iv) se $\text{car} R \neq 2$ então R é livre de 2-torção.

As demonstrações dos vários itens do teorema acima se encontram em: [H.6], lema 2.1.2; [H.8], lema 1.1.5 e corolário; [H.8], lema 1.1.6.

0.2 - TEOREMA. Sejam R um anel semiprimo e $I \neq 0$ um ideal de R . São verdadeiras as seguintes afirmações:

(i) se $z \in Z(R)^*$ então z não é nilpotente.

(ii) $\text{Anl}_e(I) = \text{Anl}_d(I)$ e $\text{Anl}_e(I) \cap I = 0$.

A demonstração do item (i) do teorema acima decorre imediatamente da definição de anel semiprimo. A demonstração de (ii) encontra-se em [H.8], lema 1.1.3 e corolário.

0.3 - TEOREMA. Seja R um anel tal que $N(R) = 0$. Então R é produto subdireto de anéis primos R/P_i com $N(R/P_i) = 0$.

A demonstração deste teorema é feita em [H.6], lema 2.2.3. Na verdade, em [H.6], não é demonstrado que $N(R/P_i) = 0$; basta, no entanto, observar a definição dos P_i para se verificar que isto ocorre.

0.4 - TEOREMA DA DENSIDADE (JACOBSON E CHEVALLEY). Sejam R um anel primitivo e V um R -módulo irredutível e fiel. Então $D = \text{Hom}_R(V, V)$ é um anel com divisão e R é denso em $\text{Hom}_D(V, V)$. Além disto, se $\dim_D V = n$ (n um inteiro positivo) então R é isomorfo à $M_n(D)$ e, se $\dim_D V = +\infty$ então para todo inteiro positivo m , existe um subanel S_m de R e um epimorfismo de S_m

em $M_m(D)$.

Este teorema e sua demonstração são resultados bastante conhecidos que se encontram por exemplo em [H.6] ou [J.1]. Queremos ressaltar aqui o seguinte corolário:

0.5 - COROLÁRIO. Sejam R um anel primitivo, $I \neq 0$ um ideal de R e V um R -módulo irredutível e fiel. Então I , considerado como anel, é primitivo; V é um I -módulo irredutível e fiel e I é denso em $\text{Hom}_D(V, V)$ onde $D = \text{Hom}_R(V, V) = \text{Hom}_I(V, V)$ é um anel com divisão.

A demonstração pode ser encontrada em [J.1], página 33, teorema 4.

Veremos agora um famoso resultado de Levitzki que será constantemente utilizado ao longo deste trabalho.

0.6 - TEOREMA (LEVITZKI). Sejam R um anel e $L \neq 0$ um ideal lateral de R . Se existe um inteiro $n > 0$ tal que $a^n = 0$ qualquer que seja $a \in L$, então R tem ideal nilpotente não nulo.

A demonstração do resultado acima encontra-se em [H.9], lema 1.1.

Outro resultado relacionado com o que acabamos de mencionar, é demonstrado por B. Felzenswalb em [F.1].

0.7 - TEOREMA (FELZENSWALB). Sejam R um anel sem ideais à direita nil não nulos e K um ideal à direita de R . Suponhamos que $a \in R$ seja tal que para todo $x \in K$ existe $n(x)$ um inteiro positivo com $x^{n(x)}a=0$; então $Ka=0$.

O seguinte resultado fornece uma condição suficiente para que um anel sem ideais nil não nulos seja comutativo.

0.8 - TEOREMA (KAPLANSKY). Seja R um anel sem ideais nil não nulos e suponhamos que para todo $x \in R$, exista um inteiro positivo $n(x)$ tal que $x^{n(x)} \in Z(R)$. Então R é comutativo.

A demonstração do teorema acima encontra-se em [H.6], teorema 3.2.2.

A definição de centróide estendido de um anel, encontra-se em [H.8], página 22. O que usaremos neste trabalho é um resultado de Martindale, que é um lema utilizado na demonstração do teorema 1.3.1 de [H.8].

0.9 - LEMA (MARTINDALE). Sejam R um anel primo, a_i e $b_i \in R$, $1 \leq i \leq n$ tais que

$$\sum_{i=1}^n a_i x b_i = 0$$

para todo $x \in R$. Então $\{a_i\}_{1 \leq i \leq n}$ é linearmente dependente sobre C , o centróide estendido de R , e $\{b_i\}_{1 \leq i \leq n}$ é linearmente dependente sobre C .

A demonstraçãõ deste resultado encontra-se em [H.8], lema 1.3.2.

O próximo resultado nos fornece um instrumento que se mostra útil para contornar a conjectura de Köethe quando ela aparece em problemas envolvendo anéis primos.

O.10 - TEOREMA (HERSTEIN). Sejam R um anel primo e $M(R)$ a união dos ideais à direita nil de R . Suponhamos que $M(R) \neq 0$. Se A é um subanel de R tal que $(1+x)A(1+x)^{-1} \subset A$ para todo $x \in M(R)$ então, ou $A \subset Z(R)$, ou A contém um ideal não nulo de R .

A demonstraçãõ deste teorema encontra-se em [H.5].

Iniciamos aqui a segunda parte deste capítulo in troduzindo a definiçãõ de uma derivaçãõ em um anel.

O.11 - DEFINIÇÃÕ. Seja R um anel. Uma funçãõ $d: R \rightarrow R$ é uma derivaçãõ em R se para quaisquer x e $y \in R$ temos:

$$d(x+y) = d(x) + d(y) \quad \text{e} \quad d(xy) = d(x)y + xd(y).$$

Algumas propriedades decorrem imeditamente da definiçãõ acima. Reunimos estes resultados na seguinte observaçãõ:

0.12 - OBSERVAÇÃO. Sejam R um anel e d uma derivação em R . São verdadeiras as seguintes afirmações:

$$(i) \quad d(0)=0.$$

(ii) se R tem unidade, então $d(1)=0$ e $d(n)=0$ para todo inteiro n .

$$(iii) \quad d(Z(R)) \subset Z(R).$$

(iv) se $x \in R$ tem inverso x^{-1} então $d(x^{-1}) = -x^{-1}d(x)x^{-1}$.

DEMONSTRAÇÃO. (i) $d(0)=d(0+0)=d(0)+d(0)$ implica $d(0)=0$.

(ii) $d(1)=d(1 \cdot 1)=1d(1)+d(1) \cdot 1=2d(1)$ implica $d(1)=0$. O fato de que $d(n)=0$ é facilmente provado por indução.

(iii) se $z \in Z(R)$ e $x \in R$ então $xz-zx=0$. Consequentemente,

$$0=d(xz-zx)=d(x)z+xd(z)-d(z)x-zd(x)=xd(z)-d(z)x$$

e concluimos que $d(z) \in Z(R)$.

(iv) Decorre imediatamente da seguinte igualdade:

$$0=d(1)=d(xx^{-1})=d(x)x^{-1}+xd(x^{-1}).$$

//

Uma pergunta que surge naturalmente é se $D = \{d: R \rightarrow R \mid d \text{ é uma derivação}\}$ tem alguma estrutura conhecida. Serão derivações a soma de duas derivações ou a composta de duas derivações? Será uma derivação o produto de uma derivação por um elemento do anel?

Em geral a resposta a estas perguntas é não. Nem sempre a composta de duas derivações é uma derivação (veremos, no capítulo 1, que em anéis primos, isto raramente ocorre); também o produto de uma derivação por um elemento do anel nem sempre é uma derivação.

A seguinte observação mostra alguns resultados positivos neste sentido, isto é, dadas duas derivações, que operações podemos efetuar para obter outra derivação?

0.13 - OBSERVAÇÃO. Sejam d_1 e d_2 duas derivações num anel R e $z \in Z(R)$. Então:

(i) $d: R \rightarrow R$ definida por $d(x) = d_1(x) + d_2(x)$ para todo $x \in R$ é uma derivação em R .

(ii) $d: R \rightarrow R$ definida por $d(x) = zd_1(x)$ para todo $x \in R$ é uma derivação em R .

(iii) $d: R \rightarrow R$ definida por $d(x) = (d_1 \circ d_2)(x) - (d_2 \circ d_1)(x)$ para todo $x \in R$ é uma derivação.

DEMONSTRAÇÃO. (i) Dados x e $y \in R$ temos:

$$d(x+y) = d_1(x+y) + d_2(x+y) = d_1(x) + d_2(x) + d_1(y) + d_2(y) = d(x) + d(y).$$

e,

$$\begin{aligned} d(xy) &= d_1(xy) + d_2(xy) = (d_1(x) + d_2(x))y + x(d_1(y) + d_2(y)) = \\ &= d(x)y + xd(y). \end{aligned}$$

Logo, d é uma derivação em R .

(ii) Dados x e $y \in R$ temos:

$$d(x+y) = zd_1(x+y) = zd_1(x) + zd_1(y) = d(x) + d(y)$$

e,

$$\begin{aligned} d(xy) &= zd_1(xy) = zd_1(x)y + xzd_1(y) = zd_1(x)y + xzd_1(y) = \\ &= d(x)y + xd(y). \end{aligned}$$

Concluimos, portanto, que d é uma derivação em R .

(iii) Sejam x e $y \in R$. Então temos:

$$\begin{aligned} d(x+y) &= (d_1 \circ d_2)(x+y) - (d_2 \circ d_1)(x+y) = d_1(d_2(x) + d_2(y)) - \\ &\quad - d_2(d_1(x) + d_1(y)) = \\ &= (d_1 \circ d_2)(x) + (d_1 \circ d_2)(y) - (d_2 \circ d_1)(x) - (d_2 \circ d_1)(y) = d(x) + d(y). \end{aligned}$$

Ainda,

$$\begin{aligned}
 d(xy) &= (d_1 \circ d_2)(xy) - (d_2 \circ d_1)(xy) = d_1(d_2(x)y + xd_2(y)) - \\
 &\quad - d_2(d_1(x)y + xd_1(y)) = (d_1 \circ d_2)(x)y + d_2(x)d_1(y) + \\
 &\quad + d_1(x)d_2(y) + x(d_1 \circ d_2)(y) - (d_1 \circ d_2)(x)y - d_1(x)d_2(y) - \\
 &\quad - d_2(x)d_1(y) - x(d_2 \circ d_1)(y) = (d_1 \circ d_2)(x)y - (d_2 \circ d_1)(x)y + \\
 &\quad + x(d_1 \circ d_2)(y) - x(d_2 \circ d_1)(y) = d(x)y + xd(y).
 \end{aligned}$$

Provamos, portanto, que d é uma derivação em R .

//

Podemos também nos perguntar se uma derivação num anel R induz uma derivação no quociente R/I onde I é um ideal de R . A resposta a esta pergunta é dada na seguinte observação:

0.14 - OBSERVAÇÃO. Sejam R um anel, I um ideal de R e d uma derivação em R tal que $d(I) \subset I$. Então d induz uma derivação $\bar{d}$ em $\bar{R} = R/I$ dada por:

$$\bar{d}(\bar{x}) = \overline{d(x)} \quad \forall x \in R$$

DEMONSTRAÇÃO. Basta verificarmos que $\bar{d}$ está bem definida, pois é óbvio que se for este o caso, então $\bar{d}$ é uma derivação. Ora, se $\bar{r}$ e $\bar{s} \in \bar{R}$ são tais que $\bar{r} = \bar{s}$ então $r - s \in I$ e, como $d(I) \subset I$, temos: $d(r - s) = d(r) - d(s) \in I$, o que implica

$\overline{d(r)} = \overline{d(s)}$. Então:

$$\overline{d(\overline{r})} = \overline{d(r)} = \overline{d(s)} = \overline{d(\overline{s})};$$

e concluímos que $\overline{d}$ está bem definida.

//

Também no caso em que R é um anel primo e d é uma derivação em R , podemos estender d à uma derivação em R_Z , o localizado de R em $Z(R)^*$. É o que mostra a seguinte observação:

0.15 - OBSERVAÇÃO. Sejam R um anel primo e d uma derivação em R . Se R_Z é o localizado de R em $Z(R)^*$ então existe D uma derivação em R_Z tal que $D(r) = d(r)$ para todo $r \in R$.

DEMONSTRAÇÃO. Dado $rz^{-1} \in R_Z$ com $r \in R$ e $z \in Z(R)^*$, definimos

$$D(rz^{-1}) = d(r)z^{-1} - rd(z)z^{-2}$$

Primeiramente vamos mostrar que D está bem definida. Sejam rz^{-1} e $sw^{-1} \in R_Z$ tais que $rz^{-1} = sw^{-1}$. Então temos que

$$rw = sz$$

e concluímos que:

$$d(r)w + rd(w) = d(s)z + sd(z). \quad (1)$$

Mas,

$$D(rz^{-1})w^2 = d(r)z^{-1}w^2 - rd(z)z^{-2}w^2.$$

Lembrando que $d(Z(R)) \subset Z(R)$, temos:

$$\begin{aligned} D(rz^{-1})w^2 &= d(r)z^{-1}w^2 - (rw)d(z)z^{-2}w = \\ &= d(r)z^{-1}w^2 - (sz)d(z)z^{-2}w = d(r)z^{-1}w^2 - \\ &\quad - sd(z)z^{-1}w = \\ &= (d(r)w - sd(z))z^{-1}w. \end{aligned} \quad (2)$$

Portanto, de (1) e (2), concluímos que:

$$\begin{aligned} D(rz^{-1})w^2 &= (d(s)z - rd(w))z^{-1}w = d(s)w - (rw)d(w)z^{-1} \\ &= d(s)w - szd(w)z^{-1} = d(s)w - sd(w). \end{aligned} \quad (3)$$

Finalmente, de (3), temos:

$$D(rz^{-1}) = (d(s)w - sd(w))w^{-2} = D(sw^{-1}),$$

e provamos que D está bem definida.

Vamos mostrar agora que D é uma derivação em R_Z . Aqui também usaremos com frequência o fato de que $d(Z(R)) \subset Z(R)$.

Dados rz^{-1} e $sw^{-1} \in R_Z$, temos:

$$\begin{aligned}
D(rz^{-1}+sw^{-1}) &= D((rw+sz)z^{-1}w^{-1}) = d(rw+sz)z^{-1}w^{-1} - \\
&\quad - (rw+sz)d(zw)(zw)^{-2} = \\
&= d(r)z^{-1} + rd(w)z^{-1}w^{-1} + d(s)w^{-1} + sd(z)z^{-1}w^{-1} \\
&\quad - rd(z)z^{-2} - rd(w)z^{-1}w^{-1} - sd(z)z^{-1}w^{-1} - \\
&\quad - sd(w)w^{-2} = D(rz^{-1}) + D(sw^{-1}).
\end{aligned}$$

Ainda,

$$\begin{aligned}
D(rz^{-1}sw^{-1}) &= D(rs z^{-1}w^{-1}) = d(rs)z^{-1}w^{-1} - rsd(zw)(zw)^{-2} = \\
&= (d(r)s + rd(s))(zw)^{-1} - rs(d(z)w + zd(w))(zw)^{-2} = \\
&= d(r)sz^{-1}w^{-1} - rsd(z)w(zw)^{-2} + rd(s)(zw)^{-1} \\
&\quad - rszd(w)(zw)^{-2} = \\
&= (d(r)z^{-1} - rd(z)z^{-2})sw^{-1} + rz^{-1}(d(s)w^{-1} - sd(w)w^{-2}) = \\
&= D(rz^{-1})sw^{-1} + rz^{-1}D(sw^{-1}).
\end{aligned}$$

Provamos, portanto, que D é uma derivação em R_Z .

É claro que se $r \in R$, então:

$$D(r) = D(rzz^{-1}) = d(rz)z^{-1} - rz d(z)z^{-2} = d(r)zz^{-1} = d(r)$$

e está provada a observação.

//

Vamos agora ver alguns exemplos de derivações. Em primeiro lugar definiremos uma derivação interna.

0.16 - DEFINIÇÃO. Dados R um anel e $a \in R$ a derivação d em R dada por:

$$d(x) = ax - xa \quad \forall x \in R$$

é chamada derivação interna dada por a .

É claro que, num anel R não comutativo, para todo elemento $a \in R$, temos em R a derivação interna dada por a . Se $a \in Z(R)$ a derivação interna dada por a é a derivação nula. Outros exemplos de derivações são dados a seguir.

0.17 - EXEMPLOS. 1 - Seja R um anel qualquer; consideremos o anel de polinômios $R[x]$. Dado $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ pertencente a $R[x]$, definimos:

$$d(p(x)) = p'(x) = na_n x^{n-1} + (n-1)a_{n-1} x^{n-2} + \dots + 2a_2 x + a_1$$

Este é um exemplo, ao qual já estamos bastante habituados, de uma derivação que não é interna. Vamos nos referir a esta derivação como derivação usual no anel de polinômios.

2 - Ainda no anel de polinômios $R[x]$ é claro que se δ é uma derivação então $\delta(x) \in Z(R[x])$ (observação 0.12, (iii)). Recíprocamente, se $a \in Z(R[x])$, definimos

$$\delta: R[x] \rightarrow R[x]$$

da seguinte forma:

$$\delta(p(x)) = ap'(x) \quad \forall p(x) \in R[x],$$

onde $p'(x)$ é a derivada usual do polinômio $p(x)$. Pelo item (ii) da observação 0.13, sabemos que δ é uma derivação e é claro que $\delta(x) = a$.

3 - Se R é um anel e G um grupo, dada uma derivação d em R , podemos definir D uma derivação em RG que estende d . Basta definirmos D da seguinte forma:

$$D\left(\sum_{g \in G} \alpha_g \cdot g\right) = \sum_{g \in G} d(\alpha_g) \cdot g;$$

para todo $\alpha = \sum_{g \in G} \alpha_g \cdot g \in RG$. É fácil verificar que D é uma derivação em RG e que $D(r) = d(r)$ para todo $r \in R$.

4 - Dada uma derivação d em um anel R , podemos estender d à uma derivação D em $M_n(R)$, o anel das matrizes $n \times n$ sobre R . Basta definir D da seguinte forma:

$$D((a_{ij})_{1 \leq i, j \leq n}) = (d(a_{ij}))_{1 \leq i, j \leq n}$$

Também neste caso é imediata a verificação de que D é uma derivação em $M_n(R)$.

Neste trabalho estaremos interessados em derivações em anéis não comutativos. Vejamos, porém, um exemplo do caso comutativo.

0.18 - EXEMPLO. Consideremos o corpo dos números reais, $\mathbb{R}$. Vamos ver como é uma derivação em $\mathbb{R}$.

Suponhamos que d é uma derivação em $\mathbb{R}$. Então, pela observação 0.12, itens (ii) e (iv), é fácil ver que $d(\mathbb{Z}) = d(\mathbb{Q}) = 0$. Ainda, se $a \in \mathbb{R}$ é algébrico sobre $\mathbb{Q}$, e

$p = \text{irr}(a, \mathbb{Q}[X])$, então, como $d(a^k) = k a^{k-1} d(a)$, pelas regras de soma e produto da derivação, temos:

$$0 = d(p(a)) = p'(a) d(a)$$

onde p' é a derivada usual do polinômio p . Neste caso, pela escolha de p , sabemos que $p'(a) \neq 0$ e portanto $d(a) = 0$.

Em suma, mostramos que qualquer derivação em $\mathbb{R}$, se anula em $F = \overline{\mathbb{Q}} \cap \mathbb{R}$ onde $\overline{\mathbb{Q}}$ é o fecho algébrico de $\mathbb{Q}$.

Vamos agora mostrar uma maneira de se construir uma derivação em $\mathbb{R}$. Seja $B = \{b_\alpha\}$ uma base de transcendência de $F \subset \mathbb{R}$. Então temos a seguinte torre de corpos:

$$\mathbb{Q} \subset F \subset F(B) \subset \mathbb{R},$$

onde $\mathbb{R}/F(B)$ é uma extensão algébrica.

Para cada $b_\alpha \in B$ escolhemos um valor arbitrário em $F(B)$ e definimos $d(b_\alpha)$. Dado $\alpha \in F(B)$, α é da forma:

$$\alpha = \frac{p(b_{\alpha_1}, b_{\alpha_2}, \dots, b_{\alpha_n})}{q(b'_{\alpha_1}, b'_{\alpha_2}, \dots, b'_{\alpha_m})},$$

onde $p \in F[x_1, x_2, \dots, x_n]$, $q \in F[x_1, x_2, \dots, x_m]$ e, $b_{\alpha_i}, b'_{\alpha_j} \in B$
 $1 \leq i \leq n, 1 \leq j \leq m$.

Já sabemos que $d(F) = 0$. Definimos, então,

$$d(\alpha) = \frac{p(d(b_{\alpha_1}), d(b_{\alpha_2}), \dots, d(b_{\alpha_n}))}{q(d(b'_{\alpha_1}), d(b'_{\alpha_2}), \dots, d(b'_{\alpha_m}))}.$$

A verificação de que d está bem definida e é uma derivação em $F(B)$ é trivial (basta lembrar que B é algebricamente in dependente sobre F). Vamos agora estender d à uma derivação em R .

Dado $r \in R$, já sabemos que r é algébrico sobre $F(B)$. Seja $q = \text{irr}(r, F(B)[X])$. Os coeficientes de q pertencem a $F(B)$; denotaremos por dq o polinômio de $F(B)[x]$, obtido aplicando d nos coeficientes de q ; denotaremos por q' a derivada usual do polinômio q . Finalmente definimos:

$$d(r) = - \frac{(dq)(r)}{q'(r)}.$$

Pela escolha de q , sabemos que $q'(r) \neq 0$. A verificação de que a definição acima realmente estende d é imediata, bem como a demonstração de que d acima definida é uma derivação.

Pelo que acabamos de mostrar, dada B uma base de transcendência de $F = \bar{\mathbb{Q}} \cap R$ e uma função $f: B \rightarrow B$ qualquer, podemos estender f à uma derivação em R . Recíprocamente, aplicando as regras de derivação, temos que uma derivação d em R está determinada se conhecemos seus valores numa base de transcendência qualquer de F .

As demonstrações que omitimos neste último exemplo, bem como as noções introduzidas encontram-se em [L.S] (em particular página 267, teorema 7).

Não só a título de exemplo, mas também porque usaremos mais tarde, nos interessa em especial os resultados sobre derivações no anel de matrizes $n \times n$ com coeficientes num anel R com unidade, $M_n(R)$. No ítem 4 dos exemplos 0.17 mostramos uma derivação em $M_n(R)$ obtida a partir

de uma derivação em R . Em [PM], F.C. Polcino Milies mostra que as derivações que aparecem no exemplo 4 e as derivações internas em $M_n(R)$ nos dão todas as derivações de $M_n(R)$. É o seguinte, o teorema demonstrado em [P.M]:

0.19 - TEOREMA. Sejam R um anel com unidade e d uma derivação em $M_n(R)$. Então d é da forma:

$$d = d_A + \bar{\delta},$$

onde d_A é a derivação interna em $M_n(R)$ dada pela matriz $A \in M_n(R)$ e $\bar{\delta}$ é uma derivação em $M_n(R)$, induzida por uma derivação δ de R , isto é,

$$\bar{\delta}((x_{ij})_{1 \leq i, j \leq n}) = (\delta(x_{ij}))_{1 \leq i, j \leq n}$$

Além disto, d é uma derivação interna em $M_n(R)$ se e somente se δ é uma derivação interna em R .

Não faremos aqui a demonstração deste teorema. Porém, como utilizamos este resultado no capítulo 3, para o caso particular $n=2$, demonstraremos aqui este caso particular. A demonstração do teorema de F.C. Polcino Milies, no caso $n=2$, é bem mais simples, porém dá uma idéia das técnicas empregadas no caso geral.

Primeiramente vamos demonstrar um lema que também será utilizado mais adiante, no capítulo 4. Este lema aparece em [B.4], onde é dito que se trata de um resultado já conhecido anteriormente.

0.20 - LEMA. Seja R um anel com unidade e d uma derivação em $M_2(R)$. Então existem $a, b, c \in R$ tais que:

$$\begin{aligned} d(e_{11}) &= \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix}, & d(e_{12}) &= \begin{bmatrix} -b & c \\ 0 & b \end{bmatrix}, \\ d(e_{21}) &= \begin{bmatrix} -a & 0 \\ -c & a \end{bmatrix} & \text{e} & d(e_{22}) &= \begin{bmatrix} 0 & -a \\ -b & 0 \end{bmatrix}. \end{aligned}$$

Ainda, dado $x \in R$, temos:

$$d\left(\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} f(x) & xa \\ bx & 0 \end{bmatrix} \quad \text{e,}$$

$$d\left(\begin{bmatrix} 0 & 0 \\ 0 & x \end{bmatrix}\right) = \begin{bmatrix} 0 & -ax \\ -xb & -f(x)+xc-cx \end{bmatrix},$$

onde f é uma derivação em R .

DEMONSTRAÇÃO. Da igualdade $e_{11}^2 = e_{11}$, temos:

$$d(e_{11}) = d(e_{11})e_{11} + e_{11}d(e_{11}).$$

Tomando

$$d(e_{11}) = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

e substituindo na igualdade acima, concluímos que $d(e_{11})$ é

da forma:

$$d(e_{11}) = \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix}.$$

Como $e_{11} + e_{22} = I$, a unidade de $M_2(R)$, temos que:

$$0 = d(I) = d(e_{11}) + d(e_{22})$$

e concluímos que

$$d(e_{22}) = \begin{bmatrix} 0 & -a \\ -b & 0 \end{bmatrix}.$$

Pelas igualdades $e_{11}e_{12}=e_{12}$ e $e_{12}e_{22}=e_{12}$, obtemos:

$$d(e_{12}) = d(e_{11})e_{12} + e_{11}d(e_{12})$$

e,

$$d(e_{12}) = d(e_{12})e_{22} + e_{12}d(e_{22}).$$

Substituindo, na igualdade acima, os valores conhecidos, concluímos que $d(e_{12})$ é da forma:

$$d(e_{12}) = \begin{bmatrix} -b & c \\ 0 & b \end{bmatrix}.$$

Analogamente, usando que $e_{21}e_{11}=e_{21}$ e $e_{22}e_{21}=e_{21}$, obtemos que $d(e_{21})$ é da forma:

$$d(e_{21}) = \begin{bmatrix} -a & 0 \\ w & a \end{bmatrix}.$$

Ainda, como $e_{21}e_{12}=e_{22}$, obtemos:

$$d(e_{22}) = d(e_{21})e_{12} + e_{21}d(e_{12})$$

e substituindo os valores já obtidos, concluímos que $w=-c$.

Seja agora $x \in R$. Então temos

$$d\left(\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} f(x) & g(x) \\ h(x) & j(x) \end{bmatrix}.$$

Aplicando a derivação d a ambos os membros das igualdades:

$$\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} e_{11} = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$$

e,

$$e_{11} \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix},$$

obtemos que $g(x)=xa$, $h(x)=bx$ e $j(x)=0$. Portanto,

$$d\left(\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} f(x) & xa \\ bx & 0 \end{bmatrix}.$$

É imediata a verificação de que f é uma derivação em R .

De forma análoga demonstra-se que

$$d\left(\begin{bmatrix} 0 & 0 \\ 0 & x \end{bmatrix}\right) = \begin{bmatrix} 0 & -ax \\ -xb & t(x) \end{bmatrix}.$$

Para demonstrar que $t(x)=f(x)+xc-cx$ basta aplicar a derivação a ambos os membros da igualdade:

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & x \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

//

A demonstração do teorema 0.19, no caso $n=2$, de corre do lema acima. É o que mostra o seguinte resultado:

0.21 - COROLÁRIO. Sejam R um anel com unidade e d uma derivação em $M_2(R)$. Então d é da forma:

$$d=d_A + \bar{\delta}$$

onde d_A é a derivação interna de $M_2(D)$ dada pela matriz $AGM_2(D)$ e $\bar{\delta}$ é a derivação em $M_2(R)$ induzida pela derivação δ de R . Além disto, d é uma derivação interna em $M_2(D)$ se e somente se δ é uma derivação interna em R .

DEMONSTRAÇÃO. Sejam $a, b, c \in R$ e f uma derivação em R como no lema 0.20. Então, dados $x, y, z, w \in R$ temos:

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} y & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & z \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + \\ + \begin{bmatrix} 0 & 0 \\ 0 & w \end{bmatrix}.$$

Aplicando a derivação d a ambos os membros da igualdade e usando as fórmulas do lema 0.20, obtemos:

$$d\left(\begin{bmatrix} x & y \\ z & w \end{bmatrix}\right) = \begin{bmatrix} f(x) & f(y) \\ f(z) & f(w) \end{bmatrix} + \begin{bmatrix} -yb-az & xa+yc-aw \\ bx-cz-wb & by+wc-cw+za \end{bmatrix} \\ = \begin{bmatrix} f(x) & f(y) \\ f(z) & f(w) \end{bmatrix} + \begin{bmatrix} 0 & -a \\ b & -c \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} - \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} 0 & -a \\ b & -c \end{bmatrix}.$$

Tomando $\delta = f$, e,

$$A = \begin{bmatrix} 0 & -a \\ b & -c \end{bmatrix},$$

é fácil ver que d é uma derivação interna em $M_2(D)$ se e so mente se δ é uma derivação interna em R . Ainda, é claro que $d = d_A + \delta$ e provamos o corolário.

O seguinte resultado caracteriza completamente as derivações F -lineares numa álgebra simples, A , de dimensão finita sobre F , onde $F=Z(A)$.

0.22 - TEOREMA. Seja A uma álgebra simples de dimensão finita sobre seu centro. Então toda derivação d , em A , tal que $d(Z(A))=0$ é uma derivação interna.

Este resultado é uma consequência do teorema de Skolem-Nöether e se encontram, ambos, em [H.6], páginas 99 e 100.

CAPÍTULO I

Os primeiros resultados obtidos com derivação em anéis não comutativos procuram de alguma forma "medir" a derivação. Até que ponto as qualidades da derivação revelam as qualidades do anel? Podemos através das derivações em um anel estudar propriedades do próprio anel?

Uma maneira natural de tentar responder a estas perguntas é estudar $\overline{d(R)}$, o subanel gerado por $d(R)$, onde d é uma derivação em R anel. Outro enfoque possível nesta direção é estudar $C_R(d(R))$, o centralizador de $d(R)$, tentando compará-lo com o centro de R , $Z(R)$. Temos ainda a tentativa de analisar $\text{Anl}_e(d(R))$ ou $\text{Anl}_d(d(R))$ os anuladores à esquerda e à direita de $d(R)$.

Em [H.1] e [H.2] I.N.Herstein estuda $\overline{d(R)}$ e $C_R(d(R))$ concluindo que se a derivação não é nilpotente de índice 3, isto é, se $d^3(R) \neq 0$ então $\overline{d(R)}$ contém ideal não nulo de R . Conclui ainda que se a derivação não é nilpotente de índice 2 e se R é primo, $C_R(d(R)) = Z(R)$. Um fato trivial é que, no caso de R ser primo, $\text{Anl}_e(d(R)) = \text{Anl}_d(d(R)) = 0$. Todas estas informações vão no sentido de mostrar que $d(R)$ é "grande".

Em [B.2], J.M.Bergen generaliza estes resultados para $\overline{d^n(R)}$ no caso em que d não é nilpotente de índice "pequeno". Vamos aqui mostrar os resultados de Bergen.

Se $a \in C_R(d(R))$, então denotando por δ a derivação interna dada por a , $(\delta, d)(r) = ad(r) - d(r)a = 0 \quad \forall r \in R$. Portanto, estudar $C_R(d(R))$ é um caso particular do estudo de compos

postas de derivações. Por esta razão, encontra-se também neste capítulo, o teorema 1.20, que diz que, em anéis primos com característica diferente de dois, a composta de duas derivações é uma derivação se e somente se uma das derivações for nula.

Finalizando o capítulo, encontram-se os resultados de J.Bergson, I.N.Herstein e J.Kerr que aparecem em [B.3]. Neste trabalho são estudados $C_R(d(U))$, $\overline{d(U)}$ e $\text{Anl}(d(U))$ onde U é um ideal de Lie de um anel primo R com $\text{car} R \neq 2$; também é provado que se a composta de duas derivações se anula num ideal de Lie de um anel primo com característica diferente de dois, então uma das derivações é nula.

Primeiramente enunciamos os resultados de Herstein em [H.1] e [H.2].

1.1 - TEOREMA. Sejam R anel qualquer e d uma derivação em R tal que $d^3 \neq 0$. Então $\overline{d(R)}$ contém um ideal não nulo de R .

1.2 - TEOREMA. Sejam R anel primo e $d \neq 0$ uma derivação em R . Então:

(i) se característica de R é diferente de dois, $C_R(d(R)) = Z(R)$.

(ii) se característica de R é dois então $\forall a \in C_R(d(R))$, $a^2 \in Z(R)$. Se $C_R(d(R)) \neq Z(R)$ então d é uma derivação interna definida por um elemento da forma λa onde λ pertence

ao centróide estendido de R e $a \in C_R(d(R))$ é tal que $a \notin Z(R)$.

Na demonstração do teorema acima, é fácil ver que se $d^2 \neq 0$ então $C_R(d(R)) = Z(R)$ e, se $d^2 = 0$, então $\text{car} R = 2$. Logo, podemos emunciar parte do teorema acima da seguinte forma:

1.3 - TEOREMA. Sejam R um anel primo e d uma derivação em R tal que $d^2 \neq 0$. Então $C_R(d(R)) = Z(R)$.

Nesta forma, o caso $\text{car} R = 2$ deixa de ser analisador, mas como é este resultado que Bergen generaliza optamos por deixá-lo, por enquanto, nesta forma. Mais adiante voltaremos a ele exibindo a demonstração de item (ii).

A generalização do primeiro resultado de Herstein é feita através dos dois teoremas a seguir:

1.4 - TEOREMA. Seja R anel qualquer e d uma derivação de R tal que $d^{3n-1} \neq 0$. Então $d^n(R)$ contém um ideal à esquerda (à direita) não nulo de R .

DEMONSTRAÇÃO. Sejam x e $y \in R$. Usando indução sobre n é fácil ver que:

$$d^n(xy) = x d^n(y) + \sum_{i=1}^n \binom{n}{i} d^i(x) d^{n-i}(y). \quad (1)$$

Substituindo, em (1), x por $d^{n-1}(x)$ e y por $d^n(y)$ obtemos:

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

Como $1 \leq i \leq n$, $n-1+i \geq n$ e $2n-i \geq n$. Portanto o segundo membro de (2) pertence à $\overline{d^n(R)}$; logo, $d^{n-1}(x)d^{2n}(y) \in \overline{d^n(R)} \quad \forall x, y \in R$.

Substituindo agora, em (1), x por $d^{n-2}(x)$ e y por $d^{n+1}(y)$ obtemos:

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

Se $2 \leq i \leq n$, então $n-2+i \geq n$ e $2n+1-i \geq n$; ainda, pelo que foi feito acima, sabemos que $d^{n-1}(x)d^{2n}(y) \in \overline{d^n(R)}$ e concluímos que o segundo membro de (3) pertence a $\overline{d^n(R)}$. Portanto $d^{n-2}(x)d^{2n+1}(y) \in \overline{d^n(R)} \quad \forall x, y \in R$.

Se formos adiante substituindo, em (1), x por $d^{n-j}(x)$ e y por $d^{n+j-1}(y)$, $j=1,2,3,\dots,n$, usando os resultados anteriores obteremos:

$$d^{n-j}(x)d^{2n+j-1}(y) \in \overline{d^n(R)} \quad \forall x, y \in R.$$

Em particular, para $j=n$, temos $xd^{3n-1}(y) \in \overline{d^n(R)} \quad \forall x, y \in R$, isto é, $Rd^{3n-1}(R) \subset \overline{d^n(R)}$. Como $d^{3n-1}(R) \neq 0$, o ideal à esquerda de R gerado por $d^{3n-1}(R)$ é não nulo e, como $Rd^{3n-1}(R) \subset \overline{d^n(R)}$ e $d^{3n-1}(R) \subset \overline{d^n(R)}$, este ideal está contido em $\overline{d^n(R)}$.

De forma análoga prova-se que $\overline{d^n(R)}$ contém o ideal à direita não nulo de R gerado por $d^{3n-1}(R)$.

//

1.5 - TEOREMA. Seja R um anel qualquer e d uma derivação de R tal que $d^{6n-3} \neq 0$. Então $\overline{d^n(R)}$ contém um ideal não nulo de R.

DEMONSTRAÇÃO. Sejam x, y e $z \in R$. Usando a mesma fórmula (1) do teorema anterior temos:

$$d^{3n-1}(yz) = d^{3n-1}(y)z + \sum_{i=1}^{3n-1} \binom{3n-1}{i} d^{3n-1-i}(y) d^i(z).$$

Multiplicando a igualdade por x obtemos:

$$xd^{3n-1}(y)z = xd^{3n-1}(yz) - x \sum_{i=1}^{3n-1} \binom{3n-1}{i} d^{3n-1-i}(y) d^i(z). \quad (1)$$

Substituindo, em (1) z por $d^{3n-2}(z)$ obtemos:

$$xd^{3n-1}(y)d^{3n-2}(z) = xd^{3n-1}(yd^{3n-2}(z)) - x \sum_{i=1}^{3n-1} \binom{3n-1}{i} d^{3n-1-i}(y) d^{3n-2+i}(z) \quad (2)$$

Ainda, se $i \geq 1$ então $3n-2+i \geq 3n-1$; logo, cada somando do 2º membro de (2) pertence a $Rd^{3n-1}(R)$. Usando o teorema anterior concluímos que o segundo membro de (2) está contido em $\overline{d^n(R)}$ e portanto $xd^{3n-1}(y)d^{3n-2}(z) \in \overline{d^n(R)} \forall x, y, z \in R$.

Substituindo agora, em (1), z por $d^{3n-3}(z)$ e y por $d(y)$ obtemos:

$$\begin{aligned}
 xd^{3n}(y)d^{3n-3}(z) &= xd^{3n-1}(d(y)d^{3n-3}(z)) - \\
 &\quad - x \sum_{i=1}^{3n-1} \binom{3n-1}{i} d^{3n-i}(y)d^{3n-3+i}(z) \quad (3)
 \end{aligned}$$

Como já sabemos que $xd^{3n-1}(y)d^{3n-2}(z) \in \overline{d^n(R)}$ e para $i \geq 2$, $3n-3+i \geq 3n-1$, fica claro que o segundo membro da igualdade, pertence a $\overline{d^n(R)}$ e portanto $xd^{3n}(y)d^{3n-3}(z) \in \overline{d^n(R)} \quad \forall x, y \text{ e } z \in R$.

Se formos adiante substituindo, em (1), z por $d^{3n-j}(z)$ e y por $d^{j-2}(y)$ para $j=2, 3, \dots, 3n$, usando os resultados obtidos anteriormente, concluímos que:

$$xd^{3n-3+j}(y)d^{3n-j}(z) \in \overline{d^n(R)} \quad \forall x, y \text{ e } z \in R, \quad \forall j \ 2 \leq j \leq n.$$

Em particular, para $j=3n$, temos: $Rd^{6n-3}(R)R \subset \overline{d^n(R)}$. Usando novamente o teorema anterior, temos $Rd^{6n-3}(R) \subset Rd^{3n-1}(R) \subset \overline{d^n(R)}$ e $d^{6n-3}(R)R \subset d^{3n-1}(R)R \subset \overline{d^n(R)}$; ainda, $d^{6n-3}(R) \subset \overline{d^n(R)}$, portanto, o ideal bilateral não nulo gerado por $d^{6n-3}(R)$ está contido em $\overline{d^n(R)}$.

//

Em particular, o teorema 1.5 nos diz que se $d^3 \neq 0$ então $\overline{d(R)}$ contém um ideal não nulo de R , Vamos mostrar agora, através de um exemplo, que supondo apenas $d^2 \neq 0$ não obtemos o mesmo resultado.

1.6 - EXEMPLO. Sejam R um anel primo com $\text{car} R \neq 2$ e $0 \neq a \in R$ tal que $a^2 = 0$. Seja d a derivação interna dada por $a, d(x) = [a, x] \quad \forall x \in R$. Vamos provar que $d^3 = 0$, $d^2 \neq 0$ e $\overline{d(R)}$ não contém ideal nulo de R .

Ora, $d^2(x) = d([a, x]) = [a, [a, x]] = -2axa \quad \forall x \in R$. Como R é primo e $\text{car} R \neq 2$, é claro que $d^2(R) \neq 0$. por outro lado, $a^2 = 0$ implica $d^3 = 0$. Ainda, $d(R) \subset aR + Ra$ e, como $a^2 = 0$, o subanel gerado por $aR + Ra$ é o próprio $aR + Ra$. Então $\overline{d(R)} \subset aR + Ra$. Se existisse $I \neq 0$ ideal de R tal que $I \subset \overline{d(R)}$, teríamos $aIa \subset a(aR + Ra)a = 0$ o que, por R ser primo e $a \neq 0$ contradiz $I \neq 0$.

Vamos agora analisar as generalizações de Bergen para $C_R(d^n(R))$ e $\text{Anl}(d^n(R))$. Os resultados obtidos nesta direção são para anéis primos. A seguir vem um exemplo que mostra que se R não é primo, não podemos esperar que $C_R(d(R)) = Z(R)$ ou $\text{Anl}_e(d(R)) = 0$.

1.7 - EXEMPLO. Seja R um anel semiprimo, mas não primo e sejam I e J ideais não nulos de R tais que $IJ = 0$. Seja ainda $a \notin J$ tal que $a \notin Z(R)$ e consideremos a derivação interna da por a :

$$d(r) = ar - ra \quad \forall r \in R.$$

Como $a \notin Z(R)$, sabemos que $d \neq 0$. Mas $d(R) \subset J$, portanto $\text{Id}(R) = 0$, isto é, $I \subset \text{Anl}_e(d(R)) \neq 0$.

Ainda, como R é semiprimo e $IJ = 0$ implica $JIRJI = 0$, temos $JI = 0$. Portanto $I \subset C_R(J) \subseteq C_R(d(R))$. Basta tomarmos I contendo um elemento nilpotente para garantirmos $I \not\subset Z(R)$ e portanto $C_R(d(R)) \neq Z(R)$.

Trabalharemos, portanto, com anéis primos. Primeiramente demonstraremos o lema 1.8, que é um caso particular

do que faremos adiante. Optamos por destacar este resultado, pois sua demonstração é muito simples e ele será constantemente requisitado ao longo deste trabalho.

1.8 - LEMA. Sejam R um anel primo e d uma derivação de R . Valem as seguintes afirmações:

(i) se $I \neq 0$ é ideal de R e $d \neq 0$ então $\text{Anl}_e(d(I)) = \text{Anl}_d(d(I)) = 0$.

(ii) se $L \neq 0$ é ideal lateral de R e $d(L) = 0$ então $d = 0$.

DEMONSTRAÇÃO. Primeiramente vamos demonstrar o item (i). Suponhamos que $a \in \text{Anl}_e(d(I))$. Então $ad(I) = 0$ e consequentemente $0 = ad(IR) = aId(R)$. Ora, mas $d \neq 0$ e R é primo, portanto $Id(R)$ é ideal à esquerda não nulo de R e $\text{Anl}_e(Id(R)) = 0$. Então $a = 0$. A demonstração de que $\text{Anl}_d(d(I)) = 0$ é análoga.

Vamos à demonstração de (ii). Suponhamos que L é ideal à esquerda de R . Então, se $d(L) = 0$, temos:

$$0 = d(RL) = d(R)L.$$

Mas R é primo, portanto anulador à esquerda de ideal à esquerda é zero e concluímos que $d(R) = 0$. A demonstração para ideal à direita é análoga.

//

O item (i) do lema 1.8 nos mostra trivialmente que os anuladores de $d(I)$ são nulos uma vez que $d \neq 0$. Bergen generaliza este resultado para $d^n(I)$ no caso em que

$d^{2n-1} \neq 0$. Vamos agora mostrar este resultado. Mas, precisaremos antes de um lema, que também será utilizado na demonstração do teorema 1.16 que virá mais adiante.

1.9 LEMA. Sejam R , anel, d uma derivação de R e I ideal de R . Então $d^m(I^n) \subset I^{n-m}$ se $0 \leq m < n$.

DEMONSTRAÇÃO. É claro que, se $m=0$, $d^m(I^n) = I^n \subset I^n$ e nada há a demonstrar. Vamos provar o lema para $1 \leq m < n$, usando indução em n . Se $n=2$, então: $d(I^2) \subset Id(I) + d(I)I \subset I$ e portanto o resultado vale para $n=2$. Suponhamos que para todo ideal I de R seja verdade que $d^m(I^n) \subset I^{n-m}$ se $1 \leq m < n$ e $n \geq 2$. Vamos mostrar que $d^k(I^{n+1}) \subset I^{n+1-k}$ se $1 \leq k < n+1$.

Utilizando a fórmula, $d^k(xy) = \sum_{i=0}^k \binom{k}{i} d^{k-i}(x)d^i(y)$
 $\forall x, y \in R$, temos que:

$$d^k(I^{n+1}) \subset \sum_{i=0}^k \binom{k}{i} d^{k-i}(I^n)d^i(I).$$

Vamos mostrar que, cada um dos somandos do 2º membro está contido em I^{n+1-k} . Se $1 \leq i \leq k$ então $0 \leq k-i \leq k-1 < n$ e a hipótese de indução nos garante que $d^{k-i}(I^n) \subset I^{n-k+i}$. Ainda, $I^{n-k+i} \subset I^{n+1-k}$ pois $i \geq 1$. Se $i=0$, $d^k(I^n)d^0(I) = d^k(I^n)I \subset I^{n+1-k}$ pois, se $k < n$ usamos a hipótese de indução e se $k=n$ o cálculo é trivial. Mostramos então que $d^{k-i}(I^n)d^i(I) \subset I^{n+1-k}$ $\forall i, k$ $0 \leq i \leq k$ e $1 \leq k < n+1$. Portanto, $d^k(I^{n+1}) \subset I^{n+1-k}$ e provamos o lema.

//

1.10 - TEOREMA. Sejam R anel primo com derivação d tal que $d^{2n-1} \neq 0$ e I ideal não nulo de R . Então $\text{Anl}_e(d^n(I)) = \text{Anl}_d(d^n(I)) = 0$.

DEMONSTRAÇÃO. Sejam $a \in \text{Anl}_e(d^n(I))$, $x \in I$ e $r \in R$. Então:

$$0 = ad^n(xr) = a \sum_{i=0}^n d^{n-i}(x) d^i(r). \quad (1)$$

Pelo lema anterior sabemos que $d^m(I^n) \subset I^{n-m} \subset I$ para todo m , $0 \leq m \leq n-1$. Seja então $y \in J = I^n$ e seja $x = d^{n-1}(y) \in d^{n-1}(I^n) \subset I$. De (1) obtemos:

$$0 = a \sum_{i=0}^n \binom{n}{i} d^{2n-i-1}(y) d^i(r) \quad (2)$$

Mas, se $0 \leq i \leq n-1$, usando o lema anterior temos:

$$d^{2n-i-1}(y) = d^n(d^{n-i-1}(y)) \in d^n(d^{n-i-1}(I^n)) \subset d^n(I^{i+1}) \subset d^n(I).$$

Portanto, $a \sum_{i=0}^{n-1} \binom{n}{i} d^{2n-i-1}(y) d^i(r) = 0$ e, de (2), concluímos que $ad^{n-1}(y) d^n(r) = 0 \quad \forall y \in J$ e $\forall r \in R$. Isto é, $ad^{n-1}(J) d^n(R) = 0$.

Tomando agora $x = d^{n-2}(y)$ com $y \in J$ e $r = d(s)$ com $s \in R$, obtemos, em (1):

$$0 = a \sum_{i=0}^n \binom{n}{i} d^{2n-i-2}(y) d^{i+1}(s). \quad (3)$$

Da mesma forma, para $0 \leq i \leq n-2$ temos $d^{2n-2-i}(y) = d^n(d^{n-2-i}(y)) \in d^n(I^{i+2}) \subset d^n(I)$. Portanto da igualdade (3) concluímos que $0 = ad^{n-2}(y) d^{n+1}(s) + nad^{n-1}(y) d^n(s) \quad \forall y \in J, s \in R$. Usando agora o resultado obtido da igualdade (2), $ad^{n-1}(J) d^n(R) = 0$, obtemos

$$\text{ad}^{n-2}(J)\text{d}^{n+1}(R)=0.$$

Se continuarmos este procedimento, substituindo em (1) x por $\text{d}^{n-j}(y)$ com $y \in J$ e r por $\text{d}^{j-1}(r)$ para $j=1,2,\dots,n$, obtemos a cada passo $0=\text{ad}^{n-j}(J)\text{d}^{n+j-1}(R)$. Em particular para $j=n$ temos $aJ\text{d}^{2n-1}(R)=0$. Como R é primo e $\text{d}^{2n-1} \neq 0$, então $J\text{d}^{2n-1}(R) \neq 0$ e concluímos que $a=0$, que é o que pretendíamos demonstrar. A demonstração de que $\text{Anl}_d(\text{d}^n(I))=0$ é análoga.

//

Vamos agora, através de dois exemplos, mostrar que as hipóteses do teorema 1.10 não podem ser enfraquecidas. O primeiro exemplo mostra que o índice $2n-1$ não pode diminuir.

1.11 - EXEMPLO. Seja R um anel primo com $\text{car}R=0$ e seja $a \in R$ tal que $a^{n-1} \neq 0$ mas $a^n=0$. Consideremos d a derivação interna dada por a , $d(x)=[a,x] \forall x \in R$. Vamos mostrar que $\text{d}^{2n-2} \neq 0$ mas $\text{Anl}_e(d(R)) \neq 0$.

Usando indução sobre k é fácil mostrar que:

$$\text{d}^k(x) = \sum_{i=0}^n \binom{n}{i} (-1)^i a^{k-i} x a^i \quad \forall x \in R, \forall k \geq 1.$$

Fica então claro que $\text{d}^{2n-1}=0$ e

$$\text{d}^{2n-2}(x) = \binom{2n-2}{n-1} (-1)^{n-1} a^{n-1} x a^{n-1} \quad \forall x \in R.$$

Como R é primo, $\text{car}R=0$ e $a^{n-1} \neq 0$ então $\text{d}^{2n-2}(R) \neq 0$.

Ainda, $d^n(R) = \sum_{i=0}^n a^{n-i} R a^i = \sum_{i=1}^{n-1} a^{n-i} R a^i$ pois $a^n = 0$.
Logo, $a^{n-1} \notin \text{Anl}_e(d^n(R)) \neq 0$, e temos o que queríamos.

A hipótese R primo, no teorema 1.10, não pode ser enfraquecida para R semiprimo. isto é o que mostra o exemplo a seguir:

1.12 - EXEMPLO. Sejam R anel primo e $d \neq 0$ uma derivação em R . Seja $S = R \oplus R$. Sabemos que S é semiprimo mas não primo. Consideremos em S a derivação $D \neq 0$ dada por $D(r,s) = (d(r), 0)$ $\forall (r,s) \in S$.

É claro que $D(S) = (d(R), 0) \subset (R, 0)$ e portanto $0 \neq (0, R) \subset \text{Anl}_e(D(S))$, e temos o que queríamos. Podemos fazer o mesmo com $D^n(S)$, isto é, se $d^{2n-1} \neq 0$ então $D^{2n-1} \neq 0$ mas $0 \neq (0, R) \subset \text{Anl}_e(D^n(S))$.

Do lema 1.8 sabemos que, se R é primo, $d \neq 0$ é uma derivação em R e I , é um ideal de R , então $d(I) = 0$ implica $d = 0$. Do teorema 1.10 sai como corolário imediato uma generalização deste fato:

1.13 - COROLÁRIO. Sejam R um anel primo e d uma derivação em R tal que $d^{2n-1} \neq 0$. Se I é um ideal de R tal que $d^n(I) = 0$ então $I = 0$.

DEMONSTRAÇÃO. Suponhamos por absurdo, que $I \neq 0$. Então pelo teorema 1.10, $\text{Anl}_e(d^n(I)) = 0$. Mas, como $d^n(I) = 0$, $R \subset \text{Anl}_e(d^n(I)) = 0$ o que é absurdo.

//

O exemplo 1.12 mostra que se R é semiprimo mesmo que $d \neq 0$ não temos necessariamente $\text{Anl}_e(d(R))=0$. Porém, para anéis semiprimos temos ainda alguns resultados positivos de demonstração imediata:

PROPOSIÇÃO 1.14. Sejam R anel semiprimo, e $d \neq 0$ uma derivação de R . Então $d(R) \cap \text{Anl}_e(d(R)) = d(R) \cap \text{Anl}_d(d(R)) = 0$.

DEMONSTRAÇÃO. Seja $a \in R$ e $d(a) \in \text{Anl}_e(d(R))$. Então:

$$0 = d(a)d(R) \supset d(a)d(Ra) = d(a)Rd(a),$$

e como R é semiprimo, $d(a)=0$. A demonstração de que $\text{Anl}_d(d(R)) \cap d(R) = 0$ é análoga.

//

PROPOSIÇÃO 1.15. Sejam R anel semiprimo e $d \neq 0$ uma derivação em R . Então $d(\text{Anl}_e d(R)) = d(\text{Anl}_d d(R)) = 0$.

DEMONSTRAÇÃO: Seja $a \in \text{Anl}_e(d(R))$. Sabemos que $ad(R)=0$ portanto: $0 = d(ad(R)) = d(a)d(R)$. Pela proposição anterior temos então $d(a)=0$. Simetricamente demonstra-se que

$$d(\text{Anl}_d d(R)) = 0.$$

//

Faremos aqui um parêntese, antes de analisar $C_R(d^n(R))$, voltando ao teorema 1.5. Nele, Bergen mostra

que se $d^{6n-3} \neq 0$ então $\overline{d(R)}$ contém um ideal não nulo de R . Nos perguntamos se podemos generalizar este resultado para $\overline{d^n(I)}$ onde I é um ideal de R tal que $d^{6n-3}(I) \neq 0$. Tentamos aplicar a mesma técnica de Bergen, mas nos deparamos com a seguinte dificuldade: não sabemos se $d^{6n-3}(I) \neq 0$ garante que $d^{3n-1}(I^k) \neq 0$ para $k \geq 2$. Porém se, o anel R é primo, conseguimos contornar a dificuldade obtendo o resultado esperado, como mostra o seguinte teorema:

1.16 - TEOREMA. Sejam R anel primo, $I \neq 0$ ideal de R e d uma derivação em R tal que $d^{6n-3} \neq 0$. Então $\overline{d^n(I)}$ contém um ideal não nulo de R .

DEMONSTRAÇÃO. Para maior clareza dividiremos a demonstração em duas afirmações:

Afirmção 1. Seja $J = I^n$. Então $Jd^{3n-1}(J)$ e $d^{3n-1}(J)J$ estão contidos em $\overline{d^n(I)}$.

Para demonstrar esta afirmação repetiremos a demonstração do teorema 1.4. Partindo da igualdade:

$$xd^n(y) = d^n(xy) - \sum_{i=1}^n \binom{n}{i} d^i(x) d^{n-i}(y) \quad \forall x, y \in I,$$

vamos substituindo x por $d^{n-j}(z)$ e y por $d^{n+j-1}(w)$ para $j=1, 2, \dots, n$. Neste caso, precisamos tomar z e w pertencentes a $J = I^n$ para garantir (lema 1.9) que $d^m(z)$ e $d^m(w) \in I$ para $0 \leq m < n$. A cada substituição, usando as substituições anteriores, obteremos:

$$d^{n-j}(z)d^{2n+j-1}(w) \in \overline{d^n(I)} \quad \forall z, w \in J.$$

Finalmente para $j=n$ teremos $zd^{3n-1} \in \overline{d^n(I)} \quad \forall z, w \in J$, isto é, $Jd^{3n-1}(J) \subset \overline{d^n(I)}$. Simetricamente obtemos

$$d^{3n-1}(J)J \subset \overline{d^n(I)},$$

e está provada a afirmação 1.

Afirmção 2. $Jd^{3n-1}(J)^2J \neq 0$.

Suponhamos, por absurdo, que $Jd^{3n-1}(J)^2J = 0$. Como R é primo, $J = I^n \neq 0$, e portanto $Jd^{3n-1}(J)^2J = 0$ implica $d^{3n-1}(J)^2 = 0$. Mas, pelo teorema 1.10, como $d^{6n-3} \neq 0$ temos $\text{Anl}_d(d^{3n-1}(J)) = 0$; logo, $d^{3n-1}(J)^2 = 0$ implica $d^{3n-1}(J) = 0$ que acarreta (corolário 1.13) $J = 0$ o que é absurdo. Portanto

$$Jd^{3n-1}(J)^2J \neq 0.$$

Para finalizar a demonstração do teorema, basta tomarmos M , o subgrupo aditivo gerado por $Jd^{3n-1}(J)^2J$.

É claro que M é um ideal de R . A afirmação 1 mostra que $M \subset \overline{d^n(I)}$ e a afirmação 2 que $M \neq 0$.

//

Vamos agora estudar $C_R(d^n(R))$. Já citamos o resultado de Herstein (teorema 1.3) que nos diz que $C_R(d(R)) = Z(R)$ se R é primo e $d^2 \neq 0$. Em [B.2] Bergen generaliza este resultado, como uma consequência imediata do teorema 1.4.

1.17 - TEOREMA. Sejam R um anel primo e d uma derivação em R tal que $d^{3n-1} \neq 0$. Então

$$C_R(d^n(R)) = Z(R).$$

DEMONSTRAÇÃO. Pelo teorema 1.4 sabemos que existe $L \neq 0$ ideal à esquerda não nulo de R tal que $L \subset \overline{d^n(R)}$. Então:

$$Z(R) \subset C_R(d^n(R)) = C_R(\overline{d^n(R)}) \subset C_R(L).$$

Mas, como R é primo, $C_R(L) = Z(R)$ (teorema 0.1) e portanto:

$$C_R(d^n(R)) = C_R(\overline{d^n(R)}) = Z(R).$$

//

Poderíamos nos perguntar se não vale o mesmo resultado para ideais de R , isto é, $d^{3n-1}(I) \neq 0$ implicaria $C_R(d^n(I)) = Z(R)$? Aqui novamente, tentando as mesmas técnicas de Bergen nos deparamos com as mesmas dificuldades mencionadas antes do teorema 1.16. É claro que, utilizando o teorema 1.16 obtemos um resultado, mais fraco, que é o seguinte:

1.18 - COROLÁRIO. Sejam R um anel primo e $I \neq 0$ ideal de R . Seja ainda d uma derivação em R tal que $d^{6n-3} \neq 0$. Então $C_R(d^n(I)) = Z(R)$.

DEMONSTRAÇÃO. Pelo teorema 1.16 sabemos que $\overline{d^n(I)} \supset K$, ideal nulo de R . Então, da mesma forma que no teorema 1.16 obte

mos:

$$Z(R) \subset C_R(d^n(I)) = C_R(\overline{d^n(I)}) \subset C_R(K) = Z(R).$$

Portanto,

$$C_R(d^n(I)) = Z(R).$$

//

Observamos aqui que se $n=1$, sabe-se que $C_R(d(I)) = Z(R)$, bastando para isto que $d^2 \neq 0$. Vamos demonstrar este fato.

1.19 - PROPOSIÇÃO. Sejam R um anel primo e d uma derivação em R tal que $d^2 \neq 0$. Se $I \neq 0$ é um ideal de R , então:

$$(i) \ 0 \neq Id^2(I) \subset \overline{d(I)}.$$

$$(ii) \ C_R(d(I)) = Z(R).$$

DEMONSTRAÇÃO. Sejam x e $y \in I$, então:

$$xd^2(y) = d(xd(y)) - d(x)d(y) \in \overline{d(I)}.$$

Portanto $Id^2(I) \subset \overline{d(I)}$. Se $d^2(I) = 0$, como $d(I^2) \subset I$, teríamos: $0 = d^2(Rd(I^2)) = d^2(R)d(I^2)$; mas neste caso, pelo teorema 1.10, $d^2 = 0$, o que é absurdo. Então $d^2(I) \neq 0$ e, como R é primo, $Id^2(I) \neq 0$. Provamos então (i).

Para demonstrar (ii) basta observar que, de (i), sabemos que o ideal à direita $\text{Id}^2(I) \subset \overline{d(I)}$. Logo,

$$Z(R) \subset C_R(d(I)) = C_R(\overline{d(I)}) \subset C_R(\text{Id}^2(I)) = Z(R),$$

o que acarreta

$$C_R(d(I)) = Z(R).$$

//

Estes resultados aqui expostos vão no sentido de mostrar que $\overline{d(R)}$, o anel gerado por $d(R)$, é "grande".

No início do capítulo, mencionamos o teorema 1.2, um resultado de Herstein. Voltaremos à ele agora. Também de mostraremos um outro teorema que trata de composta de duas derivações, e que esta relacionado com o primeiro. Os dois teoremas são os seguintes:

1.20 - TEOREMA. Sejam R anel primo, d e δ derivações em R . Se a composta d, δ é também uma derivação em R então:

(i) $\text{car} R \neq 2$ implica $d=0$ ou $\delta=0$.

(ii) $\text{car} R = 2$ e $d \neq 0$ implicam $\delta = \lambda d$ onde λ pertence a C , o centróide estendido de R .

1.2 - TEROREMA. Sejam R anel primo com derivação $d \neq 0$ e $a \in C_R(d(R))$. Valem as seguintes afirmações:

(i) $\text{car} R \neq 2$ implica $a \in Z(R)$.

(ii) $\text{car} R = 2$ implica $a^2 \in Z(R)$. Ainda, se $a \notin Z(R)$ então d é uma derivação interna dada por λa onde λ pertence a C , o centróide estendido de R .

O item (i) do teorema 1.20 é um resultado de Posner que se encontra em [P.1]. O item (ii) deste teorema foi feito por Bergen em [B.2]. O teorema 1.2 já foi citado anteriormente: é um resultado de Herstein que se encontra em [H.2].

Apesar de terem suas demonstrações independentes, o teorema 1.2 é claramente um caso particular do teorema 1.20 e por isto optamos por mostrá-los juntos, dando a demonstração do teorema 1.20 e tirando o teorema 1.2 como consequência deste.

Em ambos os teoremas, para a demonstração do item (ii), é utilizado um resultado de Martindale (lema 0.9) que foi citado no capítulo zero. Lembramos que C , o centróide estendido de R , é um corpo, centro de um anel primo Q que contém R . O anel Q tem, portanto, estrutura de C -álgebra.

DEMONSTRAÇÃO DO TEOREMA 1.20. Como $d \circ \delta$ é uma derivação, temos:

$$(d \circ \delta)(xy) = (d \circ \delta)(x)y + x(d \circ \delta)(y) \quad \forall x, y \in R.$$

Por outro lado,

$$\begin{aligned} (d \circ \delta)(xy) &= d(\delta(x)y + x\delta(y)) = (d \circ \delta)(x)y + \delta(x)d(y) + d(x)\delta(y) + \\ &\quad + x(d \circ \delta)(y). \end{aligned}$$

Concluimos então que:

$$\delta(x)d(y)+d(x)\delta(y)=0 \quad \forall x,y \in R \quad (1)$$

Substituindo x por xr em (1) obtemos:

$$\delta(x)rd(y)+d(x)r\delta(y)+x(\delta(r)d(y)+d(r)\delta(y))=0$$

e portanto,

$$\delta(x)rd(y)+d(x)r\delta(y)=0 \quad \forall x,y,r \in R \quad (2)$$

Se $d=0$, nada há a demonstrar. Suponhamos então $d \neq 0$. Vamos provar que dado $x \in R$, $d(x)=0$ implica $\delta(x)=0$. Ora, se $d(x)=0$ de (1) temos: $\delta(x)d(R)=0$ o que, pelo lema 1.8, acarreta $\delta(x)=0$.

Pelo resultado de Martindale (lema 0.9), da igualdade (2) concluimos que $\delta(x)$ e $d(x)$ são linearmente dependentes sobre C , o centróide estendido de R . Como $d(x)=0$ implica $\delta(x)=0$, podemos afirmar que:

$$\forall x \in R, \exists \lambda_x \in C \text{ tal que } \delta(x)=\lambda_x d(x).$$

Vamos mostrar que λ_x não depende x . De fato, se $d(x)=0$ então $\delta(x)=0$ e qualquer $\lambda_x \in C$ é tal que $\delta(x)=\lambda_x d(x)$. Sejam então x e $y \in R$ tais que $d(x) \neq 0$ e $d(y) \neq 0$. Sabemos que existem λ_x e $\lambda_y \in C$ tais que:

$$\delta(x)=\lambda_x d(x) \quad \text{e} \quad \delta(y)=\lambda_y d(y).$$

Substituindo, na igualdade (1), e lembrando que λ_x e λ_y co

mutam com qualquer elemento de R , obtemos:

$$(\lambda_x + \lambda_y)d(x)d(y) = 0. \quad (3)$$

Afirmamos que existe $r \in R$ tal que $d(x)d(r) \neq 0$ e $d(y)d(r) \neq 0$. De fato, como $d(x) \neq 0$ e $d(y) \neq 0$, o lema 1.8 nos garante que $d(x)d(R) \neq 0$ e $d(y)d(R) \neq 0$, portanto existem r_1 e $r_2 \in R$ tais que $d(x)d(r_1) \neq 0$ e $d(y)d(r_2) \neq 0$. Se $d(x)d(r_2) = d(y)d(r_1) = 0$, então $d(x)d(r_1 + r_2) = d(x)d(r_1) \neq 0$ e $d(y)d(r_1 + r_2) = d(y)d(r_2) \neq 0$. De qualquer forma pelo menos um entre r_1 , r_2 e $r_1 + r_2$ satisfaz o que queríamos.

Tomemos então $r \in R$ tal que $d(x)d(r) \neq 0$ e $d(y)d(r) \neq 0$. Pela igualdade (3) sabemos que $(\lambda_x + \lambda_r)d(x)d(r) = 0$ e $(\lambda_y + \lambda_r)d(y)d(r) = 0$. Como $d(x)d(r) \neq 0$, $d(y)d(r) \neq 0$ e C é corpo temos:

$$\lambda_y + \lambda_r = \lambda_x + \lambda_r = 0,$$

isto é,

$$\lambda_x = \lambda_y = -\lambda_r.$$

Concluimos, então, que λ_x independe de x , isto é, existe $\lambda \in C$ tal que $\delta = \lambda d$ e ainda que $2\lambda = 0$. está, portanto provado o item (ii).

Finalmente, se $\text{car} R \neq 2$, então $\text{car} Q \neq 2$ e como Q é anel primo, Q é livre de 2-torção. Como $2\lambda = 0$, então $\lambda = 0$ e temos $\delta = 0$.

//

Vamos agora demonstrar o teorema 1.2. Antes, porém, enfatizamos duas igualdades envolvendo comutadores que serão utilizadas não só nesta demonstração, mas frequentemente ao longo deste trabalho.

Seja R anel primo, $x, y, z \in R$. É fácil ver que:

$$[xy, z] = x[y, z] + [x, z]y \quad \text{e} \quad [x, yz] = [x, y]z + y[x, z];$$

$$[[x, y], z] = [x, [y, z]] + [y, [z, x]] \quad \text{e}$$

$$[x, [y, z]] = [[x, y], z] + [[z, x], y].$$

DEMONSTRAÇÃO DO TEOREMA 1.2. Consideremos d_a , a derivação interna dada por $a: d_a(x) = [a, x] \quad \forall x \in R$. Como $a \in C_R(d(R))$, então $[a, d(x)] = 0 \quad \forall x \in R$ e obtemos a seguinte igualdade:

$$(d_a \circ d)(x) = d_a(d(x)) = [a, d(x)] = 0 \quad \forall x \in R.$$

Logo, a composta $d_a \circ d$ é a derivação nula em R e estamos nas condições do teorema 1.20.

Se $\text{car} R \neq 2$, pelo teorema 1.20, $d_a = 0$ ou $d = 0$. Como $d \neq 0$, temos $d_a = 0$, isto é, $a \in Z(R)$ e está provado o item (i).

Suponhamos agora $\text{car} R = 2$. Se $a \in Z(R)$ então $d_a = 0$, $a^2 \in Z(R)$ e nada há a demonstrar. Se $a \notin Z(R)$, então $d_a \neq 0$ e, pelo teorema 1.20, sabemos que d é da forma $d = \lambda d_a$ onde $\lambda \in C$ o centróide estendido de R . Logo, para todo $x \in R$, temos:

$$d(x) = \lambda d_a(x) = \lambda [a, x] = [\lambda a, x],$$

pois $[\lambda, x]=0$. Resta provar que $a^2 \in Z(R)$. Ora, como $d(x)=[\lambda a, x]$ e $[a, d(x)]=0 \ \forall x \in R$, temos:

$$0=[a, d(x)]=[a, [\lambda a, x]]=\lambda[a, [a, x]].$$

Ora, mas então

$$0=\lambda[a, [a, x]]=\lambda(a^2x-2axa+xa^2)=\lambda[a^2, x]$$

pois $\text{car} R=2$. Ainda, $\lambda \neq 0$ pois $0 \neq d=\lambda d_a$. Logo, λ não é divi-
sor de zero e temos:

$$[a^2, x]=0 \quad \forall x \in R, \text{ isto é, } a^2 \in Z(R).$$

//

Em [B.3], J.Bergson, I.N.Herstein e J.W.Kerr estu-
dam $d(U)$ onde d é uma derivação em R , anel primo com $\text{car} R \neq 2$ e $U \not\subset Z(R)$ é um ideal de Lie de R . Os resultados obtidos
para $\text{Anl}_e(d(U))$, $C_R(d(U))$ e $\overline{d(U)}$ são os mesmos que os ante-
riormente obtidos para ideais de anéis primos. Mostraremos
aqui estes resultados.

Observamos que, no caso em que $U \subset Z(R)$, os resul-
tados são imediatos conforme mostra a seguinte proposição.

1.21 - PROPOSIÇÃO. Sejam R um anel primo, U ideal de Lie de
 R , tal que $U \subset Z(R)$ e d uma derivação em R . Valem as se-
guintes afirmações:

$$(i) \text{ se } d(U) \neq 0 \text{ então } \text{Anl}_e(d(U)) =$$

$$= \text{Anl}_d(d(U)) = 0.$$

$$(ii) \ C_R(d(U)) = R.$$

(iii) se $\overline{d(U)}$ contém um ideal não nulo de R então R é comutativo.

DEMONSTRAÇÃO. Já vimos no capítulo 0 que $d(Z(R)) \subset Z(R)$. Portanto $d(U) \subset Z(R)$ e temos o item (ii).

Ainda, como R é primo, $\forall z \in Z(R)$ se $z \neq 0$ então z é regular. Conclui-se então o item (i).

Se $\overline{d(U)} \supset I \neq 0$, ideal de R então $I \subset Z(R)$ e o teorema 0.1 nos dá R comutativo.

//

A proposição acima nos dá as informações desejadas sobre $d(U)$ no caso em que $U \subset Z(R)$. Vamos então aos resultados de [B.3] sobre $d(U)$ para $U \not\subset Z(R)$. Antes de começar a lidar com derivações em ideais de Lie, necessitaremos de alguns lemas mais gerais sobre ideais de Lie em anéis primos. Estes resultados preliminares se encontram em [H.9]. Porém, as demonstrações que faremos, os utilizamos numa forma distinta daquela que aparece em [H.9]; por isto eles estão refeitos aqui na forma mais adequada às demonstrações que temos a fazer.

Os primeiros resultados são para anéis semiprimos. Apesar de que só lidaremos com anéis primos optamos por deixá-los na sua forma mais geral.

1.22 - LEMA. Sejam R um anel semiprimo livre de 2-torção e d uma derivação em R tal que $d^2=0$. Então $d=0$.

DEMONSTRAÇÃO. Sejam x e $y \in R$. Como $d^2=0$, temos:

$$0 = d^2(xy) = d^2(x)y + 2d(x)d(y) + xd^2(y) = 2d(x)d(y).$$

Mas R é livre de 2-torção; logo, $2d(x)d(y)=0$ implica $d(x)d(y)=0$ e concluímos que $d(R)^2=0$. Consequentemente, pela proposição 1.14, temos $d=0$.

//

1.23 COROLÁRIO. Sejam R um anel semiprimo livre de 2-torção e $a \in R$ tal que a comuta com $[a, r] \quad \forall r \in R$. Então $a \in Z(R)$.

DEMONSTRAÇÃO. Consideremos d a derivação interna dada por a . Como a comuta com $[a, r] \quad \forall r \in R$, então $d^2=0$ e, pelo lema acima, concluímos que $d=0$, isto é, $a \in Z(R)$.

//

1.24 COROLÁRIO. Sejam R anel semiprimo livre de 2-torção e U ideal de Lie de R tal que $U \not\subset Z(R)$. Então $[U, U] \neq 0$.

DEMONSTRAÇÃO. Seja $u \in U$ tal que $u \notin Z(R)$. Se $[u, U] = 0$ então $[u, [u, r]] = 0 \quad \forall r \in R$ e pelo lema 1.22 teríamos $u \in Z(R)$. Portanto, $0 \neq [u, U] \subset [U, U]$ e está demonstrado o corolário.

//

1.25 - LEMA. Sejam R anel semiprimo livre de 2-torção e U ideal de Lie de R que também é subanel de R . Se $U \not\subset Z(R)$ o subgrupo aditivo gerado por $R[U,U]R$ é um ideal não nulo de R que está contido em U .

DEMONSTRAÇÃO. Pelo corolário acima sabemos que $[U,U] \neq 0$ e, como R é semiprimo, $R[U,U]R \neq 0$. Vamos provar que $R[U,U]R \subset U$.

Sejam $u, v \in U$ e $r \in R$. Então.

$$[u,v]r + v[u,r] = [u, vr] \in U.$$

Como $[u,r] \in U$, $v \in U$ e U é subanel de R concluímos que $v[u,r] \in U$ e portanto $[u,v]r \in U$.

Tomemos agora s e $t \in R$. Sabemos que $[u,v]s \in U$, portanto $[[u,v]s, t] \in U$. Como ainda $[u,v]st \in U$ temos:

$$t[u,v]s = [u,v]st - [[u,v]s, t] \in U$$

e concluímos que $R[U,U]R \subset U$ o que demonstra o lema.

//

Acabamos de ver pelo lema 1.25, que se $U \not\subset Z(R)$ é ideal de Lie e subanel de R , U contém $M \neq 0$, um ideal de R . Decorre daí que $d(M) \subset d(U)$ e obtemos os mesmos resultados que temos para ideais de anéis primos:

(i) $d^3 \neq 0$ implica que $\overline{d(U)}$ contém ideal não nulo de R .

$$(ii) \ d^2 \neq 0 \text{ implica } C_R(d(U))=0.$$

$$(iii) \ d \neq 0 \text{ implica } \text{Anl}_e(d(U))=\text{Anl}_d(d(U))=0.$$

$$(iv) \ d(U)=0 \text{ implica } d=0.$$

Porém nem sempre um ideal de Lie é também subanel de R vamos construir, partindo de um ideal de Lie U , um ideal de Lie, $T(U)$, que é também subanel de R . Lançando mão deste novo ideal de Lie poderemos, usando o lema 1.25, chegar a conclusões sobre o comportamento de $d(U)$.

1.26 - DEFINIÇÃO. Seja U um ideal de Lie de um anel R . Denotaremos por $T(U)$ o subconjunto:

$$T(U)=\{x \in R/[x,R] \subset U\}.$$

É óbvio que $U \subset T(U)$ e, pela definição de $T(U)$, temos que $[T(U),R] \subset U \subset T(U)$. Ainda, como $T(U)$ é, claramente, um subgrupo aditivo de R , concluímos que $T(U)$ é ideal de Lie de R . Para provar que $T(U)$ é subanel de R basta observar que dados $u,v \in T(U)$ e $r \in R$ temos:

$$[uv,r]=[u,vr]+[v,ru] \in T(U).$$

Portanto $T(U)$ é fechado para o produto. Mostramos então o seguinte:

1.27 - LEMA. Sejam R um anel e U um ideal de Lie de R . Então $U \subset T(U)$ e $T(U)$ é simultaneamente ideal de Lie e sub

anel de R .

Para os resultados que seguem necessitaremos da hipótese R primo. Lembramos que se R é primo e $\text{car} R \neq 2$ então R é livre de 2-torção (teorema 0.1).

LEMA 1.28. Sejam R anel primo de característica diferente de dois e U ideal de Lie de R tal que $U \not\subset Z(R)$. Então M o ideal gerado por $R[U, U]R$ é não nulo, $[M, R] \subset U$ e $[M, R] \not\subset Z(R)$.

DEMONSTRAÇÃO. Pelo corolário 1.24, sabemos que $[U, U] \neq 0$ e como R é primo, $M \neq 0$. Consideremos agora $T(U)$. É óbvio que $T(U) \not\subset Z(R)$ uma vez que $U \subset T(U)$ e $U \not\subset Z(R)$. Podemos então utilizar o lema 1.25 para $T(U)$ e concluir que $R[T(U), T(U)]R \subset T(U)$ e, portanto, $R[U, U]R \subset R[T(U), T(U)]R \subset T(U)$. Logo, $M \subset T(U)$ e, pela definição de $T(U)$, temos $[M, R] \subset U$.

Resta provarmos que $[M, R] \not\subset Z(R)$. Suponhamos, por absurdo, que $[M, R] \subset Z(R)$. Então $\forall m \in M$ e $\forall r \in R$ temos que m comuta com $[m, r] \in Z(R)$, o que, pelo corolário 1.23 acarreta $M \subset Z(R)$. Ora, mas R é primo e $M \neq 0$ então $M \subset Z(R)$ implica R comutativo (teorema 0.1). Ainda, R comutativo implica $U \subset Z(R) = R$, o que é absurdo. Então $[M, R] \not\subset Z(R)$ e está demonstrado o lema.

//

1.29 - LEMA. Sejam R anel primo com $\text{car} R \neq 2$ e U ideal de Lie de R . Então:

(i) $[U, U] \subset Z(R)$ se e somente se $U \subset Z(R)$.

(ii) se $U \not\subset Z(R)$, $C_R(U) = Z(R)$.

(iii) $C_R(U) = C_R([U, U])$.

DEMONSTRAÇÃO. Primeiramente vamos provar (i). Se $U \subset Z(R)$, é óbvio que $[U, U] \subset U \subset Z(R)$.

Suponhamos agora $[U, U] \subset Z(R)$ e fixemos $u \in U$ qualquer. Dado $r \in R$ seja $\alpha(r) = [u, [u, r]] \in [U, U] \subset Z(R)$. Se $\alpha(r) = 0 \forall r \in R$, então pelo corolário 1.23, $u \in Z(R)$ e nada há a demonstrar. Suponhamos então $\alpha(r) \neq 0$ para algum $r \in R$. É claro que:

$$\alpha(r)u = [u, [u, r]]u = [u, [u, ru]] \in [U, U] \subset Z(R).$$

Logo, $\alpha(r)$ e $\alpha(r)u \in Z(R)$ e, conseqüentemente, $\forall x \in R$, temos:

$$0 = [\alpha(r)u, x] = \alpha(r)[u, x].$$

Ora, mas R é primo e portanto $Z(R)^*$ não tem divisores de zero; logo, da igualdade acima concluímos que $[u, x] = 0 \forall x \in R$, isto é, $u \in Z(R)$. Provamos então o item (i).

Para demonstrar (ii) primeiramente observamos que $C_R(U)$ é subanel de R . Mas é também verdade que $C_R(U)$ é ideal de Lie de R pois dado $a \in C_R(U)$ e $r \in R$ para qualquer $u \in U$ temos:

$$[[a, r], u] = [a, [r, u]] + [r, [u, a]] = 0,$$

pois $[r, u] \in U$ e $[u, a] = 0$. Logo, $[C_R(U), R] \subset C_R(U)$. Podemos então utilizar o lema 1.25 para $C_R(U)$ e concluir que $C_R(U) \subset Z(R)$ ou $C_R(U) \supset M \neq 0$ ideal de R . Mas $M \subset C_R(U)$ acarreta $U \subset C_R(M) = Z(R)$, pois R é primo (teorema 0.1). Concluímos que $U \not\subset Z(R)$ implica $C_R(U) \subset Z(R)$ e consequentemente $C_R(U) = Z(R)$.

O item (iii) decorre imediatamente dos itens (i) e (ii).

//

O próximo lema mostra que um ideal de Lie de um anel primo, que não está contido no centro do anel conserva de certa forma, a propriedade de ser primo do anel.

1.30 - LEMA. Sejam R um anel primo com $\text{car} R \neq 2$ e U ideal de Lie de R tal que $U \not\subset Z(R)$. Se a e $b \in R$ são tais que $aUb = 0$ então $a = 0$ ou $b = 0$.

DEMONSTRAÇÃO. Pelo lema 1.28 sabemos que existe M ideal não nulo de R tal que $[M, R] \subset U$ e $[M, R] \not\subset Z(R)$. Sejam $u \in U$, $m \in M$ e $r \in R$; então $[mau, r] \subset [M, R] \subset U$ e portanto

$$0 = a[mau, r]b = a[m, r]ub + a[ma, r]ub = a[ma, r]ub$$

já que $a[u, r]b = 0$. Portanto temos:

$$0 = a[ma, r]ub = amarub - armaub = amarub.$$

Concluimos que $aMaUb=0$ e portanto $a=0$ ou $Ub=0$. Se $Ub=0$ então dados $r \in R$ e $u \in U$ temos:

$$0 = [u, r]b = urb$$

e portanto $URb=0$ o que acarreta $b=0$.

//

Os lemas que demonstramos têm, em geral, a idéia de mostrar que um ideal de Lie $U \not\subset Z(R)$ conserva certas propriedades do anel primo R . Queremos agora mostrar o mesmo para $d(U)$.

Usaremos com frequência a seguinte igualdade envolvendo comutadores e derivações: dado R um anel, d uma derivação em R e x e $y \in R$ temos:

$$d([x, y]) = [d(x), y] + [x, d(y)],$$

mais geralmente, usando indução em n , é fácil mostrar que:

$$d^n([x, y]) = \sum_{i=0}^n [d^{n-i}(x), d^i(y)].$$

1.31 - LEMA. Sejam R um anel primo com $\text{car} R \neq 2$ e $d \neq 0$ uma derivação em R . Se U é um ideal e Lie de R tal que $d(U) \subset Z(R)$ então $U \subset Z(R)$.

DEMONSTRAÇÃO. Dados u e $v \in U$, como $d(u)$ e $d(v) \in Z(R)$, temos:

$$d([u, v]) = [d(u), v] + [u, d(v)] = 0.$$

Concluimos, então que

$$d([U,U])=0$$

Sejam agora $w \in [U,U]$ e $r \in R$; é claro que $[w,r] \in [U,U]$ e $d(w)=0$, portanto

$$0=d([w,r])=[w,d(r)].$$

Logo, $w \in C_R(d(R))$ e, pelo teorema 1.2, $C_R(d(R))=Z(R)$. Concluimos, então, que $[U,U] \subset Z(R)$.

Para finalizar a demonstração do lema, basta agora usar o lema 1.29 e concluir que $U \subset Z(R)$.

//

Vamos agora mostrar um resultado análogo ao teorema 1.10, no caso $n=1$, para ideais de Lie de um anel primo.

1.32 - TEOREMA. Sejam R um anel primo com $\text{car} R \neq 2$ e $U \not\subset Z(R)$ um ideal de Lie de R . Se $d \neq 0$ é uma derivação em R , então $\text{Anl}_e(d(U)) = \text{Anl}_d(d(U)) = 0$.

DEMONSTRAÇÃO. Sejam $a \in \text{Anl}_e(d(U))$, $u \in U$ e $r \in R$. Como $[u,r]u = [u,ru] \in U$, temos:

$$0 = ad([u,r]u) = ad([u,r])u + a[u,r]d(u) = a[u,r]d(u) \quad (1)$$

Sejam agora $v \in U$ e $s \in R$. Tomando, na igualdade (1),

$r=d(v)$ s obtemos:

$$0=a[u,d(v)s]d(u)=aud(v)sd(u)-ad(v)sud(u)=aud(v)sd(u)$$

já que $ad(v)=0$. Portanto $aud(U)Rd(u)=0$, o que implica que dado $u \in U$, temos $aud(U)=0$ ou $d(u)=0$. Se $d(u)=0$ então $\forall w \in U$ temos:

$$0=ad([u,w])=a[u,d(w)]=aud(w).$$

Logo, de qualquer forma obtemos $aud(U)=0 \forall u \in U$, isto é, $aUd(U)=0$.

Usando agora os lemas 1.30 e 1.31 concluímos que $a=0$ e portanto $Anl_e(d(U))=0$. A demonstração de que $Anl_d d(U)=0$ é análoga.

//

1.33 - NOTAÇÃO. Dado U , um ideal de Lie de R tal que $U \subset Z(R)$ é fácil ver que o subgrupo aditivo gerado por $[U,U]$, que denotaremos por V , é também ideal de Lie de R e $V \subset U$. Por abuso de notação, escreveremos $V=[U,U]$. A mesma observação vale para o ideal de Lie $W=[V,V] \subset V$.

Como $U \not\subset Z(R)$, o lema 1.29 nos garante que $V \not\subset Z(R)$ e $W \not\subset Z(R)$ desde que R seja primo com $\text{car} R \neq 2$.

Se d é uma derivação em R , é óbvio que

$$d([U,U]) \subset [d(U),U] + [U,d(U)] \subset U \cap d(U)$$

e portanto $d(V) \subset U \cap d(U)$. Analogamente, $d(W) \subset V \cap d(V)$.

Faremos uso frequente destes ideais de Lie e de suas propriedades nos lemas e teoremas que seguem.

O lema abaixo é um caso particular do teorema 1.42 que será provado mais adiante.

1.34 - LEMA. Sejam R um anel primo com $\text{car} R \neq 2$, U um ideal de Lie de R e $d \neq 0$ uma derivação em R . Se $d^2(U) = 0$ então $U \subset Z(R)$.

DEMONSTRAÇÃO. Suponhamos por absurdo que $U \not\subset Z(R)$. Vamos provar que $V = [U, U] \subset Z(R)$, o que, pelo lema 1.29, é uma contradição.

Ora, se $U \not\subset Z(R)$, pelo lema 1.28, existe $M \neq 0$, ideal de R tal que $[M, R] \subset U$ mas $[M, R] \not\subset Z(R)$. Sejam $m \in [M, R] \subset U \cap M$, $v \in V = [U, U]$ e $r \in R$. Como $[md(v), r] \in [M, R] \subset U$, $d(v) \in U$ e $[d(v), r] \in U$, temos:

$$0 = d^2(m) = d^2([m, r]) = d^2([d(v), r]) = d^2(v)$$

e portanto,

$$0 = d^2([md(v), r]) = d^2(m[d(v), r] + [m, r]d(v)) = 2d(m)d([d(v), r]).$$

Pelo teorema 0.1 R é livre de 2-torção e concluímos que

$$d([M, R])d([d(V), R]) = 0.$$

Por outro lado, o subgrupo aditivo gerado por $[M, R]$, que denotaremos por M' , é ideal de Lie de R (M' é ideal de R , então $M' \subset M$ e, conseqüentemente, $[M', R] \subset [M, R] \subset M'$). Ainda, como $[M, R] \not\subset Z(R)$ é óbvio que $M' \not\subset Z(R)$. Portanto, a igualdade do parágrafo anterior, $d([M, R])d([d(V), R])=0$, implica que $d(M')d([d(V), R])=0$, o que pelo teorema 1.32, acarreta $d([d(V), R])=0$.

Ora, mas $d([d(V), R])=[d(V), d(R)]$ pois $d^2(V)=0$. Logo, do parágrafo anterior, concluímos que $[d(V), d(R)]=0$, isto é, $d(V) \subset C_R(d(R))$. Ainda, pelo teorema 1.17, sabemos que $C_R(d(R))=Z(R)$ e portanto $d(V) \subset Z(R)$. Usando agora o lema 1.31, concluímos que $V \subset Z(R)$ que é um absurdo.

//

1.35 - COROLÁRIO. Sejam R um anel primo com $\text{car} R \neq 2$, U um ideal de Lie de R e $a \in R$ tal que $[a, [a, U]] = 0$. Então $a \in Z(R)$ ou $U \subset Z(R)$.

DEMONSTRAÇÃO. Basta aplicar o lema 1.34 para a derivação interna dada por a .

//

O teorema a seguir é o resultado esperado para $C_R(d(U))$.

1.36 - TEOREMA. Sejam R um anel primo com $\text{car} R \neq 2$, $U \not\subset Z(R)$ um ideal de Lie de R e $d \neq 0$ uma derivação de R . Então

$$C_R(d(U)) = Z(R).$$

DEMONSTRAÇÃO. Seja $a \in C_R(d(U))$. Provaremos o teorema em passos sucessivos demonstrando as seguintes afirmações:

Afirmção 1. $d(a) \in Z(R)$.

Dado $v \in V = [U, U]$ já observamos que $d(v) \in U \cap d(U)$;
Logo, $d^2(v) \in d(U)$ e temos:

$$0 = [a, d(v)] = [a, d^2(v)].$$

Portanto,

$$0 = d([a, d(v)]) = [d(a), d(v)],$$

isto é,

$$d(a) \in C_R(d(V)).$$

Ainda, $d([a, v]) = [d(a), v] \in d(V)$ e consequentemente $[d(a), [d(a), v]] = 0$. Utilizando o corolário 1.35 temos $d(a) \in Z(R)$ uma vez que o lema 1.29 nos garante $V \not\subset Z(R)$.

Afirmção 2. $d(a) = 0$ ou $a \in Z(R)$.

Pelo lema 1.28 sabemos que existe $M \neq 0$ ideal de R tal que $[M, R] \subset U$ mas $[M, R] \not\subset Z(R)$. Seja $m \in [M, R] \subset U \cap M$. Então $am \in M$ e $a[m, a] = [am, a] \in [M, R] \subset U$. Ainda, $d(a)[m, a] =$

$d([am,a]) \in d(U)$ uma vez que $d(a) \in Z(R)$ e $d(m) \in d(U)$ implicam $d([m,a])=0$. Portanto,

$$0 = [d(a)[m,a], a] = d(a)[[m,a], a]. \quad (1)$$

Como $d(a) \in Z(R)$, e $Z(R)^*$ não tem divisores de zero pois R é primo, da igualdade (1) concluímos que $d(a)=0$ ou $[[m,a], a]=0$ para todo $m \in [M, R]$. Logo, $d(a)=0$ ou $[[M', a], a]=0$ onde M' é o subgrupo aditivo gerado por $[M, R]$. Mas já vimos, na demonstração do lema 1.34 que M' é ideal de Lie não central de R ; portanto, $[[M', a], a]=0$ acarreta, pelo corolário 1.35, $a \in Z(R)$.

Concluimos então que $d(a)=0$ $a \in Z(R)$ e está provada a afirmação 2.

A seguinte afirmação finaliza a demonstração do teorema.

Afirmação 3. Se $d(a)=0$ então $a \in Z(R)$.

Dados u e $v \in U$ temos: $u[a, v] + [u, v]a = [ua, v] \in U$ e $d([ua, v]) = d(u)[a, v] + d([u, v])a$ pois $d(a) = d([a, v]) = 0$. Logo,

$$0 = [a, d(u)[a, v] + d([u, v])a] = d(u)[a, [a, v]]$$

pois $[a, d(u)] = [a, d([u, v])a] = 0$. Concluimos, então que

$$d(U)[a, [a, U]] = 0.$$

Usando o teorema 1.32, temos então $[a, [a, U]] = 0$, o que pelo corolário 1.35 implica $a \in Z(R)$.

//

Vamos agora considerar $\overline{d(U)}$ o subanel de R gerado por $d(U)$. Já vimos que Herstein provou que se $d^3 \neq 0$, $\overline{d(R)}$ contém ideal não nulo de R . Mostraremos aqui, que este é também o caso de $\overline{d(U)}$ desde que R seja primo com $\text{car} R \neq 2$.

1.37 - LEMA. Seja R anel primo com $\text{car} R \neq 2$ e U ideal de Lie de R , $U \not\subseteq Z(R)$. Se d é uma derivação de R com $d^3(U)=0$ então $d^3=0$.

DEMONSTRAÇÃO. Ao longo desta demonstração usaremos os ideais de Lie $V=[U,U]$ e $W=[V,V]$ que o lema 1.29 garante serem não centrais. Também faremos uso da fórmula

$$d^n([r,s]) = \sum_{i=0}^n \binom{n}{i} [d^{n-i}(r), d^i(s)] \quad \forall r,s \in R.$$

Decorre do lema 1.34 que $d^2(U)=0$ implica $d=0$ e neste caso nada teríamos a demonstrar. Podemos então supor $d^2(U) \neq 0$.

Dividiremos a demonstração em sucessivas afirmações:

Afirmção 1. $d^4(R) \subseteq Z(R)$.

Como $d^2(W) \subseteq d(V) \subseteq U$, é óbvio que $[d^2(W), R] \subseteq U$. Ainda, com o fato de que $d^3(W) \subseteq d^3(V) \subseteq d^3(U)=0$, temos:

$$0 = d^3([d^2(w), r]) = [d^2(w), d^3(r)] \quad \forall r \in R \text{ e } \forall w \in V.$$

Mas $d(W) \subset U$, e portanto, $[d(W), R] \subset U$. Logo, $\forall r \in R$ e $\forall w \in W$ temos:

$$0 = d^3([d(w), r]) = 4[d^2(w), d^3(r)] + [d(w), d^4(r)] = [d(w), d^4(r)].$$

Concluimos então que $d^4(R) \subset C_R(d(W))$ e, portanto, decorre do teorema 1.36 que $d^4(R) \subset Z(R)$, o que demonstra a afirmação 1.

Afirmção 2. $d^3(R) \subset Z(R)$.

Tomando $u \in U$ e $r \in R$, como $d^3(U) = 0$ e $d^4(R) \subset Z(R)$, temos:

$$0 = d^3([u, d(r)]) = 3[d^2(u), d^2(r)] + 3[d(u), d^3(r)]$$

e,

$$0 = d^4([u, r]) = 6[d^2(u), d^2(r)] + 4[d(u), d^3(r)].$$

Multiplicando a primeira igualdade por 2 e subtraindo a segunda, concluimos que: $2[d(U), d^3(R)] = 0$. Ainda, do fato de R ser primo com $\text{car} R \neq 2$, sabemos que R é livre de 2-torção e portanto $[d(U), d^3(R)] = 0$, isto é, $d^3(R) \subset C_R(d(U))$. Para finalizar usamos novamente o teorema 1.36 e concluimos que $d^3(R) \subset Z(R)$.

Afirmção 3. $d^3 = 0$ ou $d^2(U) \subset Z(R)$.

De fato, decorre da afirmação anterior que

$d^3(Rd^2(U)) = d^3(R)d^2(U) \subset Z(R)$ e $d^3(R) \subset Z(R)$. Consequentemente,

$$0 = [d^3(R)d^2(U), R] = d^3(R)[d^2(U), R].$$

Como R é primo, $Z(R)^*$ não tem divisores de zero e, da igualdade acima, concluímos que $d^3=0$ ou $d^2(U) \subset Z(R)$, provando a afirmação 3.

Esta última afirmação finaliza a demonstração do teorema.

Afirmação 4. $d^2(U) \subset Z(R)$ implica $d^3=0$.

De fato, decorre da afirmação 1, que $d^4(Rd(U)) \subset Z(R)$ e portanto, para todo $r \in R$ e $u \in R$ temos:

$$d^4(rd(u)) = d^4(r)d(u) + 4d^3(r)d^2(u) \in Z(R). \quad (1)$$

Por outro lado, como $d^2(U) \subset Z(R)$, da afirmação 2, concluímos que $d^3(R)d^2(U) \subset Z(R)$. Logo, de (1), temos que $d^4(R)d(U) \subset Z(R)$. Neste caso, como $d^4(R) \subset Z(R)$, obtemos:

$$0 = [d^4(R)d(U), R] = d^4(R)[d(U), R]$$

e, como $Z(R)^*$ não tem divisores de zero, concluímos que $d(U) \subset Z(R)$ ou $d^4=0$; portanto, o lema 1.31 nos dá $d^4=0$.

Ora, mas se $d^4=0$, então:

$$0 = d^4(rd(u)) = 4d^3(r)d^2(u) \quad \forall r \in R \text{ e } \forall u \in U$$

e, como R é livre de 2-torção, concluímos que $d^3(R)d^2(U)=0$. Ainda, $Z(R)^*$ não tem divisores de zero, e $0 \neq d^2(U) \subset Z(R)$ implicam $d^3=0$, concluindo a demonstração do lema.

//

1.38 - LEMA. Sejam R anel primo com $\text{car} R \neq 2$, $U \not\subset Z(R)$ ideal de Lie de R e d uma derivação de R . Se $d^2(U)^2=0$ então $d^3=0$.

DEMONSTRAÇÃO. Já foi dito que os ideais de Lie $V=[U,U]$ e $W=[V,V]$ são não centrais, que $d(V) \subset U$ e que $d^2(W) \subset d(V) \subset U$. Primeiramente vamos mostrar que $d^4(W)=0$.

Sejam u, v e $w \in W$. Como $d^2(U)^2=0$, temos:

$$0 = d^2(u)d^2([d(v), d^2(w)]) = d^2(u)[d(v), d^4(w)] = d^2(u)d(v)d^4(w),$$

isto é, $0 = d^2(w)d(W)d^4(W)$. (1)

Por outro lado,

$$\begin{aligned} d^2([v, d(w)])d^4(u) &= \\ &= ([d^2(v), d(w)] + 2[d(v), d^2(w)] + [v, d^3(w)])d^4(u) = \\ &= d^2(v)d(w)d^4(u) - 2d^2(w)d(v)d^4(u) - d^3(w)vd^4(u), \end{aligned}$$

que pela igualdade (1) implica $d^3(w)wd^4(W)=0$. Então o lema 1.30 nos dá $d^4(W)=0$.

Ora, mas se $d^4(W)=0$, dados u, v e $w \in W$ temos:

$d^2([d^2(w), v]) = 2[d^3(w), d(v)]$ e portanto,

$$0 = d^2(u)d^2([d^2(w), v]) = -2d^2(u)d(v)d^3(w).$$

Ainda, como R é livre de 2-torção, concluímos que:

$$d^2(w)d(w)d^3(w)=0.$$

Por outro lado,

$$\begin{aligned} 0 &= d^2([u, d(v)])d^3(w) = \\ &= ([d^2(u), d(v)] + 2[d(u), d^2(v)] + [u, d^3(v)])d^3(w) = \\ &= d^2(u)d(v)d^3(w) - 2d^2(v)d(u)d^3(w) - d^3(v)ud^3(w), \end{aligned}$$

que pela igualdade (2) implica $d^3(w)wd^3(w)=0$. Utilizando agora os lemas 1.30 e 1.37 demonstraremos que $d^3=0$.

//

1.39 - LEMA. Sejam R anel primo com $\text{car} R \neq 2$, $U \not\subseteq Z(R)$ ideal de Lie de R e d uma derivação de R . Se $d^3 \neq 0$ e se $\overline{d(V)}$ contém ρ , um ideal à direita não nulo, e também contém λ , um ideal à esquerda não nulo, então $\overline{d(U)}$ contém um ideal não nulo de R .

DEMONSTRAÇÃO. Como $V=[U,U] \subset U$ e $d(V) \subset U \cap d(U)$, dados u e $v \in V$ temos que

$$d(d(u)d(v)) = d(d(u))d(v) + d(u)d(d(v)) \in \overline{d(U)}$$

e concluímos que $d(\overline{d(V)}) \subset \overline{d(U)}$:

Sejam $a \in \lambda$ e $r \in R$. Como $ra \in \overline{d(V)}$, temos:

$$d(r)a + rd(a) = d(ra) \in d(\overline{d(V)}) \subset \overline{d(U)}.$$

Mas $d(r)a \in \lambda \subset \overline{d(U)}$, logo $Rd(\lambda) \subset \overline{d(U)}$. Analogamente, $d(\rho)R \subset \overline{d(U)}$.

Dados $a \in \lambda$ e $v \in V$, obtemos:

$$d(a)v - vd(a) + ad(v) - d(v)a = d([a, v]) \in d(V) \subset d(U).$$

Mas $vd(a) \in Rd(\lambda) \subset \overline{d(U)}$, $ad(v) \in \lambda d(V) \subset \overline{d(U)}$ e $d(v)a \in \lambda \subset \overline{d(U)}$, então $d(\lambda)V \subset \overline{d(U)}$. Analogamente, $Vd(\rho) \subset \overline{d(U)}$.

Seja agora o ideal $I = \lambda V \rho$. O lema 1.30 nos garante que $I \neq 0$. Além disto, $d(I) \subset d(\lambda)V\rho + \lambda d(V)\rho + \lambda Vd(\rho) \subset \overline{d(U)}\rho + \overline{d(V)} + \lambda \overline{d(U)} \subset \overline{d(U)}$. Então $\overline{d(I)} \subset \overline{d(U)}$ e, pelo teorema 1.16, concluímos que $\overline{d(U)}$ contém ideal não nulo R .

//

Este lema mostra que, se $\overline{d(V)}$ contém ideal à esquerda não nulo e contém ideal à direita não nulo então $\overline{d(U)}$ contém ideal não nulo de R . Resta sabermos o que ocorre no caso em que $\overline{d(V)}$ não contém ideal à esquerda não nulo ou $\overline{d(V)}$ não contém ideal à direita não nulo.

O próximo lema nos dá uma informação sobre como obter ideais laterais em $\overline{d(V)}$.

1.40 LEMA. Sejam R um anel primo com $\text{car} R \neq 2$, $V \not\subset Z(R)$ um ideal de Lie de R e $d \neq 0$ uma derivação em R . Se $c \in R$ e I é um ideal de R tal que $[c, I] \subset \overline{d(V)}$ então $[c, d(V)]I \subset \overline{d(V)}$ e $I[c, d(V)] \subset \overline{d(V)}$.

DEMONSTRAÇÃO. Mostraremos que $[c, d(V)]I \subset \overline{d(V)}$. A demonstração de que $I[c, d(V)] \subset \overline{d(V)}$ é análoga.

Sejam $a \in I$ e $v \in V$. Então temos:

$$[c, d(v)]a + d(v)[c, a] = [c, d(v)a] \in [c, I] \subset \overline{d(V)}.$$

Como $d(v)[c, a] \in d(V)[c, I] \subset \overline{d(V)}$, da igualdade acima, concluímos que $[c, d(v)]a \in \overline{d(V)}$, isto é, $[c, d(V)]I \subset \overline{d(V)}$.

//

1.41 TEOREMA. Sejam R anel primo com $\text{car} R \neq 2$ e $U \not\subset Z(R)$ ideal de Lie de R . Seja ainda d uma derivação em R tal que $d^3 \neq 0$. Então $\overline{d(U)}$ contém um ideal não nulo de R .

DEMONSTRAÇÃO. Vamos utilizar os ideais de Lie não centrais $V = [U, U]$, $W = [V, V]$ e $[W, W]$. Pelo lema 1.39, sabemos que basta mostrar que $\overline{d(V)}$ contém um ideal à esquerda não nulo de R e um ideal à direita não nulo de R . Suponhamos por absurdo que $\overline{d(V)}$ não contenha um ideal à direita não nulo de R . Provaremos duas afirmações e chegaremos a um absurdo.

Afirmação 1. $d^2([W, W])^2 \subset Z(R)$.

Seja $w \in [W, W]$ e $r \in R$. É claro que $d(w) \in W \cap d(W) \subset V \cap d(V)$ e $d^2(w) \in V \cap d(V)$. Além disto, para todo $r \in R$,

$$d(w)[d(w), r] = [d(w), d(w)r] \in V$$

e portanto,

$$d(d(w)[d(w),r]) = d^2(w)[d(w),r] + d(w)d([d(w),r]) \in d(V).$$

Como $d(w)d([d(w),r]) \in \overline{d(V)}$ concluímos que:

$$d^2(w)[d(w),R] \subset \overline{d(V)}. \quad (1)$$

Ainda, $d^2(w)d([d(w),r]) \in \overline{d(V)}$, isto é, $d^2(w)[d^2(w),r] + d^2(w)[d(w),d(r)] \in \overline{d(V)}$. Mas, de (1), sabemos que $d^2(w)[d(w),d(r)] \in \overline{d(V)}$, portanto:

$$d^2(w)[d^2(w),R] \subset \overline{d(V)} \quad (2)$$

Tomando $t \in [W,W]$ e, utilizando (2) para $w+t$, w e t finalmente obtemos que para todo $r \in R$,

$$d^2(t)[d^2(w),r] + d^2(w)[d^2(t),r] \in \overline{d(V)}. \quad (3)$$

Por outro lado, se $v \in V$, então $[d(w),v] \in V$ e $d([d(w),v]) = [d^2(w),v] + [d(w),d(v)] \in \overline{d(V)}$. Como $[d(w),d(v)] \in \overline{d(V)}$, concluimos que:

$$[d^2(w),V] \subset \overline{d(V)}. \quad (4)$$

Portanto, para $t \in [W,W]$, como $d(t) \in W$, $d^2(t) \in V$ e portanto:

$$[d^2(w),[d^2(t),r]] \in \overline{d(V)} \quad \forall r \in R. \quad (5)$$

De (5) e (3) concluímos que para todo $r \in R$,

$$d^2(t)[d^2(w),r] + d^2(w)[d^2(t),r] - [d^2(w),[d^2(t),r]] \in \overline{d(V)},$$

isto é,

$$d^2(t)[d^2(w),r] + [d^2(t),r]d^2(w) = [d^2(t)d^2(w),r] \in \overline{d(V)}.$$

Portanto, temos $[d^2([W,W])^2, R] \subset \overline{d(V)}$. Finalmente, utilizando o lema 1.40, temos que $d^2([W,W])^2, d(V) \subset \overline{d(V)}$.

Ora, mas $\overline{d(V)}$ não contém ideal à direita não nulo de R , portanto, $[d^2([W,W])^2, d(V)] = 0$, isto é, $d^2([W,W])^2 \subset C_R(d(V)) = Z(R)$, e concluímos a demonstração da afirmação 1.

Afirmção 2. $d([W,W]) \subset Z(R)$.

Como $d^3 \neq 0$, decorre do lema 1.38, que $d^2([W,W])^2 \neq 0$. Fixemos w e $t \in [W,W]$ tais que $\alpha = d^2(w)d^2(t) \neq 0$. Já que $d^2(w) \in d(V)$, de (1), obtemos:

$$\alpha[d(t), R] = d^2(w)d^2(t)[d(t), R] \subset \overline{d(V)}.$$

Mas, pela afirmação 1, sabemos que $\alpha \in Z(R)^*$, portanto, $[d(t), \alpha R] = \alpha[d(t), R] \subset \overline{d(V)}$ e αR é ideal não nulo de R . O lema 1.40 acarreta, então, $[d(t), d(V)]\alpha R \subset \overline{d(V)}$. Como $\overline{d(V)}$ não contém ideal à direita não nulo de R e $\alpha R \neq 0$, concluímos que $d(t) \in C_R(d(V)) = Z(R)$ e portanto $d^2(t) \in d(Z(R)) \subset Z(R)$.

Seja agora $v \in [W,W]$ qualquer. Se $d^2(t)d^2(v) \neq 0$ usando o mesmo raciocínio do parágrafo anterior, provamos que $d(v) \in Z(R)$. Por outro lado, se $d^2(t)d^2(v) = 0$ então $d^2(t)d^2(v+t) = d^2(t)^2 \neq 0$ pois $d^2(t) \in Z(R)^*$. Novamente, usando o mesmo raciocínio do parágrafo anterior, concluímos que $d(v+t) \in Z(R)$. Ora, mas $d(v+t) = d(v) + d(t)$ e, como $d(t) \in Z(R)$, temos que $d(v) \in Z(R)$. Provamos, então a afirmação 2.

A afirmação 2 e o lema 1.31 levam a um absurdo que vem do fato de termos suposto que $\overline{d(V)}$ não contém ideal à direita não nulo de R .

Se supusermos que $\overline{d(V)}$ não contém ideal à esquerda não nulo de R , provamos de forma análoga, a afirmação 1 e a afirmação 2 chegando a um absurdo.

Concluimos, portanto, que $\overline{d(V)}$ contém ideal à esquerda não nulo de R e $\overline{d(V)}$ contém ideal à direita não nulo de R , provando o teorema.

//

O teorema a seguir é uma generalização do teorema 1.20, item (i), para ideais de Lie. É fácil ver que o teorema 1.36 é uma consequência imediata deste.

1.42 - TEOREMA. Sejam R um anel primo com $\text{car} R \neq 2$ e $U \not\subseteq Z(R)$ um ideal de Lie de R . Se δ e d são derivações de R tais que a composta $(\delta, d)(U) = 0$ então $\delta = 0$ ou $d = 0$.

DEMONSTRAÇÃO. Suponhamos que $\delta \neq 0$. Se $u \in U$ e $v \in V = [U, U] \subset U$, então $d(v) \in U$ e $0 = (\delta, d)(u) = (\delta, d)(v) = (\delta, d)(d(v))$; portanto $0 = (\delta, d)([u, d(v)]) = [\delta(u), d^2(v)]$ e concluímos que $d^2(V) \subset C_R(\delta(U))$. Como $\delta \neq 0$, o teorema 1.36 implica que $d^2(V) \subset Z(R)$. Neste caso, dado $r \in R$ e $v \in V$ temos: $0 = (\delta, d)([d(v), r]) = \delta([d(v), d(r)]) = [d(v), (\delta \circ d)(r)]$. Novamente, pelo teorema 1.36, concluímos que $d = 0$ ou $(\delta \circ d)(R) \subset Z(R)$.

Se $(\delta, d)(R) \subset Z(R)$, então, dados $v \in V$ e $u \in U$ temos:

$$d^2(v)\delta(u) = \delta(d^2(v)u + d(v)d(u)) = (\delta, d)(d(v)u) \in Z(R).$$

Mas, do parágrafo anterior, sabemos que $d^2(v) \in Z(R)$. Portanto, $\forall r \in R$ $0 = [d^2(v)\delta(u), r] = d^2(v)[\delta(u), r]$ e, como $Z(R)^*$ não tem divisores de zero, concluímos que $d^2(v) = 0$ ou $\delta(u) \in Z(R)$. Finalmente, o lema 1.31 nos garante que $\delta(U) \not\subset Z(R)$. Logo, $d^2(V) = 0$ o que, pelo lema 1.34, implica $d = 0$.

//

Para demonstrar o teorema 1.36, dado $a \in {}_R(d(U))$ basta tomar δ a derivação interna dada por a . Então $(\delta, d)(U) = 0$ e o teorema 1.42 implica $d = 0$ ou $\delta = 0$; isto é, $d = 0$ ou $a \in Z(R)$.

CAPÍTULO II

Em [H.7], I.N.Herstein define o hipercentro de um anel R .

2.1 - DEFINIÇÃO. Seja R um anel, o hipercentro de R é $T(R) = \{a \in R \mid \forall x \in R, \exists n = n(a, x) \geq 1 \text{ com } ax^n = x^n a\}$.

Neste mesmo trabalho, ele mostra que se R é um anel sem ideais nil não nulos então $T(R) = Z(R)$; em termos de derivação temos que se d , a derivação interna dada por a é tal que para todos $x \in R$, existe $n = n(x) \geq 1$ com $d(x^n) = 0$ então $d = 0$. Surge, então, a questão: se R não tem ideais nil e d é uma derivação qualquer tal que para todo $x \in R$ existe $n = n(x) \geq 1$ com $d(x^n) = 0$, podemos concluir que $d = 0$ ou R é, de alguma forma, especial?

Um exemplo fácil mostra que não podemos esperar que d seja sempre a derivação nula, basta tomar R um domínio comutativo de característica $p > 0$ e d a derivação usual no anel de polinômios $R[x]$. Neste caso para todo $f \in R[x]$, $d(f^p) = 0$ mas $d \neq 0$.

Em [F.2], B.Felzenswalb demonstra que se R é primitivo e $d \neq 0$ é uma derivação de R com a propriedade acima então ou $d = 0$ ou R é um corpo infinito de característica $p \neq 0$ e se $d(x) \neq 0$ então $p/n(x)$. É demonstrado neste mesmo trabalho que se R é apenas primo mas o conjunto de inteiros $n(x)$ é limitado então R é um domínio comutativo infinito de característica $p \neq 0$ e $d(x) \neq 0$ implica $p/n(x)$.

Mais tarde, em [F.3], B.Felzenswalb e A.Giambruno respondem afirmativamente à questão provando que se R é um anel primo sem ideais nil e d é uma derivação de R tal que para todo $x \in R$, existe um inteiro $n=n(x)>0$ com $d(x^n)=0$, então $d=0$ ou R é um domínio comutativo infinito de características $p \neq 0$ e $p/n(x)$ se $d(x) \neq 0$.

Faremos aqui diretamente a demonstração, que aparece em [F.3], deste último resultado. Mostraremos, em seguida, que os dois outros antes mencionados, são na realidade, consequências deste.

Na segunda parte deste capítulo estudaremos uma derivação d em um anel R , tal que $d(x)$ é nilpotente para todo $x \in R$. Uma tal derivação será dita derivação nil em R . Fixemos esta notação na seguinte definição:

2.2 - DEFINIÇÃO. Sejam R um anel, A um subconjunto de R e d uma derivação em R . Diremos que d é uma derivação nil em A se $d(a)$ é nilpotente para todo elemento $a \in A$.

Se existe $n \geq 1$, um inteiro fixo, tal que $d(a)^n = 0$ para todo $a \in A$, diremos que d é uma derivação nil em A de índice limitado.

Um primeiro resultado neste contexto foi feito por I.N.Herstein, em [H.3], onde é provado que se R é um anel primo e d é uma derivação interna, nil de índice limitado, em R então $d=0$. Generalizando este resultado para derivações quaisquer, A.Giambruno e o próprio Herstein provaram, em [G.1], que se R é um anel semiprimo e d é uma deriva

ção nil de índice limitado em R , então $d=0$.

Mais tarde, em [F.4], B.Felzenswalb e C.Lanski generalizam o resultado acima e demonstram o seguinte teorema:

TEOREMA. Sejam R um anel sem ideal à direita nil não nulo, $I \neq 0$ um ideal de R e d uma derivação em R que é nil em I . Então $d(I)=0$.

No final deste artigo, Felzenswalb e Lanski demonstram alguns casos especiais, entre os quais está incluído o caso estudado por Giambruno e Herstein.

Faremos aqui a demonstração deste teorema incluindo o resultado de Giambruno e Herstein.

Iniciaremos, portanto, com o seguinte resultado: sejam R um anel primo sem ideal nil não nulo e $d \neq 0$ uma derivação de R tal que para todo $x \in R$ existe $n=n(x) \geq 1$ com $d(x^n)=0$. Então R é um domínio comutativo infinito de característica $p > 0$ e se $d(x) \neq 0$ então $p/n(x)$.

Primeiramente vamos mostrar através de um exemplo que a hipótese R primo no resultado acima é necessária. Tomemos R um domínio comutativo de característica $p \neq 0$. Consideremos o anel semiprimo $A=R[x] \oplus R[x]$. É fácil ver que A não tem ideal nil não nulo. Se tomarmos, em A , a derivação $d(f,g)=(f',0)$ onde f' indica a derivada usual do polinômio

f , é claro que $d((f,g)^p) = d(f^p, g^p) = (pf^{p-1}f', 0) = 0 \quad \forall (f,g) \in A$.

Faremos agora um lema e, a seguir, a demonstração do teorema de Felzenswalb e Giambruno.

2.3 - LEMA. Sejam R um anel primo, $d \neq 0$ uma derivação e I um ideal não nulo de R . Se $[a, d(a)] = 0$ para todo $a \in I$ então R é comutativo.

DEMONSTRAÇÃO. Sejam $a, b \in I$. Como $[a, d(a)] = [b, d(b)] = [a+b, d(a+b)] = 0$ concluimos que

$$[a, d(b)] + [b, d(a)] = 0 \quad (1)$$

Substituindo, em (1), b por ab obtemos:

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

Porém $[a, d(a)] = a([a, d(b)] + [b, d(a)]) = 0$ portanto, de (2) obtemos:

$$d(a)[a, b] = 0 \quad \forall a, b \in I \quad (3)$$

Fixado $a \in I$ seja d_a a derivação interna dada por a . Então de (3) temos: $d(a)d_a(I) = 0$ e pelo lema 1.8 sabemos que $d_a = 0$ ou $d(a) = 0$, isto é, $\forall a \in I$ temos que $a \in Z(R)$ ou $d(a) = 0$. Como $d \neq 0$, sabemos que $d(I) \neq 0$ (lema 1.8) e portanto existe $a \in I$ tal que $d(a) \neq 0$. Então $a \in Z(R)$ e dado $b \in I$, $d(b) = 0$ implica $d(a+b) = d(a) + d(b) = d(a) \neq 0$ o que obriga $a+b \in Z(R)$. Mas como

$a \in Z(R)$ temos $b \in Z(R)$. Provamos então que $I \subseteq Z(R)$ e, como R é primo, temos R comutativo.

//

2.4 - TEOREMA. Sejam R um anel primo sem ideal nil não nulo e $d \neq 0$ uma derivação de R tal que para todo $x \in R$ existe $n=n(x) \geq 1$ com $d(x^n)=0$. Então R é um domínio comutativo infinito de característica $p > 0$ e se $d(x) \neq 0$ então $p/n(x)$.

DEMONSTRAÇÃO. Primeiramente observamos que é suficiente provar que R é comutativo. De fato, se R é comutativo, como R é primo, R é um domínio. Ainda, para todo $x \in R$ temos $d(x^k) = kx^{k-1}d(x)$ para todo $k > 1$. Como $d \neq 0$, existe $a \in R$ tal que $d(a) \neq 0$; então existe $n=n(a) > 1$ tal que $d(a^n) = na^{n-1}d(a) = 0$ e $d(a^{n-1}) \neq 0$. Como R é um domínio, $a^{n-1} \neq 0$ e $d(a) \neq 0$, então $a^{n-1}d(a) \neq 0$. Logo, de $na^{n-1}d(a) = 0$ temos $nRa^{n-1}d(a) = 0$ e deduzimos que $nR = 0$. Concluimos, então que $\text{car} R = p > 0$ e $p/n(a)$. Resta verificar que R é infinito. Se R , domínio comutativo, é finito então R é um corpo finito; como todo corpo finito é perfeito teríamos $R = R^p$ e portanto $d(R) = d(R^p) = 0$, o que é absurdo. Portanto R é domínio comutativo infinito.

Observamos ainda que, dados x e $y \in R$, se $n(x)=n$ e $n(y)=m$, então $d(x^{nm}) = d(y^{nm}) = 0$. Portanto, dados x e $y \in R$ existe $k=k(x,y) \geq 1$ tal que $d(x^k) = d(y^k) = 0$.

Para provarmos que R é comutativo começaremos considerando o caso em que R não é semi-simples, isto é, $J(R)$, o radical de Jacobson de R é não nulo. Vamos mostrar que para todo $x \in J(R)$ temos $[x, d(x)] = 0$ e, usando o lema 2.3, con

cluír que R é comutativo.

Sabemos que, se $x \in J(R)$ então x é um elemento quse regular de R , isto é, existe $x' \in R$ tal que $x+x'+xx'=0$ e $xx'=x'x$. Dado $a \in R$, denotaremos por $a(1+x)$ o elemento $a+ax \in R$ e, por $(1+x)a$, o elemento $a+xa \in R$. É fácil ver que $(1+x)(1+x')a = a(1+x)(1+x') = a$. Denotaremos então $(1+x')a$ por $(1+x)^{-1}a$ e $a(1+x')$ por $a(1+x)^{-1}$.

Fixemos $x \in J(R)$. Dado $r \in R$ qualquer, pela observação do segundo parágrafo, podemos escolher $n \geq 1$ tal que:

$$d((1+x)^{-1}r(1+x))^n = d(r^n) = 0$$

Mas $((1+x)^{-1}r(1+x))^n = (1+x)^{-1}r^n(1+x)$ e portanto:

$$d((1+x)^{-1}r^n(1+x)) = d(r^n) = 0$$

Então temos também:

$$d((1+x)(1+x)^{-1}r^n(1+x)) = d(r^n + r^n x) = r^n d(x) \quad (1)$$

e, por outro lado,

$$\begin{aligned} d((1+x)(1+x)^{-1}r^n(1+x)) &= d((1+x)^{-1}r^n(1+x)) + \\ &+ d(x(1+x)^{-1}r^n(1+x)) = d(x)(1+x)^{-1}r^n(1+x) \end{aligned} \quad (2)$$

Comparando (1) e (2), concluímos que:

$$d(x)(1+x)^{-1}r^n(1+x) = r^n d(x)$$

e, multiplicando à direita ambos os membros da igualdade por $(1+x)^{-1}$, concluímos que $[d(x)(1+x)^{-1}, r^n] = 0$. Portanto, dado $r \in R$, existe $n \geq 1$, que depende de r , tal que $d(x)(1+x)^{-1}$ comuta com r^n . Logo $d(x)(1+x)^{-1}$ pertence a $T(R)$, o hipercentro de R , e como R não tem ideais nil não nulos, temos que $T(R) = Z(R)$ e portanto, $d(x)(1+x)^{-1} \in Z(R)$. Em particular temos:

$$d(x)(1+x)^{-1}x = xd(x)(1+x)^{-1};$$

mas como x e $(1+x)^{-1}$ comutam deduzimos que

$$d(x)x = xd(x) \quad \forall x \in J(R),$$

que é o que queríamos demonstrar.

Suponhamos agora que R é semisimples, isto é, $J(R) = 0$. Primeiramente vamos mostrar que R é um domínio. Seja $0 \neq a \in R$. Consideremos $L = \text{Anl}_e(a) = \{x \in R / xa = 0\}$. Dados $x \in L$ e $r \in R$ sabemos que existe um inteiro $n \geq 1$ tal que:

$$d((ar+arx)^n) = d((ar)^n) = 0 \quad (1)$$

Mas $(ar+arx)^n = (ar)^n + (ar)^{n-1}arx = (ar)^n + (ar)^n x$ pois $(arx)^2 = (arx)ar = 0$. Então, de (1), temos:

$$0 = d((ar+arx)^n) = (ar)^n d(x) \quad (2)$$

Pelo teorema 0.7 e pelo fato de R ser semisimples, a igualdade (2) implica que $aRd(L) = 0$. Como R é primo, e $a \neq 0$ concluímos que $d(L) = 0$. E portanto, do capítulo 1 temos que $L = 0$ uma vez que $d \neq 0$. Logo, R é um domínio.

Como no caso anterior, vamos agora mostrar que $d(x)x = xd(x) \quad \forall x \in R$ e usar o lema 2.3 para concluir que R é comutativo. Fixemos $x \in R$, $x \neq 0$ e seja $n = n(x) \geq 1$ tal que $d(x^n) = 0$. Vamos trabalhar com o subanel de R , $A = C_R(x^n)$, o centralizador em R de x^n . Se $a \in A$, então $[a, x^n] = 0$ e consequentemente $d([a, x^n]) = [d(a), x^n] = 0$, ou seja, $d(A) \subset A$. Portanto o anel A é um domínio (pois R o é) e d é uma derivação em A . É claro que $Z(A) \neq 0$ pois $x^n \in Z(A)$. Consideremos então o localizado de A em $Z(A)^*$, que denotaremos A_Z . Sabemos que A_Z é um domínio, $A \subset A_Z$ e $Z(A_Z)$ é um corpo. Além disto, $x^n \in Z(A_Z)$, portanto x^n é inversível em A_Z e consequentemente x é inversível em A_Z . Já vimos no capítulo 0, que d pode ser estendida à uma derivação em A_Z (que também será denotada por d), dada por:

$$d(az^{-1}) = d(a)z^{-1} - ad(z)z^{-2} \quad \forall a \in A \quad \forall z \in Z(A)^*.$$

A hipótese sobre d em R estende-se para d em A_Z pois dados $a \in A$ e $z \in Z(A)^*$ existe $m \geq 1$ tal que $d(a^m) = d(z^m) = 0$. Então:

$$d((az^{-1})^m) = d(a^m z^{-m}) = d(a^m)z^{-m} - a^m d(z^m)z^{-2m} = 0$$

Da mesma forma que foi feito para d em R , fica claro que, dados $q_1, q_2 \in A_Z$, existe $m \geq 1$ tal que $d(q_1^m) = d(q_2^m) = 0$. Sejam $q \in A_Z$ e $m \geq 1$ tal que $d((x^{-1}qx)^m) = d(q^m) = 0$. Como $(x^{-1}qx)^m = x^{-1}q^m x$, temos:

$$d(x(x^{-1}q^m x)) = d(x)x^{-1}q^m x; \quad (3)$$

por outro lado,

$$d(x(x^{-1}q^m x)) = d(q^m x) = q^m d(x) \quad (4)$$

Multiplicando as igualdades (3) e (4) à direita por x^{-1} obtemos:

$$d(x)x^{-1}q^m = q^m d(x)x^{-1}$$

ou seja, $d(x)x^{-1}$ pertence a $T(A_Z)$ o hipercentro de A_Z . Mas A_Z é um domínio, portanto $T(A_Z) = Z(A_Z)$ e $d(x)x^{-1} \in Z(A_Z)$. Em particular é verdade que $d(x)x^{-1}$ comuta com x e obtemos $d(x) = xd(x)x^{-1}$, isto é, $d(x)x = xd(x)$. Concluimos então que para todo $x \in R$ vale $[x, d(x)] = 0$ e, portanto, que R é comutativo.

//

Provaremos agora três corolários deste teorema. O primeiro deles é uma generalização do teorema para um ideal de um anel primo sem ideais nil, os outros dois são precisamente os dois resultados de Felzenswalb, que aparecem em [F.2] e que já citamos no início do capítulo.

2.5 - COROLÁRIO. Sejam R um anel primo sem ideal nil não nulo e $I \neq 0$ um ideal de R . Seja ainda $d \neq 0$ uma derivação em R tal que para todo $a \in I$, existe $n = n(a) \geq 1$ tal que $d(a^n) = 0$. Então R é domínio comutativo infinito de característica $p \neq 0$ e $p/n(a)$ se $d(a) \neq 0$.

DEMONSTRAÇÃO. Seja $K = \{a \in I / d^k(a) \in I \quad \forall k \geq 1\}$. Como, dado $r \in R$ e $a \in K$, temos que

$$d^k(ar) = \sum_{i=0}^k \binom{k}{i} d^{k-i}(a) d^i(r),$$

fica claro que $d^k(ar) \in I$. Da mesma forma, $d^k(ra) \in I$ e portanto K é um ideal de R . Pela hipótese sobre I sabemos que todo elemento de I tem alguma potência em K . Logo, como R não tem ideal nil não nulo temos necessariamente que $K \neq 0$. Ainda, $d(K) \subseteq K$ e K considerado com anel é primo (pois R o é). Também é verdade que K não tem ideal nil não nulo, pois de $N \neq 0$ é ideal nil de K teríamos que $KNK \neq 0$ é um ideal nil de R . Ainda, como $K \subseteq I$, temos que para todo $a \in K$ existe $n = n(a) \geq 1$ tal que $d(a^n) = 0$. Podemos, então aplicar o teorema para K e concluir que K é comutativo de característica $p \neq 0$.

Como R é primo, e K é comutativo, temos:

$$K \subseteq C_R(K) = Z(R),$$

o que nos dá R comutativo, condição esta suficiente para que a tese se verifique como vimos na demonstração do teorema 2.4.

//

2.6- COROLÁRIO. Sejam R anel primitivo e $d \neq 0$ uma derivação em R tal que para todo $x \in R$ existe $n = n(x) \geq 1$ com $d(x^n) = 0$. Então R é corpo infinito com $\text{car} R = p \neq 0$ e $p/n(x)$ para todo $x \in R$ tal que $d(x) \neq 0$.

DEMONSTRAÇÃO. Como R é primitivo, R não tem ideal nil não nulo e, pelo teorema 2.4, sabemos que R é domínio comutativo infinito com $\text{car} R = p \neq 0$ e $p/n(x)$ para todo $x \in R$ tal que $d(x) \neq 0$. Ainda com R é primitivo e comutativo, R é um corpo.

//

2.7 - COROLÁRIO. Sejam R um anel primo e $d \neq 0$ uma derivação de R tal que para todo $x \in R$, tem-se que, $d(x^n) = 0$, para um inteiro $n > 1$ fixo. Então R é um domínio comutativo infinito com $\text{car} R = p$ e p/n .

DEMONSTRAÇÃO. Usando o teorema 2.4, basta mostrar que, nas condições do enunciado, R não tem ideal nil não nulo. Suponhamos por absurdo que $0 \neq N$ seja um ideal nil de R . Vamos provar que, neste caso, R tem ideal não nulo nilpotente, o que contradiz a hipótese R primo.

Sejam $0 \neq a \in N$ um elemento nilpotente e $m > 1$ um inteiro tal que $a^m = 0$ mas $a^{m-1} \neq 0$. Vamos provar que $ad(a) = 0$. Seja $b = a^{m-1}$ e consideremos $L = \{x \in R \mid xb = 0\}$ ideal à esquerda de R . É claro que $a \in L$. Consideremos $x \in L$ e $r \in R$. Então:

$$(br + brx)^n = (br)^n + (br)^{n-1}brx = (br)^n + (br)^n x$$

pois $(brx)^2 = (brx)br = 0$. Usando a hipótese sobre a derivação, temos:

$$0 = d((br + brx)^n) = (br)^n d(x)$$

Logo, $(br)^n d(L) = 0 \quad \forall r \in R$. Consequentemente,

$$0 = (br)^n d(L^2) = (br)^n Ld(L) \quad \forall r \in R.$$

Como R é um anel primo e $Ld(L)$ é um ideal à esquerda de R , concluímos que $(br)^n = 0 \quad \forall r \in R$ ou $Ld(L) = 0$. Mas, caso ocorra a primeira hipótese teríamos que $0 \neq bR$ é um ideal lateral nil de índice limitado e, um conhecido re

sultado de Levitzki nos garante que, neste caso, R tem ideal nilpotente não nulo, e provamos o que queríamos. Podemos, então supor que existe $r \in R$ tal que $(br)^n \neq 0$. Logo $Ld(L)=0$ e consequentemente $ad(a)=0$.

Portanto, $\forall a \in N$, temos que $ad(a)=0$. Consideremos a e $b \in N$. Como $a+b^n \in N$ e $d(b^n)=0$, temos:

$$0 = (a+b^n)d(a+b^n) = (a+b^n)d(a) = b^n d(a)$$

Logo, $b^n d(N)=0 \quad \forall b \in N$. Mas como N é ideal não nulo de R , do capítulo 1 sabemos que $Anl_e(d(N))=0$ e portanto $b^n=0 \quad \forall b \in N$. Novamente, temos que N é um ideal nil de índice limitado o que acarreta a existência de um ideal nilpotente não nulo em R .

//

Vamos agora à segunda parte deste capítulo. Nela, trataremos de provar basicamente o seguinte teorema:

2.8 - TEOREMA. Sejam R um anel sem ideais à direita nil não nulos, $I \neq 0$ um ideal de R e d uma derivação em R que é nil em I . Então $d(I)=0$.

Primeiramente mostraremos, através de um exemplo, que não podemos esperar que $d=0$, no caso em que R tem ideal à direita nil não nulo, e d é nil em R .

2.9 - EXEMPLO. Seja F um corpo e $R = \left\{ \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \mid x, y, z \in F \right\}$ um subanel de $M_2(F)$. É claro que $\begin{bmatrix} 0 & F \\ 0 & 0 \end{bmatrix}$ é um ideal à direita nil não nulo de R e se d é a derivação interna dada por $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ temos:

$$d \left(\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \right) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} - \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & z-x \\ 0 & 0 \end{bmatrix}.$$

Logo, $d \neq 0$ e d é nil em R .

Vamos agora à demonstração do teorema 2.8. A proposição que segue demonstra o teorema 2.8 no caso em que R é primitivo. Usaremos este resultado para demonstrar o caso em que R é semisimples.

2.10 - PROPOSIÇÃO. Sejam R um anel primitivo, $I \neq 0$ um ideal de R e d uma derivação em R que é nil em I . Então $d=0$.

DEMONSTRAÇÃO. Como R é primitivo, R é denso no anel $\text{Hom}_D(V, V)$ onde V é um R -módulo irredutível e fiel e $D = \text{Hom}_R(V, V)$ é um anel com divisão. No capítulo 0 já observamos que I , como anel, é também primitivo e denso em $\text{Hom}_D(V, V)$.

Vamos fazer a demonstração em vários passos.

Afirmção 1. Dados $v \in V$ e $a \in I$ tais que $va=0$, então $vd(a)=0$.

Suponhamos, por absurdo, que $vd(a) \neq 0$. Existe, em

tão um elemento $b \in I$ tal que $vd(a)b = v$. Logo, $vd(ab) = v$ e é fácil mostrar, por indução, que $vd(ab)^k = v \quad \forall k \in \mathbb{N}^*$. Mas $d(ab)$ é nilpotente, donde $v = 0$ e chegamos a um absurdo.

Afirmção 2. Dados $v \in V$ e $a \in I$, os elementos va e $vd(a) \in V$ são linearmente dependentes.

Suponhamos, por absurdo, que va e $vd(a)$ são linearmente independentes e seja $b \in I$ tal que $vab = 0$ e $vd(a)b = v$. Pela afirmação 1, $vab = 0$ implica $vad(b) = 0$ e $vd(ab) = 0$; portanto, $vd(a)b = 0$ e concluímos que $v = 0$ chegando a um absurdo.

Afirmção 3. Seja $a \in I$ tal que $\dim_D Va > 1$. Então existe $\alpha \in D$ tal que $\alpha va = vd(a) \quad \forall v \in V$.

Fixemos v e w elementos de V tais que va e wa são linearmente independentes. Pelas afirmações 1 e 2 sabemos que existem α, β e $\gamma \in D$ tais que: $\alpha va = vd(a)$, $\beta wa = wd(a)$ e $\gamma(v+w)a = (v+w)d(a)$. Das três igualdades e do fato de va e wa serem linearmente independentes concluímos que $\alpha = \beta = \gamma$.

Agora, dado $u \in V$ qualquer, ou ua e va são linearmente independentes ou ua e wa são linearmente independentes. Repetindo o argumento do parágrafo anterior concluímos que $\alpha ua = ud(a)$ e portanto está provada a afirmação 3.

Afirmção 4. Seja $a \in I$ com $\dim_D Va > 1$ então, ou $d(a) = 0$ ou a é nilpotente.

Pela afirmação 3 existe $\alpha \in D$ tal que $\alpha va = vd(a)$ $\forall v \in V$. Se $\alpha = 0$ então $vd(a) = 0$ e concluímos que $d(a) = 0$. Suponha mos então que $\alpha \neq 0$. Neste caso, para todo $v \in V$ temos:

$$vd(a)^2 = [vd(a)]d(a) = \alpha [vd(a)]a = \alpha^2 va^2$$

e, por indução, temos:

$$vd(a)^k = \alpha^k va^k \quad \forall v \in V, \quad \forall k \in \mathbb{N}^*.$$

Como $d(a)$ é nilpotente, existe $n \geq 1$ tal que $d(a)^n = 0$ e portan to, $\alpha^n va^n = 0 \quad \forall v \in V$. Ainda, sendo $\alpha \neq 0$, concluímos que $a^n = 0$, isto é, a é nilpotente.

Afirmção 5. Seja $a \in I$ com $\dim_D Va > 1$. Então $d(a) = 0$.

Pelo que foi feito acima, podemos supor $a \neq 0$ e a nilpotente. Neste caso, existem v e $w \in V$, linearmente inde pendent es, tais que $va = 0$ e $wa = v$ (se $a^{n-1} \neq 0$ e $a^n = 0$ tomamos $u \in V$ tal que $ua^{n-1} \neq 0$; fazemos $w = ua^{n-2}$ e $v = wa$. O fato de que $va = 0$ e $wa = v \neq 0$ implica v e w linearmente independentes). Logo, existe $b \in I$ tal que:

$$wb = w - v \quad \text{e} \quad vb = v,$$

e, conseqüentemente,

$$w(a+b) = w \quad \text{e} \quad v(a+b) = v.$$

Temos, portanto, que $\dim_D V(a+b) > 1$ e $\dim_D Vb > 1$. Como $vb = v$ e $w(a+b) = w$, sabemos que $vb^k = v$ e $w(a+b)^k = w \quad \forall k \in \mathbb{N}^*$ e portanto

tanto b quanto $a+b$ não podem ser nilpotentes. Pela afirmação 4, concluímos que $d(b)=d(a+b)=0$ e portanto $d(a)=0$. Provamos, então a afirmação 5.

Para finalizar a demonstração do teorema observamos que se $\dim_D V=1$, então $R \cong D$ é anel com divisão e obviamente teríamos $d=0$. Podemos então supor $\dim_D V > 1$.

Seja $a \in I$. Se $\dim_D Va > 1$ já vimos que $d(a)=0$. Se, por outro lado, $\dim_D Va=1$ então, $\dim_D \text{Ker}(a) \geq 1$ onde $\text{Ker}(a) = \{v \in V / va=0\}$ e existem v e $w \in V$ linearmente independentes e tais que $va=0$ mas $wa \neq 0$. Também existe $b \in I$ tal que $vb=wa \neq 0$ e $wb=u$ onde u e wa são linearmente independentes. Então $\dim_D Vb > 1$ e, como $v(a+b)=wa$ e $w(a+b)=wa+u$, temos também $\dim_D V(a+b) > 1$. Concluímos, portanto, pela afirmação 5, que $d(a+b)=d(b)=0$ e consequentemente $d(a)=0$. Logo, $d(I)=0$ e, como R é primo, $d=0$.

//

Os lemas que seguem, juntamente com o teorema acima, demonstram o teorema 2.8 no caso em que R é semisimples.

2.11 - LEMA. Sejam R um anel, $I \neq 0$ um ideal de R e d uma derivação em R que é nil em I . Se P é um ideal primo de R tal que $N(R/P)=0$, então $d(P) \subset P$ ou $d(I) \subset P$.

DEMONSTRAÇÃO. Denotaremos $\bar{R}$ o anel R/P e se $A \subset R$ denotaremos $\bar{A}$ a imagem de A , pela, projeção canônica, em $\bar{R}$. É claro que

$$d(IPI) \subset d(I)PI + Id(P)I + IPd(I)$$

implica $\overline{Id(P)}\overline{I} = \overline{d(IPI)} \subset \overline{d(I)}$. Ainda, d é nil em I , então $\overline{d(I)}$ é um subconjunto fechado para a soma e nil em $\overline{R}$. Logo, $\overline{Id(P)}\overline{I}$ é um ideal nil de $\overline{R}$. Como $N(\overline{R})=0$ temos $\overline{Id(P)}\overline{I}=0$. Mas $\overline{R}$ é primo, então $\overline{I}=0$ ou $\overline{d(P)}=0$, isto é, $I \subset P$ ou $d(P) \subset P$.

Se $I \subset P$, então $\overline{Rd(I)}\overline{R} = \overline{d(RIR)} \subset \overline{d(I)}$ implica que o ideal $\overline{Rd(I)}\overline{R}$ é nil e, pelo mesmo raciocínio do parágrafo anterior temos $d(I) \subset P$.

//

2.12 - LEMA. Sejam R um anel, I um ideal de R e d uma derivação de R que é nil em I . Então $d(I) \subset J(R)$.

DEMONSTRAÇÃO. Usaremos a mesma notação do lema anterior. Como $J(R)$ é a intersecção dos ideais primitivos de R , basta provar que $d(I) \subset P$ para todo ideal primitivo P de R . Ora, se P é um ideal primitivo de R , então P é ideal primo de R e $J(R/P)=0$ implica $N(R/P)=0$. Logo pelo lema anterior, temos, $d(P) \subset P$ ou $d(I) \subset P$.

Suponhamos que $d(P) \subset P$. Neste caso, d induz uma derivação $\overline{d}$ em $\overline{R}$ dada por:

$$\overline{d}(\overline{r}) = \overline{d(r)} \quad \forall r \in R.$$

É claro que $\overline{d}$ é nil em $\overline{I}$ ideal de $\overline{R}$. Além disto, R é anel primitivo e, portanto, pela proposição 2.10, $\overline{d}(\overline{I})=0$, isto é, $d(I) \subset P$.

Temos então, o resultado que queríamos para anéis semi-simples:

2.13 - TEOREMA. Sejam R um anel semi-simples e $I \neq 0$ um ideal de R . Se d é uma derivação em R , que é nil em I , então $d(I)=0$.

DEMONSTRAÇÃO. Do lema 2.12 sabemos que $d(I) \subset J(R)$. Mas R é semi-simples, portanto $0=J(R)=d(I)$.

//

Vamos agora tratar do caso em que R não é semi-simples, isto é, $J(R) \neq 0$. Obteremos, em primeiro lugar, o resultado para o caso em que R é primo. Para tanto, vamos precisar de algumas definições e alguns resultados preliminares.

Em tudo que segue, dado um anel R , usaremos a seguinte notação:

2.14 - NOTAÇÃO.

1) Se $x \in R$ é um elemento quase regular de R , denotaremos por x' seu quase inverso (isto é, $x' \in R$ é tal que: $xx' + x + x' = 0$ e $xx' = x'x$).

2) Denotaremos por G o conjunto dos elementos quase regulares de R e por A o subanel de R gerado por G . Se R tem unidade, A será o subanel de R gerado por $G \cup \{1\}$.

3) Se $x \in G$ e $a \in R$ denotaremos por $(1+x)a$ o elemento $a+xa$ e por $a(1+x)$ o elemento $a+ax$. É claro que $(1+x)(1+x')a = a(1+x')(1+x) = a$.

2.15 - OBSERVAÇÃO. A é o subgrupo aditivo gerado por G .

DEMONSTRAÇÃO. Se x e y são elementos quase regulares é fácil ver que $a = xy + x + y$ é quase regular com quase inverso $a' = x' + y' + y'x'$. Portanto $xy = a - x - y$ pertence ao subgrupo aditivo gerado por G .

//

2.16 - OBSERVAÇÃO. Se R não é semi-simples, isto é, se $J(R) \neq 0$ então A contém um ideal não nulo de R (em particular, $J(R) \subset A$).

DEMONSTRAÇÃO. $J(R)$ é um ideal quase regular, portanto $J(R) \subset G \subset A$.

//

2.17 - DEFINIÇÃO. Um subconjunto $S \subset R$ será dito invariante sob G se, para todo $x \in G$, temos: $(1+x)S(1+x') \subset S$. Analogamente, se $H \subset G$, e $S \subset R$, diremos que S é invariante sob H se $\forall x \in H, (1+x)S(1+x') \subset S$.

2.18 - LEMA. Seja R um anel primo, S um subconjunto não nu

lo de R e $r \in R$ tal que $rS=0$ ou $Sr=0$. Se S é invariante sob G e A contém um ideal não nulo de R então $r=0$.

DEMONSTRAÇÃO. Vamos fazer a demonstração no caso em que $Sr=0$ (se $rS=0$ a demonstração é análoga).

Sejam $s \in S$ e $x \in G$. Então $(1+x')s(1+x) \in S$ e portanto $0=(1+x')s(1+x)r$. Mas esta igualdade implica que $0=(1+x)[(1+x')s(1+x)r]=s(1+x)r=sxr$ e concluímos que $SGr=0$. Usando indução e a observação 2.15, $SGr=0$ implica que $SAr=0$. Mas, como A contém um ideal não nulo de R , R é primo e $S \neq 0$ concluímos que $r=0$.

//

2.19 - LEMA. Sejam R um anel, $I \neq 0$ um ideal não nulo de R e d uma derivação de R que é nil em I . Dados x e $y \in R$, se $xy=0$ então $xd(y)I$ é um ideal à direita nil de R ($Id(x)y$ é ideal à esquerda nil de R).

DEMONSTRAÇÃO. Dado $a \in I$, é claro que $yax \in I$ e portanto existe $n \geq 1$ tal que $d(yax)^n = 0$. Logo,

$$0 = xd(yax)^n = x[d(y)ax + yd(ax)]^n = x[d(y)ax]^n$$

pois $xy=0$. Consequentemente,

$$0 = x[d(y)ax]^n d(y)a = [xd(y)a]^{n+1}$$

e concluímos que $xd(y)I$ é ideal à direita nil de R (a de

monstração de que $\text{Id}(x)y$ é ideal à esquerda nil de R é análoga).

//

No caso em que R é primo temos um corolário imediato que será constantemente utilizado.

2.20 - COROLÁRIO. Sejam R um anel primo, sem ideal à direita nil não nulo, e $I \neq 0$ um ideal de R . Seja ainda d uma derivação de R que é nil em I . Então, $xy=0$ implica $xd(y)=d(x)y=0$ $\forall x,y \in R$.

DEMONSTRAÇÃO. Do lema anterior sabemos que se $xy=0$ então $xd(y)I$ é ideal à direita nil de R e portanto $xd(y)I=0$. Mas R é primo e $I \neq 0$, logo $xd(y)=0$. Ora, $xy=0$ e $xd(y)=0$ implicam $d(x)y=d(xy)-xd(y)=0$ e esta demonstrado o corolário.

//

Para facilitar a notação usaremos a seguinte definição:

2.21 - DEFINIÇÃO. Se R é um anel e d uma derivação de R , diremos que R e d satisfazem a propriedade p (ou simplesmente R satisfaz p se, não houver confusão possível sobre d) se, dados x e $y \in R$, $xy=0$ implica $xd(y)=d(x)y=0$.

Vamos agora demonstrar o teorema 2.8 no caso em

que R é primo e $J(R) \neq 0$. O corolário 2.20 nos permite concluir que nas condições do teorema 2.8 e se R é primo, então R satisfaz p . Na demonstração do teorema que segue, a hipótese de que R não contém ideais à direita nil não nulos só seria necessária quando precisássemos utilizar o fato de que R satisfaz p . Por isto, optamos por enunciar o teorema na forma que segue:

2.22 - TEOREMA. Sejam R um anel primo com $J(R) \neq 0$ e $I \neq 0$ um ideal de R . Seja ainda d uma derivação de R que é nil em I . Se R e d satisfazem p então $d=0$.

DEMONSTRAÇÃO. Primeiramente observamos que se R não tem elementos nilpotentes não nulos então $d(I)=0$ e, como já foi visto no capítulo I, o fato de R ser primo acarretaria $d=0$. Podemos, então, supor que R contém elementos nilpotentes não nulos.

Ainda, como $J(R) \neq 0$ e $J(R) \subset G = \{x \in R / x \text{ é quase regu}$
 $\text{lar}\}$, basta provarmos que $d(G)=0$. Neste caso, pelo mesmo resultado do capítulo I, teríamos $d(J(R))=0$ e consequentemen
te $d=0$.

Vamos considerar dois subconjuntos de R :

$$S = \{s \in R / s^2 = 0\}$$

e,

$$T = \{t \in R / atb = 0 \text{ implica } atb = 0, \quad \forall a \text{ e } b \in R\}$$

Iniciaremos fazendo algumas observações preliminares sobre S e T que serão constantemente utilizadas:

Observação 1. T é subanel de R .

Ora, dados a e $b \in R$ com $ab=0$ e $t, u \in T$ é claro que $a(t+u)b = atb + aub = 0$. Ainda, como $atb=0$ e $u \in T$ temos: $0 = au(tb) = autb$. Fica então claro que T é subanel de R .

Observação 2. T é invariante sob G .

Sejam $x \in G$, a e $b \in R$ com $ab=0$ e $t \in T$. É claro que $0 = ab = a(1+x)(1+x')b$ e portanto $0 = a(1+x)t(1+x')b$. Então $(1+x)t(1+x') \in T$ e provamos a afirmação 2.

Observação 3. S é invariante sob G e $S \neq 0$.

Dado $s \in S$ e $x \in G$, como $s^2=0$, então $[(1+x)s(1+x')]^2 = (1+x)s(1+x')(1+x)s(1+x') = (1+x)s^2(1+x') = 0$, o que mostra que S é invariante sob G . Como R contém elementos nilpotentes não nulos, é claro que $S \neq 0$.

Observação 4. Se $x \in G$ então $d(x)(1+x') \in T$.

Dados a e $b \in R$ como $ab=0$ temos: $0 = ab = a(1+x)(1+x')b$ e, como R satisfaz p , obtemos:

$$\begin{aligned} 0 &= d(a(1+x))(1+x')b = d(a)(1+x)(1+x')b + ad(x)(1+x')b = \\ &= d(a)b + ad(x)(1+x')b. \end{aligned}$$

Novamente, como R satisfaz p , $d(a)b=0$ e concluímos que

$ad(x)(1+x')b=0$. Portanto, $d(x)(1+x') \in T$ e está provada a afirmação 4.

Voltamos agora à demonstração do teorema. Analisaremos dois casos separadamente:

1º Caso. $T \cap S = \{0\}$

Primeiramente vamos mostrar que, neste caso, $d(S)=0$. De fato, se $s \in S$, então $s^2=0$ e a propriedade p implica $d(s)s=0$. Novamente, usando a propriedade p, temos $d(s)^2=0$. Por outro lado, $s \in G$ e seu quase inverso é $s'=-s$. Então, pela observação 4, $d(s)=d(s)(1-s) \in T$. Mas $d(s)^2=0$, portanto $d(s) \in T \cap S = 0$.

Mostraremos agora que $d^2(R)=0$. Ora, dados $r \in R$ e $s \in S$ é claro que $srs \in S$ e, como $d(S)=0$, temos $0=d(srs)=sd(r)s$. Deduzimos, então, que $sd(r) \in S$ e consequentemente $0=d(sd(r))=sd^2(r)$. Logo, $Sd^2(R)=0$ e, a observação 3 e o lema 2.18 nos permitem concluir que $d^2(R)=0$.

Finalizaremos a demonstração do 1º caso mostrando que $d(G)=0$. Dado $x \in G$, pela afirmação 4, sabemos que $d(x)(1+x') \in T$. Então, se $s \in S$, pela definição de T , temos: $sd(x)(1+x')s=0$ e consequentemente $sd(x)(1+x') \in S$. Como $d^2(R)=d(S)=0$, temos:

$$0=d(sd(x)(1+x'))=sd(x)d(x').$$

Logo, concluímos que $Sd(x)d(x')=0$ e portanto (lema 2.18) $d(x)d(x')=0$.

Por outro lado, $x+x'+xx'=0$ implica $0=d(x+x'xx') = d(x)(1+x')+(1+x)d(x')$ e portanto,

$$[d(x)(1+x')]^2 = d(x)(1+x')[-(1+x)d(x')] = -d(x)d(x') = 0.$$

Concluimos que $d(x)(1+x') \in S \cap T$ o que implica $d(x)(1+x') = 0$. Ora, mas então $0 = d(x)(1+x')(1+x) = d(x)$ e provamos que $d(G) = 0$, finalizando a demonstração do teorema no 1º caso.

2º Caso. $S \cap T \neq \{0\}$

Consideremos $\{0\} \neq W = S \cap T$. Como S e T são invariantes sob G , W também o é. Então, pelo lema 2.18, temos que $W^2 \neq \{0\}$. Mas W^2 também é invariante sob G pois dados $w \in W^2$, $w = uv$ com u e $v \in W$ e $x \in G$ temos:

$$\begin{aligned} (1+x)w(1+x') &= (1+x)uv(1+x') = \\ &= [(1+x)u(1+x')][(1+x)v(1+x')] \in W^2 \end{aligned}$$

uma vez que W é invariante sob G .

Ainda, é claro que $W^2 \subset W$. De fato, dado $w \in W^2$, $w = uv$ com u e $v \in W$ temos: $uvu = 0$ pois $u^2 = 0$ e $v \in T$; $uv \in T$ pois $u \in T$, $v \in T$ e T é subanel de R . Logo, $(uv)^2 = 0$ e $uv \in T$, o que implica $w = uv \in T \cap S = W$.

Vamos provar algumas afirmações:

Afirmção 1. Se $w \in W^2$ então $wRw \subset T$.

Sejam u e $v \in W$ tal que $w = uv$ e $r \in R$ qualquer. Como $v^2 = 0$ temos $(vruv)^2 = 0$ e portanto $vruv \in G$ e tem como quase inverso $-vruv$. Do fato de que $u \in T$ e de que T é subanel de R invariante sob G temos:

$$(1+vruv)u(1-vruv)-u \in T.$$

Mas $(1+vruv)u(1-vruv)-u = -uvruv \in T$ pois $uvu = 0$. Deduzimos, portanto, que $wRw \subset T \quad \forall w \in W^2$ provando a afirmação 1.

Afirmação 2. Se $w \in W^2$ e $x \in G$ então ou $wxw = 0$ ou $wx'w = 0$. Em particular, se x é nilpotente então $wxw = wx'w = 0$.

Em primeiro lugar vamos mostrar que se $s \in S$ e $w \in W^2$ então ou $ws = 0$ ou $sw = 0$. Ora, se $s^2 = 0$, como $wRw \subset T$, a definição de T implica $swRws = 0$. Ainda, como R é primo, temos $sw = 0$ ou $ws = 0$.

Sejam $x \in G$ e $w \in W^2$ quaisquer. Então $(1+x)w(1+x') \in W^2 \subset W \subset S$ e, pelo parágrafo anterior, temos: $w[(1+x)w(1+x')] = 0$ ou $[(1+x)w(1+x')]w = 0$ e portanto ou $w(1+x)w = 0$ ou $w(1+x')w = 0$. Mas, $w^2 = 0$, logo, ou $wxw = 0$ ou $wx'w = 0$ e provamos a primeira parte da afirmação 2.

Suponhamos agora que $x \in G$ seja nilpotente. Vamos provar que $wxw = 0$ usando indução no índice de nilpotência de x . Se $x^2 = 0$, $x' = -x$ e já vimos que $xw = 0$ ou $wx = 0$; portanto $wxw = wx'w = 0$. Seja $x \in G$ nilpotente com índice de nilpotência $n > 2$ e suponhamos válida a afirmação para elementos de R com índice de nilpotência menor que n . Como $x^n = 0$, então $x' = -x + x^2 + \dots + (-1)^{n-1}x^{n-1}$ e, como x^k para $1 < k \leq n-1$ tem índice

de nilpotência menor que n , sabemos, pela hipótese de indução que $wx^k w = 0$. Ora, então $wx'w = -wxw$ e, como $wxw = 0$ ou $wx'w = 0$, é claro que $wxw = wx'w = 0$. Finalizamos assim, a demonstração da afirmação 2.

Afirmação 3. $d(T) = d(S) = 0$

Usamos aqui, pela primeira vez nesta demonstração, que a derivação é nil em I . Sabemos que $\forall a \in I$, $d(a)$ é nilpotente. Consideremos $w \in W^2$, $t \in T$ e $a \in I$. Então $d(at)$ e $d(a)$ são nilpotentes e, pela afirmação 2 temos: $0 = wd(at)w = wd(a)w$. Como $t \in T$, temos $wd(a)tw = 0$ e portanto $0 = wd(at)w = wad(t)w$ de onde concluímos que $wId(T)w = 0 \quad \forall w \in W^2$. Do fato de R ser primo e $W^2 \neq 0$ podemos deduzir que $d(T)W^2 = 0$ e, pelo lema 2.18, que $d(T) = 0$.

Vamos agora mostrar que $d(S) = 0$. Sejam $s \in S$ e $w \in W^2$. Como $s^2 = 0$, sabemos que $-s$ é o quase inverso de s e, na demonstração da afirmação 2 foi provado que $ws = 0$ ou $sw = 0$. Suponhamos que $ws = 0$. Do fato de T ser subanel de R invariante sob G temos: $(1+s)w(1-s) - w \in T$. Mas, $(1+s)w(1-s) - w = sw - ws - sws$ e como $ws = 0$ temos $sw \in T$. Neste caso, $0 = d(sw) = d(s)w$ pois $d(w) \in d(T) = 0$. Se, por outro lado, tivermos $sw = 0$ a propriedade p nos garante que $d(s)w = 0$. Portanto, de qualquer forma, obtemos $d(s)w = 0$ e, consequentemente $d(S)W^2 = 0$. Usando novamente o lema 2.18 deduzimos que $d(S) = 0$, finalizando assim a demonstração da afirmação 3.

Podemos agora concluir a demonstração do teorema provando que $d(G) = 0$. Sejam $x \in G$ e $w \in W^2$. Da afirmação 2, sabemos que $wxw = 0$ ou $wx'w = 0$. Suponhamos que $wx'w = 0$. Neste caso, $wx' \in S$ e $0 = d(wx') = wd(x')$. Mas, $(1+x)w(1+x') \in T$ e, como $d(T) = 0$

temos:

$$0 = d((1+x)w(1+x')) = d(x)w + d(x)wx' = d(x)w(1+x')$$

pois $d(wx') = 0$. Portanto $d(x)w(1+x')(1+x) = d(x)w = 0$. Se, por outro lado, $wxw = 0$, então $xw \in S$ e $0 = d(xw) = d(x)w$. Portanto, de qualquer forma, temos $d(x)w = 0$ e deduzimos que $d(G)W^2 = 0$. Novamente, usando o lema 2.18, concluímos que $d(G) = 0$ finalizando assim a demonstração do teorema.

//

O corolário a seguir é o resultado que queríamos para anéis primos:

2.23 - COROLÁRIO. Sejam R um anel primo e $I \neq 0$ um ideal de R . Seja ainda d uma derivação de R que é nil em I . Se R não contém à direita nil não nulo, então $d = 0$.

DEMONSTRAÇÃO. Pelo corolário 2.20, sabemos que R , nas condições acima, satisfaz a propriedade p. Portanto, se $J(R) \neq 0$ o teorema 2.22 nos permite concluir que $d = 0$. Se, por outro lado, $J(R) = 0$, então o teorema 2.13 mostra que $d(I) = 0$ e, como R é primo, temos $d = 0$.

//

Estamos agora em condições de demonstrar o teorema 2.8.

DEMONSTRAÇÃO DO TEOREMA 2.8. Se $J(R)=0$, o lema 2.12 implica $d(I) \subset J(R)=0$. Suponhamos, então, que $J(R) \neq 0$.

Como R não tem ideais laterais nil não nulos, sabemos que $N(R)=0$ e portanto R é produto subdireto de anéis primos $\{R/P\} \mid P \in \mathcal{P}$ onde $\mathcal{P}$ é uma família de ideais primos de R com $N(R/P)=0 \quad \forall P \in \mathcal{P}$ (teorema 0.3). Vamos mostrar que $d(I) \subset P$ para todo ideal primo P de R com $N(R/P)=0$. Neste caso, $d(I) \subset \bigcap_{P \in \mathcal{P}} P=0$ e esta demonstrado o teorema.

Suponhamos, por absurdo, que $d(I) \not\subset P$ para algum P ideal primo de R com $N(R/P)=0$. Demonstraremos uma série de afirmações que nos levarão à concluir que $d(R) \subset P$, o que é um absurdo.

Denotaremos o anel primo R/P por $\bar{R}$ e, se $A \subset R$, $\bar{A}$ designará a imagem de A em $\bar{R}$, pela projeção canônica.

Afirmção 1. $d(P) \subset P$, $\bar{I} \neq 0$ e $\overline{J(R)} \neq 0$

Pelo lema 2.11 sabemos que $d(I) \subset P$ ou $d(P) \subset P$. Como estamos supondo que $d(I) \not\subset P$ temos que $d(P) \subset P$.

Se $I \subset P$, como $d(RIR) \subset d(R)IR + Rd(I)R + RI d(R)$, temos: $\overline{d(I)} \supset \overline{d(RIR)} = \overline{Rd(I)}\bar{R}$. Logo, como d é nil em I , $\overline{Rd(I)}\bar{R}$ é ideal nil de $\bar{R}$. Mas $N(\bar{R})=0$, portanto $\overline{Rd(I)}\bar{R}=0$, isto é, $d(I) \subset P$ que é absurdo. Então $I \not\subset P$ ou equivalentemente, $\bar{I} \neq 0$.

Se $J(R) \subset P$, então o lema 2.12 nos permite concluir que $d(I) \subset J(R) \subset P$ e chegamos novamente à um absurdo. Então $\overline{J(R)} \neq 0$ e concluímos a demonstração da afirmação 1.

Usando a afirmação 1, como $d(P) \subset P$, sabemos que d induz uma derivação $\bar{d}$ em $\bar{R}$ dada por $\bar{d}(\bar{r}) = \overline{d(r)} \quad \forall r \in R$. Obviamente, $\bar{d}$ é nil em $\bar{I}$. Provaremos agora a seguinte afirmação:

Afirmação 2. $\overline{J(R)}$ é um anel primo que tem ideal à direita nil não nulo.

Como $\bar{R}$ é primo, é claro que $\overline{J(R)}$, ideal de $\bar{R}$, é primo como anel. Se $\bar{R}$ não tem ideal à direita nil não nulos, então, pelo corolário 2.23, temos $0 = \bar{d}(\bar{I}) = \overline{d(I)}$, isto é, $d(I) \subset P$, o que é absurdo. Portanto $\bar{R}$ contém ideal à direita nil não nulo. Seja B tal ideal. Então $B\overline{J(R)}$ é ideal à direita nil de $\overline{J(R)}$. Ainda, $B\overline{J(R)} \neq 0$ pois $\bar{R}$ é primo. Provamos, então, a afirmação 2.

Consideremos agora o seguinte subconjunto de R :

$$T = \{t \in J(R) / atb = 0, \quad \forall a, b \in I \text{ com } ab = 0\}$$

Provaremos as seguintes afirmações sobre T :

Afirmação 3. $\bar{T}$ é subanel de $\overline{J(R)}$

É claro que basta provarmos que T é subanel de $J(R)$. Sejam t e $u \in T$, a e $b \in I$ com $ab = 0$. É claro que $a(t+u)b = atb + aub = 0$; ainda, como $(at)b = 0$, $at \in I$ e $b \in I$, é claro que $atub = 0$. Fica então claro que T é subanel de R e provamos a afirmação 3.

Afirmção 4. Se $\bar{x} \in J(\bar{R})$ e $\bar{y} \in J(\bar{R})$ é seu quase-inverso, en
tão $(1+\bar{x})\bar{T}(1+\bar{y}) \subset \bar{T}$.

Sabemos que $\bar{x} = \bar{w}$ para algum $w \in J(R)$. Se w' é o qua
se inverso de w e $a, b \in I$ com $ab=0$, então: $0=ab=a(1+w)(1+w')b$
implica $a(1+w)T(1+w')b=0$, pois $a(1+w)$ e $(1+w')b \in I$. Portanto
 $(1+w)T(1+w') \subset T$. Mas $\bar{x} = \bar{w}$, consequentemente $\bar{y} = \bar{w}'$ e temos:

$$(1+\bar{x})\bar{T}(1+\bar{y}) = (1+\bar{w})\bar{T}(1+\bar{w}') = \overline{(1+w)T(1+w')} \subset \bar{T},$$

o que prova a afirmação 4.

Afirmção 5. $\bar{T} \subset Z(J(\bar{R}))$ ou $\bar{T} \supset K$ ideal não nulo de $J(\bar{R})$

Esta afirmação é uma consequência imediata do
teorema 0.10 de Herstein, pois $\bar{T}$ é subanel do anel primo
 $J(\bar{R})$, $J(\bar{R})$ contém ideal à direita nil não nulo e, pela afir
mação 4, $\bar{T}$ é invariante sob $J(\bar{R})$.

Finalizamos a demonstração do teorema provando a
seguinte afirmação, que contradiz a hipótese $d(I) \not\subset P$:

Afirmção 6. $\bar{d}=0$, isto é, $d(R) \subset P$.

Vamos analisar os dois casos possíveis que apare
cem na afirmação 4:

1º Caso. $\bar{T} \subset Z(J(\bar{R}))$.

Primeiramente vamos mostrar que, dados a e $b \in I$ com $ab=0$ então $ad(b)=0$. De fato, já vimos no lema 2.19, que $ad(b)I$ é um ideal à direita nil de R e portanto, $ad(b)I=0$. Logo, $ad(b) \in \text{Anl}_e(I) \cap I$ que é um ideal lateral nilpotente. Mas, como R não tem ideal à direita nil não nulo, então R não tem ideal lateral nilpotente não nulo e portanto $ad(b) \in \text{Anl}_e(I) \cap I = 0$.

Vamos agora mostrar que $(1+x')d(x) \in T \quad \forall x \in J(R)I$. Ora, dados $x \in J(R)I$ com x' seu quase inverso e $a, b \in I$ tais que $ab=0$ temos: $0=ab=a(1+x')(1+x)b$. Ainda, $a(1+x') \in I$ e $(1+x)b \in I$; portanto, pelo parágrafo anterior, concluímos que

$$0 = a(1+x')d((1+x)b) = a(1+x')(1+x)d(b) + a(1+x')d(x)b.$$

Novamente, pelo parágrafo anterior, sabemos que

$$0 = ad(b) = a(1+x')(1+x)b \quad \text{e concluímos que}$$

$$0 = a(1+x')d(x)b.$$

Para mostrar que $(1+x')d(x) \in T$, resta verificarmos que $(1+x')d(x) \in J(R)$. Ora, mas $x \in J(R)I$, portanto $d(x) \in d(I)$ e, pelo lema 2.12, $d(I) \subset J(R)$. Logo,

$$(1+x')d(x) = d(x) + x'd(x) \in J(R)$$

Concluímos, enfim, que se $x \in J(R)I$ então $(1+x')d(x) \in T$.

Ainda, é fácil ver que, neste caso, se $\bar{x} \in \overline{J(R)I}$ e $\bar{y}$ é seu quase inverso, então $(1+\bar{y})\bar{d}(\bar{x}) \in \bar{T}$.

Estamos supondo $\bar{T} \subset Z(\overline{J(R)})$. logo, do parágrafo anterior, concluímos que para todo $\bar{x} \in \overline{J(R)} \setminus I$ temos $(1+\bar{y})\bar{d}(\bar{x}) \in Z(\overline{J(R)})$ onde $\bar{y}$ é o quase inverso de $\bar{x}$. Mas $\bar{d}(\bar{x})$ é nilpotente pois $\bar{x} \in I$. Logo, $(1+\bar{y})\bar{d}(\bar{x})$ é um elemento central e não regular do anel primo $\overline{J(R)}$ e portanto $(1+\bar{y})\bar{d}(\bar{x})=0$. Neste caso, $0=(1+\bar{x})(1+\bar{y})\bar{d}(\bar{x})=\bar{d}(\bar{x})$ e concluímos que $\bar{d}(\overline{J(R)} \setminus I)=0$. Mas R é primo e, $\overline{J(R)} \setminus I \neq 0$ donde concluímos que $\bar{d}=0$, provando a afirmação e no 1º caso.

2º Caso. $\bar{T} \supset K$ ideal não nulo de $\overline{J(R)}$

Neste caso, $\bar{T} \supset K \supset \overline{J(R)}K\overline{J(R)}=M$ ideal não nulo de $\bar{R}$. Vamos provar que, se $a \in I$ e a é nilpotente, então $a \in P$.

Dado $a \in I$, com índice de nilpotência $n > 0$, temos que $a^n = 0$ e, pela definição de T , $a^{n-1}Ta = 0$. Logo, $a^{n-2}TaTa = 0$ e, continuando este procedimento, concluímos que $(aT)^{n-1}a = 0$ e portanto, $(aT)^n = 0$. Neste caso, como $M \subset \bar{T}$ temos que

$$(\bar{a}M)^n \subset (\bar{a}T)^n = 0,$$

e conseqüentemente, $\bar{a}M$ é um ideal à direita nilpotente de $\bar{R}$. Concluímos, então, que $\bar{a}M = 0$ e como $M \neq 0$ é um ideal, temos $\bar{a} = 0$, isto é, $a \in P$. Provamos então que todo elemento de I que é nilpotente, pretence também a P .

Podemos então concluir, do parágrafo anterior que $d(I^2) \subset P$, pois $d(I^2) \subset Id(I) + d(I)I \subset d(I) \cap I$. Portanto, $\bar{d}(\bar{I}^2) = 0$ e como $\bar{R}$ é primo, temos $\bar{d} = 0$.

Em qualquer dos casos citados na afirmação 4, con

cluimos que $\bar{d}=0$ o que contradiz a hipótese $d(I) \not\subseteq P$. Concluimos então que $d(I) \subseteq P$ e está provado o teorema.

//

No teorema 2.8, que acabamos de provar, supusemos R um anel sem ideal à direita nil não nulo. Seria natural se perguntar se o teorema seria válido supondo apenas R sem ideal nil não nulo. Mostraremos que esta conjectura é equivalente à conjectura de Köethe.

É óbvio que, se for válida a conjectura de Köethe então um anel sem ideais nil não nulos também não tem ideais laterais nil não nulos e então vale o teorema 2.8 se trocarmos a hipótese R sem ideal à direita nil não nulo por $N(R)=0$.

Suponhamos, por outro lado, que não é válida a conjectura de Köethe. Neste caso, existe R um anel com $N(R)=0$ e $L \neq 0$ um ideal à direita nil de R . O seguinte exemplo mostra que, neste caso, existe uma derivação em R , que é nil e não nula.

2.24 - EXEMPLO. Suponhamos que existe um anel R tal que $N(R)=0$ mas R contenha $L \neq 0$ um ideal à direita nil de R . Seja $a \in L$ tal que $a \neq 0$, mas $a^2=0$ e consideremos d a derivação interna dada por a : $d(x)=ax-xa \quad \forall x \in R$. Como $a^2=0$, a é nilpotente e, como $N(R)=0$, R é semiprimo. Logo, $a \notin Z(R)$, isto é, $d \neq 0$ (teorema 0.2).

Vamos provar que d é nil em R . Ora, dado $x \in R$, $ax \in L$ e portanto ax é nilpotente; logo, existe um inteiro

$n \geq 2$ tal que $(ax)^{n-1} = 0$. Neste caso, $(xa)^n = x(ax)^{n-1}a = 0$. Temos então:

$$d(x)^{2n} = (ax - xa)^{2n} = 0$$

e portanto d é nil em R .

Para finalizar o capítulo, resta-nos demonstrar o resultado de Giamb Bruno e Herstein, já citado anteriormente. Faremos aqui a demonstração dada por Felzenswalb e Lanski em [F.4].

2.5 - TEOREMA. Sejam R um anel, $I \neq 0$ ideal de R e d uma derivação em R que é nil em I de índice limitado (isto é existe $n > 0$ tal que $d(x)^n = 0$, $\forall x \in I$). Então $d = 0$.

DEMONSTRAÇÃO. Usando o teorema 2.13 podemos supor $J(R) \neq 0$. Pelo teorema 2.22, basta provarmos que, nas condições acima, R satisfaz p. Mas, dados x e $y \in R$ com $xy = 0$, pela demonstração do lema 2.19, observamos que $[xd(y)a]^{n+1} = 0 \quad \forall a \in I$. Portanto, $xd(y)I$ é um ideal à direita nil de índice limitado. Como R é primo, o teorema de Levitski implica $xd(y)I = 0$ e conseqüentemente $xd(y) = 0$. Ainda $xy = 0$ implica $d(xy) = 0$ e portanto $xd(y) = d(x)y = 0$.

//

O próximo corolário generaliza o resultado acima para o caso em que R é semiprimo.

2.26 - COROLÁRIO. Sejam R anel semiprimo, $I \neq 0$ ideal de R e d uma derivação em R tal que existe um inteiro $n > 0$, com $d(x)^n = 0$ para todo $x \in I$. Então $d(I) = 0$.

DEMONSTRAÇÃO. Como R é semiprimo, sabemos que $\bigcap_{P \in \mathcal{P}} P = 0$ onde $\mathcal{P} = \{P \subseteq R \mid P \text{ é ideal primo de } R\}$. Basta então provarmos que para todo P ideal primo de R , $d(I) \subseteq P$.

Em primeiro lugar vamos analisar o caso em que $\text{Anl}(I) = \{x \in R \mid Ix = 0\} = 0$. Neste caso, se $M = \bigcap_{\substack{P \in \mathcal{P} \\ I \subseteq P}} P$ e $N = \bigcap_{\substack{P \in \mathcal{P} \\ I \not\subseteq P}} P$ é

claro que $MN \subseteq \bigcap_{P \in \mathcal{P}} P = (0)$. Ainda, $I \subseteq M$ e portanto $IN \subseteq MN = 0$ o que implica $N = 0$. Basta então provarmos que $d(I) \subseteq P$ para todo $P \in \mathcal{P}$ com $I \not\subseteq P$. Na verdade vamos provar que $d(R) \subseteq P$, para todo $P \in \mathcal{P}$ com $I \not\subseteq P$.

Consideremos $P \in \mathcal{P}$ com $I \not\subseteq P$. Vamos mostrar que $d(P) \subseteq P$. Denotaremos por $\bar{R}$ o anel primo R/P e, se $A \subseteq R$, $\bar{A}$ designará a imagem de A pela projeção canônica. Dados $x \in P$ e $a \in I$, é claro que $0 = d(ax)^n = [d(a)x + ad(x)]^n$ implica $[ad(x)]^n \in P$. Consequentemente $\overline{Id(P)}$ é um ideal lateral de $\bar{R}$ nil de índice limitado e, pelo teorema de Levitski, $\overline{Id(P)} = 0$. Ora, mas $I \not\subseteq P$; logo $\bar{I}$ é um ideal não nulo de $\bar{R}$ e portanto $\overline{Id(P)} = 0$ implica $\overline{d(P)} = 0$, isto é, $d(P) \subseteq P$.

Como $d(P) \subseteq P$, d induz uma derivação $\bar{d}$ em $\bar{R}$ dada por $\bar{d}(\bar{r}) = \overline{d(r)}$ $\forall r \in R$. É claro que $\bar{d}(\bar{a})^n = 0$ $\forall \bar{a} \in \bar{I}$ e $\bar{R}$ é primo. Estamos portanto nas condições do teorema 2.25 e deduzimos que $\bar{d} = 0$, isto é, $d(R) \subseteq P$. Concluimos portanto que, se $\text{Anl}(I) = 0$, então $d = 0$.

Se, por outro lado, $\text{Anl}(I) \neq 0$ tomamos o anel semi primo $R/\text{Anl}(I)$. Vamos provar que $d(\text{Anl}(I)) \subset \text{Anl}(I)$. Dados $a \in I$ e $x \in \text{Anl}(I)$, $ax=0$ e pela demonstração do lema 2.19 concluimos que $[\text{ad}(x)b]^{n+1}=0 \quad \forall b \in I$, isto é, $\text{ad}(x)I$ é um ideal lateral nil de índice limitado, e pelo teorema de Levitzki, $\text{ad}(x)I=0$. Então $\text{ad}(x) \in I \cap \text{Anl}(I)=0$ pois é um ideal nilpotente de R . Portanto $\text{ad}(x)=0$ e temos $d(x) \in \text{Anl}(I)$.

Para não haver confusão com a notação acima, denotaremos R' o anel semiprimo $R/\text{Anl}(I)$ e, se $A \subset R$ denotaremos por A' a imagem de A pela projeção canônica. Como $d(\text{Anl}(I)) \subset \text{Anl}(I)$ d induz uma derivação d' em R' dada por $d'(r')=d(r)'$ $\forall r \in R$. É claro que $I' \neq 0$, $d'(a')^n=0 \quad \forall a' \in I'$ e $\text{Anl}(I')=\text{Anl}(I)'=0$. Voltamos então às condições que analisamos anteriormente e concluimos que $d'=0$ isto é, $d(R) \subset \text{Anl}(I)$. Ora, mas neste caso, $d(I)$ é um ideal à direita de R , pois $d(I)$ é fechado para a soma e, dados $d(a) \in d(I)$ e $r \in R$ $d(a)r=d(ar)-\text{ad}(r)=d(ar) \in d(I)$. Como $d(a)^n=0 \quad \forall a \in I$, $d(I)$ é um ideal à direita de R nil de índice limitado. Novamente usando o teorema de Levitzki temos $d(I)=0$.

//

CAPÍTULO III

Este capítulo é uma continuação natural da última parte do capítulo anterior. Veremos aqui o que ocorre quando num anel R , sem ideais à direita nil temos uma derivação d tal que $d(x)^{n(x)} \in Z(R)$ para todo $x \in I$, ideal de R .

O primeiro trabalho onde temos um resultado desta natureza é em [H.3] onde I.N.Herstein demonstra o seguinte: sejam R um anel primo, $a \in R$ e $n > 0$ um inteiro fixo tais que $(ax - xa)^n \in Z(R)$ para todo x num ideal I não nulo de R . Então ou $a \in Z(R)$ ou R é uma ordem numa álgebra simples de dimensão 4 sobre seu centro.

Mais tarde, em [H.4], Herstein generaliza seu próprio resultado para derivações quaisquer, provando que num anel primo R , se existe uma derivação $d \neq 0$ tal que $d(x)^n \in Z(R)$, onde $n > 0$ é um inteiro fixo, então R é uma ordem numa álgebra simples de dimensão no máximo 4 sobre seu centro.

Usando os mesmos métodos de Herstein, C.Lanski generaliza mais uma vez o resultado acima provando, em [L.1], o seguinte teorema: sejam R um anel primo, não comutativo, sem ideais à direita nil não nulos e $d \neq 0$ uma derivação em R tal que $d(x)^{n(x)} \in Z(R)$ para todo $x \in I$, ideal não nulo de R . Então ou R é um domínio e R_Z , o localizado de R no seu centro, é um anel com divisão ou $R_Z = M_2(F)$, onde F é corpo. Ainda, se R é um domínio e $Z(R)$ é não enumerável, então R_Z tem dimensão no máximo 4 sobre seu centro.

Lanski, conclui portanto, que R é uma ordem numa

álgebra simples de dimensão no máximo 4 sobre seu centro, no caso em que $R_Z = M_2(F)$ ou no caso em que $Z(R)$ é não enumerável.

Faremos aqui uma nova demonstração, que engloba o segundo resultado de Herstein e o resultado de Lanski. Esta demonstração utiliza basicamente os mesmos métodos que Herstein e posteriormente Lanski utilizaram em [H.4] e [L.1] respectivamente. Porém, provamos uma pequena generalização de um teorema de Bergen (que aparece em [B.1]), que faz com que não precisemos utilizar o resultado de Herstein de [H.3] e tampouco os lemas sobre identidades polinomiais que aparecem tanto em [H.4] quanto em [L.1].

Ao longo das demonstrações tanto de Herstein quanto de Lanski, dos teoremas supra-citados, percebemos que a hipótese de R ser primo é utilizada apenas para garantir que $Z(R)^*$ não tem divisores de zero e consequentemente, $d(x)^{n(x)} \in Z(R)$ implica $d(x)$ nilpotente ou $d(x)$ regular. Provaremos aqui uma proposição que nos permitirá enfraquecer, no teorema de Herstein, a hipótese para R semiprimo, contando que suponhamos $d(x)^n = 0$ ou $d(x)^n$ central e regular. Esta mesma proposição também nos permitirá, no teorema de Lanski, suprimir a hipótese de R ser primo, desde que suponhamos $d(x)^{n(x)} = 0$ ou $d(x)^{n(x)}$ central e regular.

Finalmente, analisamos, nas condições do teorema de Lanski, o caso em que R tem características $p > 0$, conseguindo provar que, também neste caso, R é uma ordem numa álgebra simples de dimensão no máximo 4 sobre seu centro.

Este capítulo tratará, portanto de provar os seguintes teoremas:

3.1 - TEOREMA. Sejam R um anel não comutativo, sem ideais à direita nil não nulos, d uma derivação em R e $I \neq 0$ ideal de R tais que $d(I) \neq 0$ e para todo $x \in I$, existe $n(x) > 0$ tal que $d(x)^{n(x)} \in Z_p(R) = \{x \in Z(R) \mid x \text{ é regular}\} \cup \{0\}$. Então valem as seguintes afirmações:

(i) se R não é um domínio então $R_Z = M_2(F)$ onde F é um corpo (e portanto R é uma ordem numa álgebra simples de dimensão 4 sobre seu centro).

(ii) se R é um domínio, então R_Z é um anel com divisão (e portanto R é uma ordem em R_Z).

(iii) se R é um domínio e $Z(R)$ é não enumerável então R_Z tem dimensão 4 sobre seu centro.

(iv) se R é um domínio e $\text{car} R = p > 0$, então R_Z tem dimensão 4 sobre seu centro.

3.2 - TEOREMA. Sejam R um anel semiprimo, não comutativo, d uma derivação em R e $I \neq 0$ um ideal de R tais que $d(I) \neq 0$ e, para todo $x \in I$, $d(x)^n \in Z_p(R) = \{x \in Z(R) \mid x \text{ é regular}\} \cup \{0\}$, para um inteiro $n > 0$ fixo. Então R é uma ordem numa álgebra simples de dimensão 4 sobre seu centro.

Os dois lemas a seguir mostram que tanto nas condições do teorema 3.1 quanto nas condições do teorema 3.2 podemos concluir que d não é nil em nenhum ideal não nulo de R . Estes lemas e a proposição que os segue nos permitem concluir que, nas condições de qualquer dos teoremas, o anel R é primo e R_Z é simples com unidade. Na verdade tanto

os lemas quanto a conclusão de que R é primo valem num contexto mais geral, pois sua demonstração só utiliza o fato de $d(x)^{n(x)}$ ser regular (não é necessário que $d(x)^{n(x)}$ seja central). No capítulo 4 voltaremos a este resultado na sua forma mais geral.

3.3 - LEMA. Sejam R , I e d nas condições do teorema 3.1. Então d não é nil em nenhum ideal não nulo de R .

DEMONSTRAÇÃO. Como R não tem ideais à direita nil não nulos e $d(I) \neq 0$, o teorema 2.8, implica que d não é nil em I . Neste caso, existe $a \in I$ tal que $0 \neq d(a)^{n(a)} \in Z_p(R)$ e consequentemente $d(a)$ é regular.

Seja agora $J \neq 0$ um ideal de R . Vamos mostrar que d não é nil em J . Ora, se d é nil em J então, pelo teorema 2.8 temos $d(J) = 0$ e consequentemente, $0 = d(aJ) = d(a)J$ que é absurdo pois $d(a)$ é regular e $J \neq 0$.

//

3.4 - LEMA. Sejam R , I e d nas condições do teorema 3.2. Então d não é nil em nenhum ideal não nulo de R .

DEMONSTRAÇÃO. Como R é semiprimo e $d(I) \neq 0$ o corolário 2.26 implica que d não é nil em I . Neste caso, existe $a \in I$ tal que $0 \neq d(a)^n \in Z_p(R)$ e consequentemente $d(a)$ é regular.

Vamos provar que $d(I^2) \neq 0$. Ora, se $d(I^2) = 0$, então

$0 = d(aI^2) = d(a)I^2$ e consequentemente $I^2 = 0$ o que é absurdo, pois R é semiprimo.

Vamos agora mostrar que I contém um elemento regular. De fato, como $d(I^2) \neq 0$, o corolário 2.26 implica que d não é nil em I^2 e portanto existe $b \in I^2$ tal que $0 \neq d(b)^n \in Z_p(R)$. Então $d(b)$ é regular e temos:

$$d(b) \in d(I^2) \subset d(I)I + Id(I) \subset I.$$

Logo, existe um elemento regular em I .

Seja agora $J \neq 0$ um ideal de R . Vamos provar que d não é nil em J . Ora, se d é nil em J , dado $x \in IJ \subset I \cap J$ temos que $d(x)$ não é regular e, como $d(x)^n \in Z_p(R)$, concluímos que $d(x)^n = 0$. Neste caso, o corolário 2.26 implica $d(IJ) = 0$. Já vimos que existe $a \in I$ tal que $d(a)$ é regular; portanto, se $d(IJ) = 0$ então $0 = d(aIJ) = d(a)IJ$ e concluímos que $IJ = 0$. Também já vimos que I contém um elemento regular, portanto $IJ = 0$ implica $J = 0$, que é um absurdo. Logo, concluímos que d não é nil em J , finalizando a demonstração do lema.

//

3.5 - PROPOSIÇÃO. Sejam R um anel semiprimo, d uma derivação em R e $I \neq 0$ um ideal de R tais que para cada $x \in I$, existe um inteiro $n = n(x) > 0$ com $d(x)^n \in Z_p(R)$. Suponhamos ainda que d não é nil em nenhum ideal não nulo de R . Então valem as seguintes afirmações:

(i) se $J \neq 0$ é ideal de R , então $J \cap Z_p(R) \neq 0$.

(ii) R é primo e consequentemente $Z(R) = Z_\rho(R)$.

(iii) R_Z é simples com 1.

DEMONSTRAÇÃO. (i) Primeiramente vamos provar que $I \cap Z_\rho(R) \neq 0$. De fato, como R é semiprimo, $I^2 \neq 0$ e consequentemente d não é nil em I^2 . Neste caso, existe $b \in I^2$ tal que $0 \neq d(b)^{n(b)} \in Z_\rho(R)$ e portanto $d(b)$ é regular. Mas,

$$d(b)^{n(b)} \in d(I^2)^{n(b)} \subset [d(I)I + Id(I)]^{n(b)} \subset I$$

e concluímos que $0 \neq d(b)^{n(b)} \in I \cap Z_\rho(R)$.

Seja agora $J \neq 0$ um ideal de R . Como I contém um elemento regular, sabemos que $IJ \neq 0$. Mas R é semiprimo, portanto $(IJ)^2 \neq 0$ e, consequentemente, d não é nil em $(IJ)^2$. Logo, existe $c \in (IJ)^2$ tal que $0 \neq d(c)^{n(c)} \in Z_\rho(R)$. Mas, $d(c)^{n(c)} \in d((IJ)^2)^{n(c)} \subset IJ \subset J$; portanto concluímos que $0 \neq d(c)^{n(c)} \in Z_\rho(R) \cap J$ finalizando a demonstração do item (i).

(ii) A demonstração deste item é uma consequência imediata de (i), pois se todo ideal não nulo de R contém um elemento regular, então dados J_1 e J_2 ideais de R temos: $J_1 J_2 = 0$ implica que $J_1 = 0$ ou $J_2 = 0$. Portanto, R é primo e consequentemente $Z_\rho(R) = Z(R)$ (teorema 0.1).

(iii) Do item (ii) sabemos que $Z_\rho(R) = Z(R)$ e portanto podemos definir R_Z , o localizado de R em $Z(R)^*$ (o fato de d não ser nil em I garante $Z(R) \neq 0$). É claro que

R_Z tem unidade.

Vamos mostrar que R_Z é simples. Seja $J' \neq 0$ um ideal de R_Z . É claro que $J = J' \cap R$ é um ideal não nulo de R e, pelos itens anteriores, sabemos que $J \cap Z(R) \neq 0$. Consequentemente, existe $z \in J' \cap Z(R)^*$ e, portanto, $1 = z^{-1} \cdot z \in R_Z J' = J'$. Logo, $J' = R_Z$ e concluímos a demonstração de (iii).

//

Mostraremos, agora, que $R_Z = D$ ou $R_Z = M_2(D)$ onde D é um anel com divisão. Para tanto usaremos, no teorema a seguir, a mesmíssima técnica usada por Bergen em [B.1], seguindo uma pequena generalização de seu trabalho. Como este resultado pode ter interesse independente, voltaremos a ele no capítulo 4, onde também demonstraremos o resultado de Bergen que aparece em [B.1].

3.6 - TEOREMA. Seja R um anel primo tal que R_Z , o localizador de R em $Z(R)^*$, é um anel primitivo. Sejam, ainda $d \neq 0$ uma derivação em R e $I \neq 0$ ideal de R tais que para todo $x \in I$ ou $d(x)$ é nilpotente ou $d(x)$ é inversível de R_Z . Então $R_Z = D$ ou $R_Z = M_2(D)$, onde D é um anel com divisão.

DEMONSTRAÇÃO. Como R_Z é primitivo, pelo teorema da densidade de Jacobson, existe V , um R_Z módulo irredutível e fiel, tal que R_Z é denso em $\text{Hom}_D(V, V)$ onde $D = \text{Hom}_R(V, V)$ é um anel com divisão. Já mencionamos, no capítulo 0, que se K é um ideal não nulo de R_Z então V é também um K -módulo irredutível e fiel e K é denso em $\text{Hom}_D(V, V)$. Vamos usar frequen

temente nesta demonstração o teorema da densidade de Jacobson para o ideal $I' = \{az^{-1} \mid a \in I \text{ e } z \in Z(R)^*\}$ de R_Z .

Sabemos ainda que, se $\dim_D V \leq 2$ então $R = D$ ou $R = M_2(D)$. Suponhamos por absurdo que $\dim_D V > 2$; faremos a demonstração através de uma série de passos chegando, finalmente, à conclusão de que $d=0$ o que é um absurdo.

Afirmção 1. Sejam $v \neq 0$ e $w \neq 0$ elementos de V e $a \in I$ tal que $va = wa = 0$. Então $\{vd(a), wd(a)\}$ é ld sobre D .

Suponhamos, por absurdo, que $\{vd(a), wd(a)\}$ é li sobre D . Neste caso, como I' é denso em $\text{Hom}_D(V, V)$, existe $bz^{-1} \in I'$ tal que:

$$vd(a)bz^{-1} = v \quad \text{e} \quad wd(a)bz^{-1} = 0,$$

e portanto,

$$vd(a)b = vz \quad \text{e} \quad wd(a)b = 0.$$

Mas, neste caso, temos:

$$vd(ab) = vd(a)b = vz$$

$$wd(ab) = wd(a)b = 0.$$

Como $ab \in I$, $d(ab)$ é nilpotente ou inversível. Se $d(ab)$ é nilpotente então existe um inteiro $n > 0$ tal que $d(ab)^n = 0$, mas $vd(ab) = vz$ e portanto $vd(ab)^2 = vd(ab)z = vz^2$ e prova-se, por indução que $vd(ab)^n = vz^n$. Logo, se $d(ab)^n = 0$ então $vz^n = 0$ e, co

mo z é inversível em R_Z temos $v=0$, um absurdo.

Se, por outro lado, $d(ab)$ é inversível, então $wd(ab)=0$ implica que $w=0$, o que também é um absurdo. Concluimos, então, que $\{vd(a), wd(a)\}$ é ld sobre D .

Afirmção 2. Sejam $v, w \in V$, li e $a \in I$ tal que $va=wa=0$. Então $d(a)$ é nilpotente.

Da afirmação 1 sabemos que $\{vd(a), wd(a)\}$ é ld sobre D . Então, existem α e $\beta \in D$ não ambos nulos e tais que $0 = \alpha vd(a) + \beta wd(a) = (\alpha v + \beta w)d(a)$. Se $d(a)$ fosse inversível então $\alpha v + \beta w = 0$ o que contradiz a hipótese $\{v, w\}$ li. Logo $d(a)$ é nilpotente e provamos a afirmação 2.

Afirmção 3. Sejam $v, w \in V$ li e $a \in I$ tal que $va=wa=0$. Então $vd(a)=wd(a)=0$.

É suficiente demonstrar que $vd(a)=0$. Ora, se $vd(a) \neq 0$ existe $bz^{-1} \in I'$ tal que $vd(a)bz^{-1}=v$ e portanto $vd(a)b=vz$. Neste caso, temos $vd(ab)=vd(a)b=vz$ e prova-se, por indução, que $vd(ab)^n=vz^n \quad \forall n > 0$. Mas, da afirmação 2, sabemos que $d(ab)$ é nilpotente pois $vab=wab=0$. Portanto, existe um inteiro $k > 0$ tal que $0 = vd(ab)^k = vz^k$ o que implica $v=0$ uma vez que z é inversível. Chegamos, então, a um absurdo que vem do fato de termos suposto $vd(a) \neq 0$ e provamos a afirmação 3.

Afirmção 4. Sejam $v \in V$ e $a \in I$ com $va=0$. Então $vd(a)=0$.

Vamos analisar primeiro o caso em que $\dim_D V a > 1$. Suponhamos, por absurdo, que $vd(a) \neq 0$. Ora, se $\dim_D V a > 1$ e $vd(a) \neq 0$, então existe $w \in V$ tal que wa e $vd(a)$ são li. Vamos provar que v e w são li. De fato, se α e $\beta \in D$ são tais que $\alpha v + \beta w = 0$ então $0 = \alpha va + \beta wa = \beta wa$ o que implica $\beta = 0$ e consequentemente $\alpha = 0$ (pois $vd(a) \neq 0$ implica $v \neq 0$). Temos, portanto, v e w li e wa e $vd(a)$ também li.

Logo, existe $bz^{-1} \in I'$ tal que: $wabz^{-1} = 0$ e $vd(a)bz^{-1} = v$; consequentemente, $wab = 0$ e $vd(a)b = vz$. Mas então, $vab = wab = 0$ e, da afirmação 3, concluímos que $vd(ab) = wd(ab) = 0$. Mas $vd(ab) = vd(a)b = vz$; portanto concluímos que $vz = 0$ o que implica $v = 0$, um absurdo. Demonstramos, então, que $\dim_D V a > 1$ implica $vd(a) = 0$.

Suponhamos agora que $\dim_D V a = 1$. Como estamos supondo $\dim_D V > 2$, temos $\dim_D \text{Ker}(a) \geq 2$ onde $\text{Ker}(a) = \{w \in V \mid wa = 0\}$. Neste caso, existe $w \in V$ com $wa = 0$ e $\{w, v\}$ li. Podemos então usar a afirmação 3 para concluir que $vd(a) = 0$.

Concluímos, desta forma, a demonstração da afirmação 4.

Afirmção 5. Sejam $v \in V$ e $a \in I$. Então $\{va, vd(a)\}$ é ld.

Suponhamos, por absurdo, que va e $vd(a)$ são li. Então existe $bz^{-1} \in I'$ tal que $vabz^{-1} = 0$ e $vd(a)bz^{-1} = v$; consequentemente, $vab = 0$ e $vd(a)b = vz$. Mas, se $vab = 0$, pela afirmação 4, sabemos que $vad(b) = vd(ab) = 0$. Portanto temos:

$$vz = vd(a)b = v[d(ab) - ad(b)] = 0$$

o que implica $v=0$, uma contradição.

Logo, va e $vd(a)$ são li o que demonstra a afirmação 5.

Afirmção 6. Seja $a \in I$ tal que $\dim_D Va > 1$ e $d(a)$ é nilpotente. Então ou $d(a)=0$ ou a é nilpotente.

Pelas afirmações 4 e 5 sabemos que para cada $v \in V$ existe $\lambda(v) \in D$ tal que $vd(a) = \lambda(v)va$. Vamos mostrar $\lambda(v)$ não depende de v .

Fixados v e $w \in V$ com $\{va, wa\}$ li temos:

$$vd(a) = \lambda(v)va, \quad wd(a) = \lambda(w)wa \quad e$$

$$(v+w)d(a) = \lambda(v+w)(v+w)a.$$

Como va e wa são li concluímos que $\lambda(v) = \lambda(w) = \lambda(v+w) = \lambda$. Mas $\forall u \in V$, se $ua=0$, da afirmação 4 sabemos que $ud(a)=0$ e portanto $ud(a) = \lambda ua$. Por outro lado, se $ua \neq 0$, então ou ua e va são li ou ua e wa são li e, pelo mesmo argumento usado acima, concluímos que $\lambda(u) = \lambda$. Portanto, $\forall u \in V$ temos: $ud(a) = \lambda ua$.

Se $\lambda=0$ então $Vd(a)=0$ e concluímos que $d(a)=0$. Se, por outro lado, $\lambda \neq 0$, então $\forall u \in V$ temos:

$$ud(a)^2 = (ud(a))d(a) = (\lambda ua)d(a) = \lambda(\lambda ua)a = \lambda^2 ua^2,$$

e é fácil mostrar, por indução, que $ud(a)^n = \lambda^n ua^n$ para todo inteiro $n > 0$. Como $d(a)$ é nilpotente, existe $k > 0$ tal que

$\lambda^k u a^k = 0 \quad \forall u \in V$. Mas, $\lambda \neq 0$, portanto $u a^k = 0 \quad \forall u \in V$ e concluímos que $a^k = 0$, finalizando a prova da afirmação 6.

Afirmação 7. Seja $a \in I$ com $\dim_D V a > 1$ e $d(a)$ nilpotente. Então $d(a) = 0$.

Pela afirmação anterior $d(a) = 0$ ou a é nilpotente. Suponhamos que a seja nilpotente. Primeiramente vamos provar que existem w, u e $v \in V$ linearmente independentes e tais que:

$$va = w, wa = 0 \quad \text{e} \quad ua \neq 0.$$

Ora, como a é nilpotente, existe um inteiro $m, m \geq 2$, tal que $a^m = 0$ e $a^{m-1} \neq 0$. Então, existe $t \in V$ com $ta^{m-1} \neq 0$. Seja $w = ta^{m-1}$ e $v = ta^{m-2}$; como $\dim_D V a > 1$, existe $u \in V$ tal que $u a$ e $va = w$ são li. Para verificar que u, v e w são li basta observar que se α, β e $\gamma \in D$ são tais que $\alpha u + \beta v + \gamma w = 0$ então $0 = \alpha u a + \beta v a + \gamma w a = \alpha u a + \beta w$ o que implica $\alpha = \beta = 0$, pois $u a$ e w são li. Logo, $0 = \gamma w$ e temos $\alpha = \beta = \gamma = 0$.

Como u, v e w são li, existe $bz^{-1} \in I'$ tal que:

$$vbz^{-1} = v - w, wbz^{-1} = w \quad \text{e} \quad ubz^{-1} = -ua$$

e portanto,

$$\begin{array}{lll} vb = (v - w)z & v(az + b) = vz & v(az^2 + bz) = vz^2 \\ wb = wz & , & w(az + b) = wz \quad \text{e} \quad w(az^2 + bz) = wz^2 \\ ub = -uaz & u(az + b) = 0 & u(az^2 + bz) = 0 \end{array} \quad (1)$$

Temos, então $\dim_D V(az+b) > 1$ e, como $u(az+b)=0$, da afirmação 4, concluímos que $ud(az+b)=0$ e consequentemente $d(az+b)$ não é inversível de R_Z . Ainda, $az+b \in I$ (pois $a \in I$ e $b \in I$); logo, $d(az+b)$ é nilpotente e, da afirmação 6, temos $d(az+b)=0$ ou $az+b$ nilpotente. Mas $w(az+b)=wz$ e z é central; prova-se então, facilmente que $w(az+b)^n = wz^n$ para todo inteiro $n > 0$. Logo, $az+b$ não é nilpotente. Finalmente, concluímos que $d(az+b)=0$.

Exatamente, pelos mesmos argumentos concluímos também que $d(az^2+bz)=0$ e portanto,

$$0 = d(az^2+bz) = (az+b)d(z).$$

Mas, já vimos no capítulo zero, que $d(Z(R)) \subset Z(R)$. Portanto $(az+b)d(z)=0$ implica $d(z)=0$ ou $az+b=0$. Mas $w(az+b)=wz$ implica $az+b \neq 0$ e concluímos que $d(z)=0$.

Neste caso, $0 = d(az+b) = d(a)z + d(b)$, isto é, $d(b)z^{-1} = -d(a)$. Como $d(a)$ é nilpotente, segue que $d(b)z^{-1}$ também é nilpotente e concluímos que $d(b)$ é nilpotente.

Analisando as igualdades de (1), é claro que $\dim_D Vb > 1$ portanto, da afirmação 6, concluímos que $d(b)=0$ ou b é nilpotente. Mas $wb=wz$ implica $wb^n = wz^n$ para todo inteiro $n > 0$; logo, b não é nilpotente e concluímos que $d(b)=0$.

Então, $0 = d(az+b) = d(a)z$ e portanto $d(a)=0$ o que conclui a demonstração da afirmação 7.

Afirmação 8. $d=0$

Seja $v \in V$, $v \neq 0$ e consideremos $T = \{x \in I \mid vx = 0\}$. É claro que T é um ideal à direita de R e $T \neq 0$ pois o teorema da densidade de Jacobson garante que existe $0 \neq a \in I$ tal que $va = 0$. Ainda, dado $a \in T$ é claro que $d(a)$ é nilpotente pois $va = 0$ implica $vd(a) = 0$ que por sua vez acarreta que $d(a)$ não inversível de R_Z .

Vamos mostrar que $d(T) = 0$. Ora, se $a \in T$ e $\dim_D Va > 1$ então a afirmação anterior implica $d(a) = 0$. Por outro lado, se $\dim_D Va = 1$ então, como $\dim_D V > 2$, temos $\dim_D \text{Ker}(a) > 1$ onde $\text{Ker}(a) = \{w \in V \mid wa = 0\}$. Podemos, então, tomar $w \in \text{Ker}(a)$ tal que v e w são li e $u \in V$ com $ua \neq 0$.

Vamos mostrar que u , v e w são li. De fato, se α , β e $\gamma \in D$ são tais que $\alpha u + \beta v + \gamma w = 0$ então $0 = \alpha ua + \beta va + \gamma wa = \alpha ua$ o que implica $\alpha = 0$ e, como v e w são li, $\alpha = \beta = \gamma = 0$.

Logo, dados t_1 e $t_2 \in V$ tais que $\{ua, t_1, t_2\}$ é li, existe $bz^{-1} \in I'$ tal que:

$$vbz^{-1} = 0, \quad wbz^{-1} = t_1 \quad \text{e} \quad ubz^{-1} = t_2$$

e portanto,

$$vb = 0, \quad wb = t_1 z \quad \text{e} \quad ub = t_2 z.$$

Como $\{t_1, t_2\}$ é li então $\{t_1 z, t_2 z\}$ é li e conclu
mos que $\dim_D Vb > 1$. Ainda, $vb = 0$ e portanto $b \in T$ e já observa
mos que se $b \in T$ e $\dim_D Vb > 1$ então $d(b) = 0$.

Mas, como $va = wa = 0$ temos:

$$v(a+b)=0, w(a+b)=t_1z \text{ e}$$

$$u(a+b)=ua+t_2z.$$

Vamos mostrar que $\{t_1z, ua+t_2z\}$ é li. Ora, como $\{ua, t_1, t_2\}$ é li basta mostrar que para todo $t \in V$, $t \neq 0$ e $c \in Z(R)^*$ temos $\{t, tc\}$ ld. De fato, se $\{t, tc\}$ é li então existe $rs^{-1} \in I$ tal que

$$trs^{-1}=0 \text{ e } tc rs^{-1}=t$$

e, neste caso, como $c \in Z(R)$, concluímos que $t = tc rs^{-1} = trs^{-1}c = 0$ o que é absurdo.

Mas, se $\{t_1z, ua+t_2z\}$ é li então $\dim_D V(a+b) > 1$ e, como $v(a+b)=0$, temos $a+b \in T$. Neste caso, já concluímos que $d(a+b)=0$.

Temos, portanto, que $d(a+b)=d(b)=0$. Logo, $d(a)=0$ e demonstramos que $d(T)=0$. Mas T é um ideal à direita não nulo de R ; como R é primo, do capítulo 1, temos que $d(T)=0$ implica $d(R)=0$.

Concluímos então a demonstração da afirmação 8 e do teorema.

//

O corolário deste teorema que nos interessa para demonstrar os teoremas 3.1 e 3.2 é o seguinte:

3.7 - COROLÁRIO. Tanto nas condições do teorema 3.1 quanto nas condições do teorema 3.2 concluímos que ou $R_Z = D$ ou $R_Z = M_2(D)$, onde D é um anel com divisão.

DEMONSTRAÇÃO. Os lemas 3.3 e 3.4 e a proposição 3.5 implicam que tanto nas condições do teorema 3.1 quanto nas condições do teorema 3.2, R é primo e R_Z é simples com 1, portanto primitivo.

Nas hipóteses dos dois teoremas temos d uma derivação tal que $d(x)^{n(x)} \in Z(R) = Z_p(R) \quad \forall x \in I$. Neste caso, ou $d(x)^{n(x)} = 0$ e temos que $d(x)$ é nilpotente, ou $d(x)^{n(x)} \in Z(R)^*$ e temos que $d(x)^{-1} = d(x)^{n(x)-1} d(x)^{-n(x)}$, isto é, $d(x)$ é inversível de R_Z . Estamos, portanto, nas hipóteses do teorema 3.6 e concluímos que $R_Z = D$ ou $R_Z = M_2(D)$ que demonstra o corolário.

//

Vamos agora demonstrar que, no caso em $R_Z = M_2(D)$ D é, na verdade, um corpo. A proposição que segue utiliza um resultado de F.C.Polcino Milies que aparece em [PM] e que já foi citado no capítulo 0.

3.8 - PROPOSIÇÃO. Sejam R um anel primo, $d \neq 0$ uma derivação em R e $I \neq 0$ um ideal de R tal que para todo $a \in I$ existe um inteiro $n(a) > 0$ tal que $d(a)^{n(a)} \in Z(R)$. Suponhamos ainda que $R_Z = M_2(D)$ para algum anel com divisão D . Então D é um corpo.

DEMONSTRAÇÃO. Denotaremos os elementos de D por letras minúsculas e os elementos de $R_Z = M_2(D)$ por maiúsculas.

Já vimos, no capítulo 0, que podemos estender d a uma derivação Δ em R_Z definida da seguinte forma: dado $XC^{-1}eR_Z$ com $X \in R$ e $C \in Z(R)^*$,

$$\Delta(XC^{-1}) = [d(X)C - Xd(C)]C^{-2}eR_Z.$$

Mas $R_Z = M_2(D)$ e o resultado de Polcino Milies em [PM] que se encontra no capítulo 0, teorema 0.19, implica que

$$\Delta = d_A + \bar{\delta}$$

onde d_A é a derivação interna dada por uma matriz $A \in M_2(D)$ e $\bar{\delta}$ é uma derivação de $M_2(D)$ induzida por uma derivação δ de D . Isto é, dada $\begin{bmatrix} x & y \\ t & w \end{bmatrix} \in M_2(D)$,

$$\begin{aligned} \Delta \left(\begin{bmatrix} x & y \\ t & w \end{bmatrix} \right) &= \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} x & y \\ t & w \end{bmatrix} - \begin{bmatrix} x & y \\ t & w \end{bmatrix} \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} + \\ &+ \begin{bmatrix} \delta(x) & \delta(y) \\ \delta(t) & \delta(w) \end{bmatrix} \end{aligned} \quad (1)$$

onde $A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$.

Observamos inicialmente que, como $R_Z = M_2(D)$ é simples e $I_Z = \{AC^{-1} \mid A \in I \text{ e } C \in Z(R)^*\}$ é um ideal não nulo de R_Z , então $I_Z = R_Z = M_2(D)$. Portanto, para todo $X \in M_2(D)$, temos que X é da forma $X = BC^{-1}$ com $B \in I$ e $C \in Z(R)^*$; logo $XC \in I$ e, da hipótese sobre d temos que existe um inteiro positivo $n = n(XC)$ tal que $d(XC)^n \in Z(R) \subset Z(M_2(D))$. Como $\Delta(Y) = d(Y) \quad \forall Y \in R$, temos: $\Delta(XC)^n \in Z(M_2(D))$. Fica claro que, se $S \in Z(R)$ então $XCSE \in I$ e também existe $m = n(XCS)$ tal que $\Delta(XCS)^m \in Z(M_2(D))$.

Vamos agora demonstrar que D é corpo, calculando valores da derivação Δ de $M_2(D)$. Suponhamos, por absurdo, que D não seja corpo, isto é, que D não seja comutativo. Vamos chegar à conclusão de que $d=0$, o que é absurdo.

Dado $x \in D$, consideremos $X = \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} \in M_2(D)$. Da observação acima, sabemos que existe $C \in Z(R)^* \subset Z(M_2(D))^*$ e $n = n(XC)$

tal que $\Delta(XC)^n \in Z(M_2(D))$. Ora, $Z(M_2(D)) = \left\{ \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix} \mid z \in Z(D) \right\}$; portanto C é da forma $C = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$ com $c \in Z(D)^*$ e de (1) temos:

$$\begin{aligned} \Delta(XC) &= \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} 0 & xc \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & xc \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} + \begin{bmatrix} 0 & \delta(xc) \\ 0 & 0 \end{bmatrix} = \\ &= \begin{bmatrix} -cxa_3 & a_1xc - xca_4 + \delta(xc) \\ 0 & cxa_3 \end{bmatrix} . \end{aligned}$$

Portanto, $\Delta(XC)^n$ é da forma

$$\Delta(XC)^n = \begin{bmatrix} c^n(-xa_3)^n & 0 \\ 0 & c^n(xa_3)^n \end{bmatrix} \in Z(M_2(D)).$$

e concluímos que $c^n(xa_3)^n \in Z(D)$. Mas $c \in Z(D)^*$ e D é anel com divisão, consequentemente $(xa_3)^n \in Z(D)$. Em suma, dado $x \in D$ qualquer, existe $n=n(x)$ tal que $(xa_3)^n \in Z(D)$. Mas, se $a_3 \neq 0$, então $Da_3 = D$ e teríamos: $\forall y \in D$ existe um inteiro positivo $n(y)=n$ tal que $y^n \in Z(D)$ o que pelo teorema 0.8, implicaria D comutativo. Concluímos, portanto, que $a_3 = 0$.

Dado $x \in D$ qualquer, tomando $X = \begin{bmatrix} 0 & 0 \\ x & 0 \end{bmatrix} \in M_2(D)$ e repetindo o raciocínio do parágrafo anterior, concluímos que $a_2 = 0$.

Portanto, $A = \begin{bmatrix} a_1 & 0 \\ 0 & a_4 \end{bmatrix}$ e Δ é da forma:

$$\begin{aligned} \Delta \left(\begin{bmatrix} x & y \\ t & w \end{bmatrix} \right) &= \begin{bmatrix} a_1 & 0 \\ 0 & a_4 \end{bmatrix} \begin{bmatrix} x & y \\ t & w \end{bmatrix} - \begin{bmatrix} x & y \\ t & w \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ 0 & a_4 \end{bmatrix} + \\ &+ \begin{bmatrix} \delta(x) & \delta(y) \\ \delta(t) & \delta(w) \end{bmatrix}. \end{aligned} \quad (2)$$

Consideremos agora $E = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(D)$. Pela observa

ção inicial, existe $C = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} \in Z(R)^* \subset Z(M_2(D))^*$ e $n = n(EC)$ tais que $EC \in I$ e $\Delta(EC)^n \in Z(M_2(D))$. Também pela mesma observação sabemos que $\forall S \in Z(R)^*$, $S = \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}$, $ECS \in I$, e portanto existe $m = n(ECS)$ tal que $\Delta(ECS)^m \in Z(M_2(D))$. Então, por (2), e pelo fato de que c e s pertencem a $Z(D)^*$, temos:

$$\Delta(EC)^n = \Delta \left(\begin{bmatrix} c & 0 \\ 0 & 0 \end{bmatrix} \right)^n = \begin{bmatrix} \delta(c)^n & 0 \\ 0 & 0 \end{bmatrix} \in Z(M_2(D))$$

e,

$$\Delta(ECS)^m = \Delta \left(\begin{bmatrix} cs & 0 \\ 0 & 0 \end{bmatrix} \right)^m = \begin{bmatrix} \delta(cs)^m & 0 \\ 0 & 0 \end{bmatrix} \in Z(M_2(D)).$$

Concluimos, pela forma dos elementos de $Z(M_2(D))$, que $\delta(c)^n = \delta(cs)^m = 0$ e, como D é anel com divisão, temos que $\delta(c) = \delta(cs) = 0$. Logo, $0 = \delta(cs) = c\delta(s)$ o que implica $\delta(s) = 0$.

Em suma, provamos que dado $S \in Z(R)^* \subset Z(M_2(D))^*$, S é da forma $S = \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}$, onde $s \in Z(D)^*$ e $\delta(s) = 0$.

Seja agora $x \in D$ qualquer e consideremos $X = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \in M_2(D)$. Novamente pela observação inicial, sabemos que existe $C \in Z(R)^*$ e um inteiro positivo $n = n(XC)$ tais que

$\Delta(XC)^n \in Z(M_2(D))$. Já vimos acima que se $C = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$, então $c \in Z(D)^*$ e $\delta(c) = 0$. Logo,

$$\Delta(XC)^n = \Delta \left(\begin{bmatrix} xc & 0 \\ 0 & 0 \end{bmatrix} \right)^n = \begin{bmatrix} c(a_1x - xa_1) + c\delta(x) & 0 \\ 0 & 0 \end{bmatrix}^n \in Z(M_2(D)).$$

Novamente, pela forma dos elementos de $Z(M_2(D))$, concluímos que $0 = (c(a_1x - xa_1) + c\delta(x))^n = c^n(a_1x - xa_1 + \delta(x))^n$. Finalmente, como $c \in Z(D)^*$ e D é anel com divisão, temos:

$$a_1x - xa_1 + \delta(x) = 0 \quad \forall x \in D.$$

Tomando $x \in D$ qualquer e $X = \begin{bmatrix} 0 & 0 \\ 0 & x \end{bmatrix} \in M_2(D)$, usando o mesmo raciocínio do parágrafo anterior, concluímos que

$$a_4x - xa_4 + \delta(x) = 0 \quad \forall x \in D.$$

Destas duas igualdades concluímos que $a_1 - a_4 \in Z(D)$ e que $\delta(x) = xa_1 - a_1x = xa_4 - a_4x$ para todo $x \in D$.

Seja novamente $x \in D$ qualquer e, $X = \begin{bmatrix} 0 & x \\ x & 0 \end{bmatrix} \in M_2(D)$,

$C = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} \in Z(R)^* \subset Z(M_2(D))^*$ e $n = n(XC)$ tal que

$\Delta(XC)^n \in Z(M_2(D))$. Então temos:

$$\begin{aligned}
\Delta \left(\begin{bmatrix} 0 & xc \\ xc & 0 \end{bmatrix} \right)^n &= \left(\begin{bmatrix} a_1 & 0 \\ 0 & a_4 \end{bmatrix} \begin{bmatrix} 0 & xc \\ xc & 0 \end{bmatrix} - \begin{bmatrix} 0 & xc \\ xc & 0 \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ 0 & a_4 \end{bmatrix} \right) + \\
&\quad + \begin{bmatrix} 0 & c(xa_1 - a_1x) \\ c(xa_4 - a_4x) & 0 \end{bmatrix}^n \\
&= \begin{bmatrix} 0 & cx(a_1 - a_4) \\ cx(a_4 - a_1) & 0 \end{bmatrix}^n \in Z(M_2(D)).
\end{aligned}$$

Ora, como $a_1 - a_4 \in Z(D)$, $\Delta(XC)^n$ é de uma das seguintes formas:

$$\begin{bmatrix} 0 & \pm c^n(a_1 - a_4)^n x^n \\ \pm c^n(a_1 - a_4)^n x^n & 0 \end{bmatrix}$$

ou

$$\begin{bmatrix} \pm c^n(a_1 - a_4)^n x^n & 0 \\ 0 & \pm c^n(a_1 - a_4)^n x^n \end{bmatrix}$$

dependendo se n for ímpar ou par. Mas pela forma dos elementos de $Z(M_2(D))$, sabemos que $\Delta(XC)^n \in Z(M_2(D))$, então $\Delta(XC)^n$ é do segundo tipo e $c^n(a_1 - a_4)^n x^n \in Z(D)$.

Em suma, concluimos que, para todo $x \in D$, existe $n=n(x)$ tal que:

$$c^n(a_1 - a_4)^n x^n \in Z(D).$$

Se $c(a_1 - a_4) \neq 0$ então para todo $x \in D$ existe $n=n(x)$ tal que $x^n \in Z(D)$ e, o teorema 0.8, nos garante que, neste caso, D é comutativo. Portanto $c(a_1 - a_4) = 0$ e, como $c \neq 0$, concluimos que $a_1 = a_4$.

Finalmente concluimos que para qualquer

$$\begin{bmatrix} x & y \\ t & w \end{bmatrix} \in M_2(D), \quad \text{temos:}$$

$$\begin{aligned} \Delta \left(\begin{bmatrix} x & y \\ t & w \end{bmatrix} \right) &= \begin{bmatrix} a_1 & 0 \\ 0 & a_1 \end{bmatrix} \begin{bmatrix} x & y \\ t & w \end{bmatrix} - \begin{bmatrix} x & y \\ t & w \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ 0 & a_1 \end{bmatrix} + \\ &+ \begin{bmatrix} xa_1 - a_1x & ya_1 - a_1y \\ ta_1 - a_1t & wa_1 - a_1w \end{bmatrix} = 0. \end{aligned}$$

Portanto $d=0$ e chegamos a uma contradição.

Logo, D é comutativo, isto é D é um corpo.

//

Já sabemos, portanto, que nas condições do teorema 3.1 ou nas condições do teorema 3.2, R é um anel primo, e R_Z o localizado de R em $Z(R)^*$ é um anel com divisão ou é um anel de matrizes 2×2 sobre um corpo. É claro que nestes dois casos R é uma ordem em R_Z , pois todo elemento de R que é regular, é inversível em R_Z .

No caso em que $R_Z = M_2(F)$ onde F é um corpo, já sabemos, portanto, que R é uma ordem numa álgebra simples de dimensão 4 sobre seu centro. Vamos agora estudar o caso em que $R_Z = D$ anel com divisão.

Primeiramente trataremos de mostrar que, se R_Z é um anel com divisão então, sob certas condições, $d(Z(R)) = 0$. Isto será demonstrado através de dois lemas que seguem.

Lembramos que se R é um anel primo, então $Z(R)$ é um domínio comutativo e portanto podemos definir o corpo de frações de $Z(R)$ que será denominado Q .

Usaremos aqui frequentemente o fato de que $d(Z(R)) \subset Z(R)$ que já foi provado no capítulo 0.

O lema que segue trata da cardinalidade de um subconjunto de Q .

3.9 - LEMA. Sejam R um anel primo, Q o corpo de frações de $Z(R)$ e d uma derivação em R . Se $d(Z(R)) \neq 0$ então $Z(R)$ é infinito e o subconjunto $\Omega \subset Q$ dado por $\Omega = \{d(\alpha)/\alpha \mid \alpha \in Z(R)^*\}$ tem a mesma cardinalidade de $Z(R)$.

DEMONSTRAÇÃO. Primeiramente vamos demonstrar que $Z(R)$ é in finito. De fato, como R é primo, $Z(R)$ é um domínio e portanto se $Z(R)$ é finito temos que $Z(R)$ é um corpo finito de característica $p > 0$. Ainda, como todo corpo finito é perfeito, então $Z(R)$ é perfeito, isto é, $\forall \alpha \in Z(R)$, $\alpha = \beta^p$ para algum $\beta \in Z(R)$. Mas, prova-se facilmente, por indução, que $d(\beta^p) = p\beta^{p-1}d(\beta) = 0 \quad \forall \beta \in Z(R)$. Concluimos então que $d(Z(R)) = 0$ chegando à uma contradição.

Vamos agora mostrar que, nas hipóteses acima, a cardinalidade de Ω igual à cardinalidade de $Z(R)$.

Denotaremos por $|A|$ a cardinalidade de um conjunto A qualquer. É claro que $|Q| = |Z(R) \times Z(R)^*| = |Z(R)|$ e, como $\Omega \subset Q$ temos $|\Omega| \leq |Z(R)|$. Resta-nos provar que $|\Omega| \geq |Z(R)|$.

Primeiramente vamos mostrar que se $K = \{\beta \in Z(R) \mid d(\beta) = 0\}$ e K^C é o complementar de K em $Z(R)$ então $|K^C| = |Z(R)|$. Fixemos $\alpha \in Z(R)$ com $d(\alpha) \neq 0$. Dado $\beta \in K$, $\beta \neq 0$, temes que $d(\alpha\beta) = d(\alpha)\beta \neq 0$, pois $Z(R)^*$ não tem divisores de zero. Portanto, a aplicação injetora $L_\alpha: K - \{0\} \rightarrow Z(R)$ dada por $L_\alpha(\beta) = \alpha\beta \quad \forall \beta \in K - \{0\}$ tem como imagem o conjunto $\text{Im}(L_\alpha) \subset K^C$. Concluimos então que $|K^C| \geq |K - \{0\}|$. Finalmente, como $K \cup K^C = Z(R)$ é infinito, então K^C é infinito e $|Z(R)| = \max\{|K|, |K^C|\} = |K^C|$ o que prova o que queríamos.

Agora, usando o fato de que $|K^C| = |Z(R)|$ e supondo, por absurdo, que $|\Omega| < |Z(R)|$ vamos chegar a uma contradição.

Consideremos $\Omega^* = \{d(\beta)/\beta \in \Omega \mid \beta \in K^C\} = \Omega - \{0\}$. Como $\Omega^* \subset \Omega$ e estamos supondo $|\Omega| < |Z(R)|$ é claro que $|\Omega^*| < |Z(R)|$.

Podemos construir uma aplicação $\psi: K^C \rightarrow \Omega^*$ dada por $\psi(\alpha) = d(\alpha)/\alpha \quad \forall \alpha \in K^C$. Denotaremos por $\psi^{-1}(d(\alpha)/\alpha)$ o subconjunto

$$\psi^{-1}\left(\frac{d(\alpha)}{\alpha}\right) = \left\{ \beta \in K^C \mid \frac{d(\beta)}{\beta} = \frac{d(\alpha)}{\alpha} \right\}.$$

É claro que $K^C = \bigcup_{\frac{d(\alpha)}{\alpha} \in \Omega^*} \psi^{-1}\left(\frac{d(\alpha)}{\alpha}\right)$ e, como K^C é infinito, temos:

$$|K^C| = \max_{\frac{d(\alpha)}{\alpha} \in \Omega^*} \left\{ |\Omega^*|, \left| \psi^{-1}\left(\frac{d(\alpha)}{\alpha}\right) \right| \right\}.$$

Mas $|\Omega^*| < |Z(R)| = |K^C|$, logo existe $\frac{d(\alpha)}{\alpha} \in \Omega^*$ tal que

$$\psi^{-1}\left(\frac{d(\alpha)}{\alpha}\right) = |K^C|.$$

Seja então $\Omega_\alpha = \left\{ \frac{d(\alpha^2 + \beta)}{\alpha^2 + \beta} \mid \beta \in \psi^{-1}\left(\frac{d(\alpha)}{\alpha}\right) \right\}$. É fácil ver que dado $\beta \in \psi^{-1}\left(\frac{d(\alpha)}{\alpha}\right)$ então $\alpha^2 + \beta \neq 0$. De fato, se $\alpha^2 + \beta = 0$ então

$$2d(\alpha)\alpha = -d(\beta) \quad \text{e, como} \quad \frac{d(\alpha)}{\alpha} = \frac{d(\beta)}{\beta}, \quad \text{temos}$$

$2d(\alpha)\alpha^2 = -d(\beta)\alpha = -d(\alpha)\beta$; mas $d(\alpha) \in Z(R)^*$, portanto $2\alpha^2 = -\beta$, o que com $\alpha^2 + \beta = 0$ nos dá $\alpha = 0$, uma contradição. É claro, portanto, que Ω_α está bem definido e $\Omega_\alpha \subset \Omega$. Vamos mostrar que

$|\Omega_\alpha| \geq |\psi^{-1}(\frac{d(\alpha)}{\alpha})| = |K^C| = |Z(R)|$ chegando à uma contradição.

Seja ϕ a aplicação que a cada $\beta \in \psi^{-1}(\frac{d(\alpha)}{\alpha})$ associa o elemento $\phi(\beta) = \frac{d(\alpha^2 + \beta)}{\alpha^2 + \beta} \in \Omega_\alpha$. É fácil ver que ϕ é injetora pois se

$$\frac{d(\alpha^2 + \beta)}{\alpha^2 + \beta} = \frac{d(\alpha^2 + \gamma)}{\alpha^2 + \gamma} \quad \text{com} \quad \beta \neq \gamma \in \psi^{-1}(\frac{d(\alpha)}{\alpha}) \quad \text{então}$$

$\frac{d(\alpha)}{\alpha} = \frac{d(\beta)}{\beta} = \frac{d(\gamma)}{\gamma}$ e, substituindo convenientemente na igualdade acima, obtemos:

$$\frac{d(\alpha^2 + \beta)}{\alpha^2 + \beta} = \frac{d(\alpha^2 + \gamma)}{\alpha^2 + \gamma}$$

implica

$$d(\alpha^2)\alpha^2 + d(\alpha^2)\gamma + d(\beta)\alpha^2 + d(\beta)\gamma = d(\alpha^2)\alpha^2 + d(\alpha^2)\beta + d(\gamma)\alpha^2 + d(\gamma)\beta,$$

que, por sua vez implica

$$2\alpha d(\alpha)\gamma + d(\beta)\alpha^2 = 2\alpha d(\alpha)\beta + d(\gamma)\alpha^2,$$

isto é

$$2\alpha d(\alpha)\gamma + d(\alpha)\alpha\beta = 2\alpha d(\alpha)\beta + d(\alpha)\alpha\gamma.$$

Mas então,

$$d(\alpha)\alpha\gamma = d(\alpha)\alpha\beta,$$

ou seja

$$d(\alpha)\alpha(\gamma - \beta) = 0.$$

Mas $\alpha \in K^C$, portanto $d(\alpha)\alpha \in Z(R)^*$ e $d(\alpha)\alpha(\gamma-\beta)=0$ se e somente se $\gamma=\beta$. Construímos, então uma aplicação injetora

$$\phi: \psi^{-1}\left(\frac{d(\alpha)}{\alpha}\right) \rightarrow \Omega_\alpha. \text{ Como } \left| \psi^{-1}\left(\frac{d(\alpha)}{\alpha}\right) \right| = |K^C| \text{ então}$$

$|K^C| \leq |\Omega_\alpha| = |\Omega|$ e chegamos a uma contradição que vem do fato de termos suposto $|\Omega| < |K^C|$. Portanto $|\Omega| \geq |K^C| = |Z(R)|$ e provamos o lema.

//

É óbvio que se R_Z é um anel com divisão, então R é um domínio. Fixaremos este resultado através da seguinte observação:

3.10 - OBSERVAÇÃO. Sejam R um anel primo e R_Z , o localiza do de R em $Z(R)^*$. Então R_Z é domínio se e somente se R é do mínio.

DEMONSTRAÇÃO. Como $R \subset R_Z$ é obvio que se R_Z é um domínio então R é um domínio.

Se, por outro lado, R é um domínio então dados rz^{-1} e $sw^{-1} \in R_Z$ temos que $(rz^{-1})(sw^{-1})=0$ implica $(rz^{-1})(sw^{-1})zw=rs=0$ e portanto $r=0$ ou $s=0$. Concluimos então a demonstração.

//

Vamos agora mostrar que sob certas condições, $d(Z(R))=0$ no caso em que R é um domínio.

3.11 - LEMA. Sejam R um domínio não comutativo, I ideal de R e d uma derivação em R tal que $d(I) \neq 0$ e, para todo $x \in I$, existe um inteiro $n(x) > 0$ tal que $d(x)^{n(x)} \in Z(R)$. Então $d(Z(R)) = 0$ se vale uma das seguintes condições:

(i) $Z(R)$ é finito.

(ii) existe n fixo tal que $d(x)^n \in Z(R) \quad \forall x \in I$.

(iii) $Z(R)$ é não enumerável.

DEMONSTRAÇÃO. O item (i) é uma consequência direta do lema 3.9 pois se $Z(R)$ é finito então $d(Z(R)) = 0$.

Resta-nos, então, demonstrar (ii) e (iii) no caso em que $Z(R)$ é infinito. Tanto na demonstração de (ii) quanto na de (iii) vamos supor por absurdo que $d(Z(R)) \neq 0$ e, para cada $x \in I$, montaremos um sistema de equações com coeficientes em Q , o corpo de frações de $Z(R)$. A solução deste sistema, será uma m -upla em Q^m da qual x^m é uma coordenada. Concluiremos, então que $x^m \in Z(R)$ e que R é comutativo chegando a uma contradição.

(ii) Suponhamos que $Z(R)$ é infinito e $d(x)^n \in I \quad \forall x \in I$. Também vamos supor, por absurdo, que $d(Z(R)) \neq 0$.

Fixemos $x \in I$ qualquer. Dado $\alpha \in Z(R)^*$, é claro que $\alpha x \in I$ e, $d(\alpha x)^n = (d(\alpha)x + \alpha d(x))^n \in Z(R)$. Então,

$$\left[\frac{d(\alpha)}{\alpha} x + d(x) \right]^n = \frac{d(\alpha x)^n}{\alpha^n} \in Q$$

onde Q é o corpo de frações de $Z(R)$. O desenvolvimento desta expressão nos dá uma igualdade da forma:

$$\left(\frac{d(\alpha)}{\alpha}\right)^n x^n + \left(\frac{d(\alpha)}{\alpha}\right)^{n-1} a_{n-1} + \dots + \frac{d(\alpha)}{\alpha} a_1 + d(x)^n = q_\alpha \in Q \quad (1)$$

onde os a_i $1 \leq i \leq n-1$ são somatórias de produtos envolvendo x e $d(x)$. Para cada $\alpha \in Z(R)^*$ existe $q_\alpha \in Q$ para o qual vale a igualdade (1).

Ora, como $d(Z(R)) \neq 0$ e $Z(R)$ é infinito, o lema 3.9 implica que $\Omega = \left\{ \frac{d(\alpha)}{\alpha} \in Q \mid \alpha \in Z(R)^* \right\}$ é infinito. Podemos então tomar $\alpha_1, \alpha_2, \dots, \alpha_{n+1} \in Z(R)^*$ tais que $\frac{d(\alpha_i)}{\alpha_i} \neq \frac{d(\alpha_j)}{\alpha_j}$ se $i \neq j$, e montar um sistema de $n+1$ equações com coeficientes em Q e $n+1$ incógnitas:

$$\begin{aligned} \left(\frac{d(\alpha_1)}{\alpha_1}\right)^n y_n + \left(\frac{d(\alpha_1)}{\alpha_1}\right)^{n-1} y_{n-1} + \dots + \frac{d(\alpha_1)}{\alpha_1} y_1 + y_0 &= q_{\alpha_1} \\ \cdot & \cdot \cdot \\ \cdot & \cdot \cdot \cdot \\ \cdot & \cdot \cdot \cdot \\ \left(\frac{d(\alpha_{n+1})}{\alpha_{n+1}}\right)^n y_n + \left(\frac{d(\alpha_{n+1})}{\alpha_{n+1}}\right)^{n-1} y_{n-1} + \dots + \frac{d(\alpha_{n+1})}{\alpha_{n+1}} y_1 + y_0 &= q_{\alpha_{n+1}} \end{aligned}$$

O determinante da matriz deste sistema é do tipo de Van der Monde dado por

$$\prod_{i < j} \left(\frac{d(\alpha_i)}{\alpha_i} - \frac{d(\alpha_j)}{\alpha_j} \right).$$

Pela escolha dos α_i o determinante é não nulo e portanto o sistema tem uma única solução $(y_n, y_{n-1}, \dots, y_1, y_0) \in Q^{n+1}$.

Ora, $(x^n, a_{n-1}, \dots, a_1, d(x)^n)$ é solução deste sistema; logo, $x^n \in Q$.

Em suma, dado $x \in I$, concluímos que $x^n \in Q$. Portanto $x^n \in Q \cap R = Z(R)$, e o teorema 0.8, implica que R é comutativo. Chegamos então a uma contradição que vem do fato de termos suposto $d(Z(R)) \neq 0$.

(iii) Suponhamos agora que $Z(R)$ é não enumerável e também, por absurdo, que $d(Z(R)) \neq 0$. Fixemos $x \in I$ qualquer e, para cada $\alpha \in Z(R)$ seja $m(\alpha) = \min\{n \in \mathbb{N}^* \mid d(\alpha x)^n \in Z(R)\}$.

Seja $\Omega = \left\{ \frac{d(\alpha)}{\alpha} \in Q \mid \alpha \in Z(R)^* \right\}$ e consideremos $\theta: \Omega \rightarrow \mathbb{N}^*$ dada por $\theta\left(\frac{d(\alpha)}{\alpha}\right) = m(\alpha)$. A aplicação θ está bem definida pois se $\frac{d(\alpha)}{\alpha} = \frac{d(\beta)}{\beta}$ então $d(\alpha x)^{m(\alpha)} = [d(\alpha)x + \alpha d(x)]^{m(\alpha)} \in Z(R)$ implica que $\left[\frac{d(\alpha)}{\alpha}x + d(x)\right]^{m(\alpha)} \in Q$, e portanto, $\left[\frac{d(\beta)}{\beta}x + d(x)\right]^{m(\alpha)} \in Q$.

Mas, neste caso, $[d(\beta)x + \beta d(x)]^{m(\alpha)} = \beta^{m(\alpha)} \left[\frac{d(\beta)}{\beta}x + d(x)\right]^{m(\alpha)} \in$

$\in Q \cap R = Z(R)$, e concluímos que $m(\alpha) \geq m(\beta)$. Da mesma forma te

mos que $m(\beta) \geq m(\alpha)$ e portanto $m(\alpha) = m(\beta)$.

A aplicação $\theta: \Omega \rightarrow \mathbb{N}^*$ está, portanto, bem definida e, temos: $\Omega = \bigcup_{m \in \mathbb{N}} \theta^{-1}(m)$. Como $Z(R)$ é não enumerável, o lema

3.9 implica que Ω é não enumerável. Então, como $|\Omega| = \max\{|\mathbb{N}|, |\theta^{-1}(m)|\}$ existe um inteiro $m > 0$ tal que $\theta^{-1}(m)$ é não enumerável.

Em suma, dado $x \in I$ existe um inteiro $m > 0$ tal que $\theta^{-1}(m) = \left\{ \frac{d(\alpha)}{\alpha} \in \Omega \mid d(\alpha x)^m \in Z(R) \right\}$ é não enumerável. Portanto da do $x \in I$ existem $m+1$ elementos $\alpha_1, \alpha_2, \dots, \alpha_{m+1} \in Z(R)$ tais

que $\frac{d(\alpha_i)}{\alpha_i} \neq \frac{d(\alpha_j)}{\alpha_j}$ se $i \neq j$ $1 \leq i, j \leq m+1$ e $d(\alpha_i x)^m \in Z(R)$ para

$1 \leq i \leq m+1$. Portanto, como no item (i), para cada α_i , $1 \leq i \leq m+1$,

existe $q_{\alpha_i} \in Q$ tal que $\left(\frac{d(\alpha_i)}{\alpha_i} x + d(x) \right)^m = q_{\alpha_i}$. Logo, a $m+1$ -upla

$(x^m, a_{m-1}, \dots, a_1, d(x)^m)$ é solução do sistema:

$$\begin{pmatrix} \frac{d(\alpha_1)}{\alpha_1} \end{pmatrix}^m y_m + \begin{pmatrix} \frac{d(\alpha_1)}{\alpha_1} \end{pmatrix}^{m-1} y_{m-1} + \dots + \frac{d(\alpha_1)}{\alpha_1} y_1 + y_0 = q_{\alpha_1}$$

$$\vdots$$

$$\begin{pmatrix} \frac{d(\alpha_{m+1})}{\alpha_{m+1}} \end{pmatrix}^m y_m + \begin{pmatrix} \frac{d(\alpha_{m+1})}{\alpha_{m+1}} \end{pmatrix}^{m-1} y_{m-1} + \dots + \frac{d(\alpha_{m+1})}{\alpha_{m+1}} y_1 + y_0 = q_{\alpha_{m+1}}$$

Novamente, a escolha dos α_i nos garante que o determinante do sistema, dado por

$$\prod_{i < j} \left(\frac{d(\alpha_i)}{\alpha_i} - \frac{d(\alpha_j)}{\alpha_j} \right),$$

é diferente de zero e portanto $(x^m, a_{m+1}, \dots, a_1, d(x)^m) \in Q^{m+1}$. Em particular temos $x^m \in Q \cap R = Z(R)$.

Em suma, dado $x \in I$, existe um inteiro $m(x) > 0$ tal que $x^{m(x)} \in Z(R)$ e, pelo teorema 0.8, concluímos que R é comutativo o que é uma contradição.

Portanto, $d(Z(R)) = 0$ e concluímos a demonstração do item (iii).

//

Temos agora certas condições sob as quais $d(Z(R)) = 0$ se R é um domínio. Mas se $d(Z(R)) = 0$, a extensão canônica da derivação d em R para uma derivação Δ em R_Z da da por

$$\Delta(rz^{-1}) = (d(r)z - rd(z))z^{-2}$$

se reduz à

$$\Delta(rz^{-1}) = d(r)z^{-1}.$$

O seguinte lema, mostra que as propriedades de d em I passam para Δ em R_Z :

3.12 - LEMA. Sejam R um domínio não comutativo com R_Z anel com divisão, I um ideal de R e d uma derivação em R tal que $d(I) \neq 0$ e para cada $x \in I$ existe um inteiro $n(x) > 0$ tal que $d(x)^{n(x)} \in Z(R)$. Então existe Δ uma derivação em R_Z para a qual são verdadeiras as seguintes afirmações:

- (i) se n é fixo então $\Delta(rz^{-1})^n \in Z(R_Z) \quad \forall rz^{-1} \in R_Z$.
- (ii) se $R(Z)$ é não enumerável então dado $rz^{-1} \in R_Z$, existe um inteiro $n(rz^{-1}) > 0$ tal que $\Delta(rz^{-1})^{n(rz^{-1})} \in Z(R_Z)$.

DEMONSTRAÇÃO. Definimos $\Delta: R_Z \rightarrow R_Z$ por $\Delta(rz)^{-1} = (d(r)z - rd(z))z^{-2} \quad \forall rz^{-1} \in R_Z$. Já vimos no capítulo 0 que Δ é uma derivação em R_Z e que $\Delta(r) = d(r) \quad \forall r \in R$. Além disto, se R_Z é um anel com divisão, R_Z é simples e, como, $I_Z = \{az^{-1} \mid a \in I\}$ é um ideal não nulo de R_Z , temos que $R_Z = I_Z$.

Vamos agora demonstrar separadamente (i) e (ii).

(i) Se n é fixo, o lema 3.11 implica que $d(Z(R)) = 0$ e portanto $\Delta(rz^{-1}) = d(r)z^{-1} \quad \forall rz^{-1} \in R_Z$. Mas $R_Z = I_Z$, portanto dado $az^{-1} \in R_Z$ podemos supor $a \in I$ e temos $d(a)^n \in Z(R)$. Logo,

$$\Delta(az^{-1})^n = (d(a)z^{-1})^n = d(a)^n z^{-n} \in Z(R_Z)$$

e provamos a afirmação (i).

(ii) Se $Z(R)$ é não enumerável, também pelo lema 3.11, sabemos que $d(Z(R)) = 0$. Também $R_Z = I_Z$ e, dado $az^{-1} \in R_Z$

podemos supor $a \in I$ e portanto existe $n(a) > 0$ tal que $d(a)^{n(a)} \in Z(R)$. Logo,

$$\Delta (az^{-1})^{n(a)} = (d(a)z^{-1})^{n(a)} = d(a)^{n(a)} z^{-n(a)} \in Z(R_Z),$$

o que prova a afirmação (ii).

//

Já sabemos, portanto que se R_Z é anel com divisão e $d(Z(R))=0$, então R é uma ordem em R_Z e, em R_Z , temos uma derivação Δ que satisfaz $\Delta(x)^{n(x)} \in Z(R_Z) \quad \forall x \in R_Z$. Resta provarmos que R_Z tem dimensão 4 sobre seu centro. Isto será analisado a seguir. Antes, porém vamos demonstrar alguns lemas.

3.13 - LEMA. Seja $R[x_1, x_2, \dots, x_n]$ um anel de polinômios em n variáveis não comutativas e G o subgrupo aditivo de $R[x_1, x_2, \dots, x_n]$ gerado pelo subconjunto

$$\left\{ \left(\sum_{i \in I} x_i \right)^n \mid I \subset \{1, 2, \dots, n\} \right\}.$$

Então:

$$\sum_{\sigma \in S_n} x_{\sigma(1)} \cdots x_{\sigma(n)} \in G.$$

onde S_n , é grupo das permutações de $\{1, 2, \dots, n\}$.

DEMONSTRAÇÃO. Consideremos o desenvolvimento de $(x_1+x_2+\dots+x_n)^n$. Denotaremos por $S(1)$ a soma dos termos que envolvem apenas uma variável $S(2)$ a soma dos termos que envolvem duas variáveis e assim por diante. Assim,

$$S(1)=x_1^n+x_2^n+\dots+x_n^n,$$

$$S(n)=\sum_{\sigma \in S_n} x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(n)} \quad \text{e}$$

$$(x_1+x_2+\dots+x_n)^n = S(1)+S(2)+\dots+S(n).$$

É fácil verificar que vale a seguinte fórmula:

$$S(m)=\sum_{1 \leq i_1 < i_2 < \dots < i_m \leq n} (x_{i_1}+x_{i_2}+\dots+x_{i_m})^n - \binom{n-1}{m-1} S(1) - \\ - \binom{n-2}{m-2} S(2) - \dots - \binom{n-m+1}{1} S(m-1)$$

para todo m com $2 \leq m \leq n$. Mas, para qualquer escolha de $i_1, i_2, \dots, i_m$ com $1 \leq i_1 < i_2 < \dots < i_m \leq n$ sabemos que $(x_{i_1}+\dots+x_{i_m})^n \in G$ e que $S(1)=x_1^n+x_2^n+\dots+x_n^n \in G$. Portanto, a fórmula acima aplicada indutivamente nos fornece $S(2) \in G$, $S(3) \in G$, ..., $S(n) \in G$, que é o que queríamos demonstrar.

//

3.14 - LEMA. Sejam D um anel com divisão não comutativo, $K=Z(D)$ e $d \neq 0$ uma derivação em D tal que existe um inteiro $n > 0$ com $d(a)^n \in K$ para todo $a \in D$. Consideremos $R = D \bigotimes_K E$ onde

E é um corpo, que contém K . Então existe uma derivação Δ em R que estende d e tal que para todo $r \in R$ $\Delta(r)^n \in Z(R) = K \bigotimes_K E$.

DEMONSTRAÇÃO. Dado $r = \sum_{i=1}^m a_i \bigotimes k_i \in R$, definimos

$$\Delta(r) = \sum_{i=1}^m d(a_i) \bigotimes k_i.$$

Lembrando que o lema 3.11 implica que $d(K) = 0$, é fácil ver que Δ está bem definida e é uma derivação em R .

Vamos provar que $\Delta(r)^n \in Z(R)$. Ora,

$$\begin{aligned} \Delta(r)^n &= \left(\sum_{i=1}^m d(a_i) \bigotimes k_i \right)^n = \\ &= \sum_{1 \leq i_1, i_2, \dots, i_n \leq m} d(a_{i_1}) d(a_{i_2}) \dots d(a_{i_n}) \bigotimes k_{i_1} k_{i_2} \dots k_{i_n} = \\ &= \sum_{1 \leq i_1 \leq i_2 \leq \dots \leq i_n \leq m} \left(\sum_{\sigma \in S_n} d(a_{i_{\sigma(1)}}) \dots d(a_{i_{\sigma(n)}}) \bigotimes k_{i_1} k_{i_2} \dots k_{i_n} \right). \end{aligned}$$

Ainda, fixados $i_1 \leq i_2 \leq \dots \leq i_n$ temos:

$$\sum_{k \in I} d(a_{i_k})^n \in K$$

para qualquer $I \subset \{1, 2, \dots, n\}$. Observamos ainda que isto ocorre mesmo se tivermos $a_{i_j} = a_{i_k}$ com $j \neq k$. Podemos, portanto, aplicar o lema anterior para concluir que

$$\sum_{\sigma \in S_n} d(a_{i_{\sigma(1)}}) \dots d(a_{i_{\sigma(n)}}) \in K,$$

o que demonstra que $\Delta(r)^n \in K \otimes E = Z(R)$.

//

3.15 - LEMA. Sejam D um anel com divisão não comutativo e tal que $K = Z(D)$ é não enumerável. Seja ainda $d \neq 0$ uma derivação em D tal que para cada $a \in D$ existe um inteiro $n(a) > 0$ que verifica $d(a)^{n(a)} \in Z(D) = K$. Consideremos $R = D \otimes_K E$ onde E é um

corpo que contém K . Então existe uma derivação Δ em R tal que para todo $r \in R$ existe $n(r) > 0$ que verifica

$$\Delta(r)^{n(r)} \in Z(R) = K \otimes E.$$

DEMONSTRAÇÃO. Da mesma que na proposição anterior, dado $r \in R$

$$r = \sum_{i=1}^m a_i \otimes k_i,$$

definimos:

$$\Delta(r) = \sum_{i=1}^m d(a_i) \otimes k_i$$

Novamente, o lema 3.11 implica que $d(K)=0$ e é fácil ver que Δ é uma derivação em R .

A demonstração de que dado $r \in R$ existe $n(r) > 0$ tal que $\Delta(r)^{n(r)} \in Z(R) = K \otimes E$ é, neste caso, trabalhosa.

Primeiramente, vamos fixar uma notação. Dados $x_1, \dots, x_m \in D$ e $n, t_1, \dots, t_m \in \mathbb{N}$ tais que $n = t_1 + t_2 + \dots + t_m$, denotaremos por

$$S_{t_1, t_2, \dots, t_m}^{(n)}(x_1, x_2, \dots, x_m)$$

à soma dos termos, que aparecem no desenvolvimento de $(d(x_1) + d(x_2) + \dots + d(x_m))^n$ em que $d(x_1)$ aparece t_1 vezes, $d(x_2)$ aparece t_2 vezes e, em geral, $d(x_i)$ aparece t_i vezes. É claro que:

$$\begin{aligned} & (d(x_1) + d(x_2) + \dots + d(x_m))^n = \\ &= \sum_{\substack{1 \leq t_1, t_2, \dots, t_m \leq n \\ t_1 + t_2 + \dots + t_m = n}} S_{t_1, t_2, \dots, t_m}^{(n)}(x_1, x_2, \dots, x_m) \end{aligned}$$

Ainda, denotaremos por $S_{t_1}^{(n)}(x_1, \dots, x_m)$ à soma dos termos em que $d(x_1)$ aparece t_1 vezes ($d(x_i)$ para $i > 1$ ficam livres);

$S_{t_1, t_2}^{(n)}(x_1, \dots, x_m)$ denotará a soma dos termos em que $d(x_1)$ aparece t_1 vezes e $d(x_2)$ aparece t_2 vezes ($d(x_i)$ para $i > 2$ ficam livres). Em geral, $S_{t_1, t_2, \dots, t_r}^{(n)}(x_1, \dots, x_m)$ para $r < m$ denotará a soma dos termos em que $d(x_1)$ aparece t_1 vezes, $\dots, d(x_r)$ aparece t_r vezes e não há restrição para $d(x_i)$ quando $i > r$. É claro que:

$$\begin{aligned}
 & S_{t_1, \dots, t_r}^{(n)}(x_1, \dots, x_m) = \\
 & = \sum_{\substack{1 \leq t_{r+1}, \dots, t_m \leq n \\ t_{r+1} + \dots + t_m = n - t_1 - \dots - t_r}} S_{t_1, \dots, t_m}^{(n)}(x_1, \dots, x_m).
 \end{aligned}$$

Seja agora $r \in \mathbb{R}$ fixado, da forma:

$$r = \sum_{i=1}^m a_i \otimes k_i.$$

Vamos mostrar que $\exists N \in \mathbb{N}^*$ tal que

$$S_{t_1, t_2, \dots, t_m}^{(N)}(a_1, a_2, \dots, a_m) \in Z(D)$$

para qualquer m -upla $(t_1, \dots, t_m)$ tal que $t_1 + t_2 + \dots + t_m = N$.

Sejam $\alpha_1, \alpha_2, \dots, \alpha_m \in K$ e consideremos

$$d\left(\sum_{i=1}^m \alpha_i a_i\right) = \sum_{i=1}^m \alpha_i d(a_i).$$

Pela hipótese sobre d sabemos que existe $n = n(\alpha_1, \alpha_2, \dots, \alpha_m) \in \mathbb{N}^*$ tal que

$$\left(\sum_{i=1}^m \alpha_i d(a_i)\right)^n \in K.$$

Seja $\phi_1: K \rightarrow \mathbb{N}^*$ dada por $\phi_1(\alpha) = n(\alpha, \alpha_2, \dots, \alpha_m)$. Como $\mathbb{N}^*$ é enumerável e $K = \bigcup_{n \in \mathbb{N}^*} \phi_1^{-1}(n)$ é não enumerável, então existe

$n_1 \in \mathbb{N}^*$ tal que $\phi_1^{-1}(n_1)$ é não enumerável. Portanto dado

$\beta \in \phi_1^{-1}(n_1)$ temos:

$$d(\beta a_1 + \alpha_2 a_2 + \dots + \alpha_m a_m)^{n_1} = \beta' \in K$$

e desenvolvendo a expressão obtemos:

$$\begin{aligned} & \beta^{n_1} S_{n_1}^{(n_1)}(a_1, \alpha_2 a_2, \dots, \alpha_m a_m) + \\ & + \beta^{n_1-1} S_{n_1-1}^{(n_1)}(a_1, \alpha_2 a_2, \dots, \alpha_m a_m) + \dots + \end{aligned}$$

$$+ \beta S_1^{(n_1)}(a_1, \alpha_2 a_2, \dots, \alpha_m a_m) +$$

$$+ S_0^{(n_1)}(a_1, \alpha_2 a_2, \dots, \alpha_m a_m) = \beta'$$

Portanto, escolhendo $\beta_1, \beta_2, \dots, \beta_{n_1+1}$ elementos distintos de $\phi_1^{-1}(n_1)$, todos não nulos, temos:

$$\begin{bmatrix} \beta_1^{n_1} & \beta_1^{n_1-1} & \dots & \beta_1 & 1 \\ \beta_2^{n_1} & \beta_2^{n_1-1} & \dots & \beta_2 & 1 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \beta_{n_1+1}^{n_1} & \beta_{n_1+1}^{n_1-1} & \dots & \beta_{n_1+1} & 1 \end{bmatrix} \begin{bmatrix} S_{n_1} \\ S_{n_1-1} \\ \cdot \\ \cdot \\ \cdot \\ S_0 \end{bmatrix} = \begin{bmatrix} \beta'_1 \\ \beta'_2 \\ \cdot \\ \cdot \\ \cdot \\ \beta'_{n_1+1} \end{bmatrix}$$

onde $S_i = S_i^{(n_1)}(a_1, \alpha_2 a_2, \dots, \alpha_m a_m)$ $0 \leq i \leq n_1$. O fato dos β_i serem distintos garante que o determinante da matriz acima, que é do tipo de Van der Monde, é não nulo dado por

$$\prod_{i>j} (\beta_i - \beta_j).$$

Portanto a matriz é inversível em $M_{n_1+1}(K)$ e temos

$(s_{n_1}, s_{n_1-1}, \dots, s_0) \in K^{n_1+1}$. Em suma dados $\alpha_2, \dots, \alpha_m \in K$ existe $n_1 = n_1(\alpha_2, \dots, \alpha_m) > 0$ tal que

$$s_t^{(n_1)}(a_1, \alpha_2 a_2, \dots, \alpha_m a_m) \in K \quad \forall t \quad 0 \leq t \leq n_1.$$

Faremos agora um segundo passo, construindo a aplicação $\phi_2: K \rightarrow \mathbb{N}^*$ dada por

$$\phi_2(\alpha) = n_1(\alpha, \alpha_3, \dots, \alpha_m).$$

Da mesma forma, existe $n_2 \in \mathbb{N}^*$ tal que $\phi_2^{-1}(n_2)$ é não enumerável e, dado $\beta \in \phi_2^{-1}(n_2)$ temos:

$$s_t^{(n_2)}(a_1, \beta a_2, \alpha_3 a_3, \dots, \alpha_m a_m) = \beta' \in K \quad \forall t \quad 0 \leq t \leq n_2.$$

Ora,

$$\begin{aligned} s_t^{(n_2)}(a_1, \beta a_2, \alpha_3 a_3, \dots, \alpha_m a_m) &= \\ &= \beta^{n_2-t} s_{t, n_2-t}^{(n_2)}(a_1, a_2, \alpha_3 a_3, \dots, \alpha_m a_m) + \end{aligned}$$

$$\begin{aligned}
& + \beta^{n_2-t-1} S_{t,n_2-t-1}^{(n_2)}(a_1, a_2, \alpha_3 a_3, \dots, \alpha_m a_m) + \dots + \\
& + \beta S_{t,1}^{(n_2)}(a_1, a_2, \alpha_3 a_3, \dots, \alpha_m a_m) + \\
& + S_{t,0}^{(n_2)}(a_1, a_2, \alpha_3 a_3, \dots, \alpha_m a_m).
\end{aligned}$$

Portanto, escolhendo $\beta_1, \beta_2, \dots, \beta_{n_2+1}$ elementos não nulos e distintos de $\phi_2^{-1}(n_2)$ obtemos:

$$\begin{bmatrix}
\beta_1^{n_2-t} & \beta_1^{n_2-t-1} & \dots & \beta_1 & 1 \\
\beta_2^{n_2-t} & \beta_2^{n_2-t-1} & \dots & \beta_2 & 1 \\
\cdot & \cdot & & \cdot & \cdot \\
\cdot & \cdot & & \cdot & \cdot \\
\cdot & \cdot & & \cdot & \cdot \\
\beta_{n_2+1}^{n_2-t} & \beta_{n_2+1}^{n_2-t-1} & & \beta_{n_2+1} & 1
\end{bmatrix}
\begin{bmatrix}
S_{t,n_2-t} \\
S_{t,n_2-t-1} \\
\cdot \\
\cdot \\
\cdot \\
S_{t,0}
\end{bmatrix}
=
\begin{bmatrix}
\beta'_1 \\
\beta'_2 \\
\cdot \\
\cdot \\
\cdot \\
\beta'_{n_2+1}
\end{bmatrix},$$

onde $S_{t,k} = S_{t,k}^{(n_2)}(a_1, a_2, \alpha_3 a_3, \dots, \alpha_m a_m) \quad \forall k, \quad 0 \leq k \leq n_2 - t.$

Pelos mesmos argumentos anteriormente utilizados, concluimos que:

$$s_{t,k}^{(n_2)}(a_1, a_2, \alpha_3 a_3, \dots, \alpha_m a_m) \in K \quad \forall k, \quad 0 \leq k \leq n_2 - t.$$

Mas isto vale para todo t , com $0 \leq t \leq n_2$. Em suma, concluimos que dados $m-2$ elementos de K , $\alpha_3, \alpha_4, \dots, \alpha_m$, existe $n_2 = n_2(\alpha_3, \alpha_4, \dots, \alpha_m)$ tal que

$$s_{t,k}^{(n_2)}(a_1, a_2, \alpha_3 a_3, \dots, \alpha_m a_m) \in K \quad \forall t, k$$

$$0 \leq t \leq n_2, \quad 0 \leq k \leq n_2 - t.$$

Utilizando este mesmo procedimento m vezes, acabaremos por concluir que existe $N \in \mathbb{N}^*$, $N = N(a_1, a_2, \dots, a_m)$ tal que

$$s_{t_1, t_2, \dots, t_m}^{(N)}(a_1, a_2, \dots, a_m) \in K$$

para quaisquer $t_1, t_2, \dots, t_m$ com $t_1 + t_2 + \dots + t_m = N$, que é o que queríamos demonstrar.

Finalmente, para $N \in \mathbb{N}^*$ que obtivemos acima, temos:

$$\Delta(r)^N = \left(\sum_{i=1}^m d(a_i) \otimes k_i \right)^N =$$

$$= \sum_{\substack{0 \leq t_1, t_2, \dots, t_m \leq N \\ t_1 + t_2 + \dots + t_m = N}} s_{t_1, t_2, \dots, t_m} (a_1, \dots, a_m) \otimes k_1^{t_1} k_2^{t_2} \dots k_m^{t_m} \in$$

$$\in K \otimes E = Z(R).$$

//

Queremos trabalhar com o anel $R = D \otimes_K E$ onde $K = Z(D)$

e E é um corpo que contém K . Vamos tomar E , o fecho algébrico de K . A seguinte proposição nos dá uma condição suficiente para que $E \neq K$.

3.16 - PROPOSIÇÃO. Seja R um domínio não comutativo tal que $K = Z(R)$ é um corpo. Se existem $r \in R$, $r \notin K$ e $n \in \mathbb{N}^*$ tais que $r^n \in K$ então K não é algebricamente fechado.

DEMONSTRAÇÃO. Suponhamos por absurdo que $r^n \in K$, $r \notin K$ e K é algebricamente fechado.

Seja $m = \min\{n \in \mathbb{N}^* \mid r^n \in K\}$. Como $r^m \in K$ e K é algebricamente fechado existe $k \in K$ tal que $r^m = k^m$. Como $r \notin K$, temos $r \neq 0$ e, conseqüentemente, $r^m \neq 0$ e $k \neq 0$.

Vamos provar que o polinômio $f(X) = X^m - k^m \in K(X)$ não tem raízes múltiplas em K . Ora, se $k_0 \in K$ é uma raiz múltipla de $f(X)$ então k_0 também é raiz de $f'(X) = mX^{m-1}$ e portanto

$mk_0^{m-1}=0$. Além disto, como $k_0^m=k^m \neq 0$, então $k_0 \neq 0$. Se $\text{car} R=0$ então $mk_0^{m-1}=0$ implica que $k_0=0$, uma contradição. Se $\text{car} R=p>0$ então $mk_0^{m-1}=0$ e $k_0 \neq 0$ implicam que $p|m$. Neste caso teríamos $m=p^\alpha \cdot q$ onde $\alpha \geq 1$ e $\text{mdc}(p,q)=1$; Logo, $0=r^{p^\alpha \cdot q}-k^{p^\alpha \cdot q}=(r^q-k^q)^{p^\alpha}$ que implica $r^q-k^q=0$. Mas então, $r^q \in K$ e $q < m$ o que contradiz a escolha de m . Chegamos portanto à conclusão de $f(X)$ tem m raízes distintas de K .

Sejam $k_1, k_2, \dots, k_m$ as raízes de $f(X)$ em K , É claro que $r^m=k_i^m \quad \forall i \quad 1 \leq i \leq m$, portanto:

$$0=(k_i^m-r^m)=(k_i-r)(k_i^{m-1}+k_i^{m-2}r+\dots+k_i r^{m-2}+r^{m-1}).$$

Mas, como $r \notin K$, temos $k_i-r \neq 0$ e portanto,

$$k_i^{m-1}+k_i^{m-2}r+\dots+k_i r^{m-2}+r^{m-1}=0.$$

Logo, temos a seguinte igualdade em $M_m(R)$:

$$\begin{bmatrix} k_1^{m-1} & k_1^{m-2} & \dots & k_1 & 1 \\ k_2^{m-1} & k_2^{m-2} & \dots & k_2 & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ k_m^{m-1} & k_m^{m-2} & \dots & k_m & 1 \end{bmatrix} \begin{bmatrix} 1 \\ r \\ \vdots \\ r^{m-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Porém o determinante da matriz da equação acima é dado por $\prod_{i < j} (k_i - k_j)$.

Como $k_i \neq k_j$, se $i \neq j$, sabemos que este determinante é não nulo e portanto a matriz é inversível em $M_m(K) \subset M_m(R)$. Neste caso, concluímos que $(1, r, \dots, r^{m-1}) = (0, 0, \dots, 0)$ o que é absurdo.

Chegamos então a um absurdo que vem do fato de termos suposto K algebricamente fechado.

//

3.17 - COROLÁRIO. Sejam D um anel com divisão não comutativo e $d \neq 0$ uma derivação em D tal que $d(r)^{n(r)} \in Z(D) \quad \forall x \in D$. Então $Z(D)$ não é algebricamente fechado.

DEMONSTRAÇÃO. Basta mostrarmos que $d(D) \not\subset Z(D)$ e aplicar o lema anterior.

Suponhamos, por absurdo, que $d(D) \subset Z(D)$; vamos chegar a uma contradição mostrando que $d=0$.

Sejam x e $y \in D$ quaisquer. Então:

$$\begin{aligned} 0 &= d(xy)x - xd(xy) = \\ &= d(x)yx + xd(y)x - xd(x)y - x^2d(y) = d(x)(yx - xy) \end{aligned}$$

pois $d(x)$, $d(y)$ e $d(xy) \in Z(D)$. Concluimos portanto que se $x \notin Z(D)$ então $d(x)=0$.

Sejam agora $z \in Z(D)$ e $a \notin Z(D)$. Então $d(a)=0$ e, como $a+z \in Z(D)$, também temos $d(a+z)=0$. Logo, $d(z)=d(a+z)-d(a)=0$. Portanto, $d(D)=0$ e chegamos a uma contradição.

//

Estamos agora aptos a provar o seguinte teorema:

3.18 - TEOREMA. Sejam D um anel com divisão não comutativo, $K=Z(D)$ e $d \neq 0$ uma derivação em D tal que $d(a)^{n(a)} \in K$ $\forall a \in D$. Suponhamos ainda que vale uma das seguintes condições:

(i) existe $n \in \mathbb{N}$ fixo tal que $d(a)^n \in K$.

(ii) K é não enumerável.

Então $\dim_K D = 4$.

DEMONSTRAÇÃO. O corolário 3.17 implica que K não é algebricamente fechado. Seja $\bar{K}$ o fecho algébrico de K e consideremos $R = D \bigotimes_K \bar{K}$.

Se vale a condição (i) o lema 3.14 implica que existe Δ , uma derivação em R , tal que $\Delta(r)^n \in Z(R) = 1 \bigotimes_K \bar{K}$. Se vale a condição (ii) é o lema 3.15 que implica que existe uma derivação Δ , em R , tal que $\Delta(r)^{n(r)} \in Z(R) = 1 \bigotimes_K \bar{K}$. Mas, em

tão, em ambos os casos, o corolário 3.7 e a proposição 3.8 implicam que R_Z , o localizado de R em $Z(R)^*$, é um anel com divisão ou $R_Z = M_2(F)$ onde F é um corpo.

Como $Z(R) = 1 \bigotimes_K \bar{K} = \bar{K}$ temos que $Z(R)$ é um corpo. Neste caso, $R_Z = R$ e concluímos que R é um anel com divisão ou $R = M_2(F)$ onde F é um corpo.

Se R é um anel com divisão, então o corolário 3.17 implica que $Z(R)$ não é algebricamente fechado. Por outro lado, $Z(R) = \bar{K}$ é algebricamente fechado, o que é absurdo. Logo, $R = M_2(F)$ onde F é um corpo.

Finalmente, $R = M_2(F)$ implica que

$$\dim_{Z(R)} R = \dim_F M_2(F) = 4$$

Ainda por um conhecido resultado de produtos tensoriais temos:

$$\dim_{\bar{K}} D \otimes_K K = \dim_K D,$$

e portanto, como $R = D \otimes_K \bar{K}$ e $Z(R) = \bar{K}$, concluímos que

$$\dim_K D = 4.$$

//

Com os resultados que provamos até aqui estamos aptos a demonstrar o teorema 3.2 e o teorema 3.1 excetuando-se a afirmação (iv). Vamos agora demonstrar um lema que será utilizado na demonstração da afirmação (iv). Em seguida faremos a demonstração do teorema 3.1 detendo-se apenas nesta última afirmação que exigirá novos recursos.

3.19 - LEMA. Sejam R um domínio tal que $Z(R) \neq 0$ e G um grupo abeliano, que é não enumerável e ordenado. Sejam d uma derivação em R e $I \neq 0$ um ideal de R . Então o anel de grupo RG é um domínio, $Z(RG) = Z(R)G$ e não enumerável; IG é um ideal não nulo de RG e existe uma derivação Δ em RG que estende d .

DEMOSTRAÇÃO. Em primeiro lugar vamos provar que RG é um domínio.

Dado $x \in RG$, $x = \sum_{g \in G} x(g)g$, denotaremos por $\text{supp}(x)$ ao subconjunto finito de G dado por:

$$\text{supp}(x) = \{g \in G \mid x(g) \neq 0\}.$$

Dados a e $b \in RG$ ambos não nulos sejam $g_0 = \max \text{supp}(a)$ e $h_0 = \max \text{supp}(b)$. Como a e b são não nulos então $a(g_0) \neq 0$ e $b(h_0) \neq 0$. Além disto, se $g \in \text{supp}(a)$ e $h \in \text{supp}(b)$ com $g \neq g_0$ e $h \neq h_0$ então $g < g_0$ e $h < h_0$ o que implica $gh < g_0 h_0$. Portanto $ab = \sum_{g \in G} r(g)g$ onde $r(g_0 h_0) = a(g_0)b(h_0) \neq 0$ o que implica $ab \neq 0$.

Provamos então que RG é um domínio.

Se $IG = \{x \in RG \mid x(g) \in I \ \forall g \in G\}$ é claro que IG é um ideal de RG . Além disto, se $I \neq 0$, é claro que $IG \neq 0$.

Também é claro que, como $Z(R) \neq 0$, então para qualquer $\alpha \in Z(R)^*$, $\alpha G \subset Z(R)G = Z(RG)$. Mas, αG é não enumerável, portanto $Z(RG)$ é não enumerável.

Se d é uma derivação em R , definimos $\Delta: RG \rightarrow RG$ da seguinte maneira: dado $x = \sum_{g \in G} x(g)g$,

$$\Delta(x) = \sum_{g \in G} d(x(g))g.$$

É fácil ver que Δ é uma derivação em RG , pois dados x e $y \in RG$, da forma, $x = \sum_{g \in G} x(g)g$ e $y = \sum_{g \in G} y(g)g$, temos:

$$\begin{aligned}
 1) \quad \Delta(x+y) &= \Delta \left[\sum_{g \in G} (x(g) + y(g))g \right] = \sum_{g \in G} d(x(g) + y(g))g = \\
 &= \sum_{g \in G} d(x(g))g + \sum_{g \in G} d(y(g))g = \Delta(x) + \Delta(y)
 \end{aligned}$$

$$2) \quad \Delta(xy) = \Delta \left[\sum_{g \in G} (xy)(g)g \right],$$

$$\text{onde } (xy)(g) = \sum_{hh'=g} x(h)y(h').$$

Portanto,

$$\begin{aligned}
 \Delta(xy) &= \sum_{g \in G} \left[\sum_{hh'=g} d(x(h)y(h')) \right] g = \\
 &= \sum_{g \in G} \left[\sum_{hh'=g} d(x(h))y(h') + x(h)d(y(h')) \right] g = \\
 &= \sum_{g \in G} \left[\sum_{hh'=g} d(x(h))y(h') \right] g + \sum_{g \in G} \left[\sum_{hh'=g} x(h)d(y(h')) \right] g = \\
 &= \Delta(x)y + x\Delta(y).
 \end{aligned}$$

É claro que dado $r \in R$, $\Delta(r) = d(r)$ e concluímos a demonstração do lema.

//

DEMONSTRAÇÃO DO TEOREMA 3.1.

(i) e (ii). O lema 3.4 e a proposição 3.5 implicam que R é primo. Então, pelo corolário 3.7 e, pela proposição 3.8, sabemos que R_Z é um anel com divisão ou $R_Z = M_2(F)$ onde F é um corpo. Obviamente, em ambos os casos R é uma ordem em R_Z .

Ora, pela observação 3.10, sabemos que se R é domínio então R_Z é anel com divisão e se R não é domínio então $R_Z = M_2(F)$. Estão provadas as afirmações (i) e (ii).

(iii) se R é um domínio, então R_Z é um anel com divisão. No caso em que R_Z é comutativo, temos que R é comutativo o que é absurdo. Se, por outro lado R_Z é não comutativo o lema 3.12, item (ii), define uma derivação em R_Z que está nas condições do teorema 3.18, item (ii). Concluímos, então, que $\dim_{Z(R_Z)} R_Z = 4$, finalizando a demonstração de (iii).

(iv) neste caso, R é um domínio e $\text{car} R = p > 0$. Consideremos um anel de grupo, RG , onde G é um grupo abelino, ordenado e não enumerável (por exemplo $(\mathbb{R}, +)$). Já vimos no lema 3.19 que RG é um domínio, IG é um ideal de RG , $Z(RG) = Z(R)G$ é não enumerável e $\Delta: RG \rightarrow RG$ definida por

$$\Delta \left[\sum_{g \in G} a(g)g \right] = \sum_{g \in G} d(a(g))g \quad \forall a = \sum_{g \in G} a(g)g \in RG$$

é uma derivação em RG.

Vamos mostrar que dado $a \in IG$, da forma, $a = \sum_{g \in G} a(g)g$, existe um inteiro $n = n(a) > 0$ tal que:

$$\Delta(a)^{n(a)} \in Z(RG).$$

Seja $\text{supp } a = \{g \in G \mid a(g) \neq 0\} = \{g_1, g_2, \dots, g_t\}$. Denotando $a(g_i)$ por a_i $1 \leq i \leq t$, temos:

$$a = \sum_{i=1}^t a_i g_i, \quad \text{com } a_i \in I$$

Consideremos A, o subconjunto de R, dado por:

$$A = \{z_1 d(a_1) + z_2 d(a_2) + \dots + z_t d(a_t) \in R \mid z_1, z_2, \dots, z_t \text{ são inteiros}\}$$

Como $\text{car } R = p > 0$ este conjunto é finito. Ainda, da hipótese sobre a derivação em I, temos: para cada $r \in A$ existe $n(r) > 0$ tal que $r^{n(r)} \in Z(R)$. Tomando $n = n(a) = t \prod n(r)$, é claro que para todo $r \in A$ temos que $r^n \in Z(R)$.

Vamos provar que $\Delta(a)^n \in Z(RG) = Z(R)G$. É claro que:

$$\Delta(a)^n = \left(\sum_{i=1}^t d(a_i) g_i \right)^n = \sum_{g \in G} b(g),$$

onde

$$\begin{aligned} b(g) &= \sum_{\substack{g_{i_1} g_{i_2} \dots g_{i_n} = g}} d(a_{i_1}) \dots d(a_{i_n}) = \\ &= \sum_{\substack{g_{i_1} g_{i_2} \dots g_{i_n} = g \\ 1 \leq i_1 \leq i_2 \leq \dots \leq i_n \leq t}} \sum_{\sigma \in S_n} d(a_{i_{\sigma(1)}}) \dots d(a_{i_{\sigma(n)}}). \end{aligned}$$

Ainda, fixados $i_1 \leq i_2 \leq \dots \leq i_n$, pela escolha de n , é claro que

$$\left(\sum_{j \in J} d(a_{i_j}) \right)^n \in Z(R),$$

para qualquer subconjunto $J \subset \{1, 2, \dots, n\}$. Portanto, pelo lema 3.13, temos que

$$\sum_{\sigma \in S_n} d(a_{i_{\sigma(1)}}) \dots d(a_{i_{\sigma(n)}}) \in Z(R),$$

o que demonstra $\Delta(a)^n = \Delta(a)^{n(a)} \in Z(RG) = Z(R)G$.

Portanto, RG é um domínio tal que RG , Δ e IG es tão nas condições do item anterior. Concluimos então que

RG é uma ordem em RG_Z , o localizado de RG em $Z(RG)^*$ e $\dim_{\mathcal{L}} RG_Z \leq 4$ onde $\mathcal{L} = Z(RG_Z)$.

Vamos provar que, neste caso, $\dim_{Z(R_Z)} R_Z \leq 4$.

Utilizaremos, para tanto, a inclusão canônica $i: R_Z \rightarrow RG_Z$ dada por: $i(r\alpha^{-1}) = \sum_{g \in G} a(g)g$ onde $a(g) = r\alpha^{-1}$ se $g=1$ e $a(g)=0$ se $g \neq 1$. É claro que $i(Z(R)) \subset \mathcal{L}$. Temos então o diagrama:

$$\begin{array}{ccc} R_Z & \xhookrightarrow{i} & RG_Z \\ \uparrow & & \uparrow \\ Z(R) & \xhookrightarrow{i} & \mathcal{L} \end{array}$$

Dados $r_1\alpha_1^{-1}, r_2\alpha_2^{-1}, \dots, r_5\alpha_5^{-1} \in R_Z$ com $r_i \in R$ e $\alpha_i \in Z(R)^*$, consideremos $r_i\alpha_i^{-1}$ como elementos de RG_Z . Como $\dim_{\mathcal{L}} RG_Z \leq 4$, existem elementos $\gamma_i\beta_i^{-1} \in \mathcal{L}$, onde $\gamma_i = \sum_{g \in G} \gamma_i(g)g$, $\beta_i = \sum_{g \in G} \beta_i(g)g \in Z(R)G$, são tais que $\sum_{i=1}^5 \gamma_i\beta_i^{-1}r_i\alpha_i^{-1} = 0$ e $\gamma_i \neq 0$ para algum i , $1 \leq i \leq 5$.

Multiplicando a igualdade acima por $\beta_1\beta_2 \dots \beta_5$ obtemos:

$$\sum_{i=1}^5 \gamma'_i r_i \alpha_i^{-1} = 0,$$

onde,

$$\gamma'_i = \sum_{g \in G} \gamma'_i(g) g \in Z(R)G$$

e $\gamma'_i \neq 0$ para algum i $1 \leq i \leq 5$.

Sem perda de generalidade, podemos supor que $\gamma'_1 \neq 0$ e portanto, que existe $g \in G$ tal que $\gamma'_1(g) \neq 0$. Neste caso temos:

$$0 = \sum_{i=1} \gamma'_i r_i \alpha_i^{-1}(g) = \sum_{i=1} \gamma'_1(g) r_i \alpha_i^{-1}.$$

Portanto $\gamma'_1(g), \gamma'_2(g), \dots, \gamma'_5(g)$ são elementos de $Z(R) \subset Z(R_Z)$ com $\gamma'_1(g) \neq 0$ e tais que:

$$\sum_{i=1} \gamma'_i(g) r_i \alpha_i^{-1} = 0.$$

Concluimos, portanto, que $r_1 \alpha_1^{-1}, \dots, r_5 \alpha_5^{-1}$ são l.d. e consequentemente, que:

$$\dim_{Z(R_Z)} R_Z \leq 4.$$

Já sabemos também que R_Z é um anel com divisão ou $R_Z = M_2(F)$ onde F é um corpo. Em ambos os casos, é claro que R é uma ordem em R_Z e concluimos a demonstração da afirmação (iv).

//

DEMONSTRAÇÃO DO TEOREMA 3.2.

O lema 3.3 e a proposição 3.5 implicam que R é primo. Então pelo corolário 3.7 e pela proposição 3.8, concluimos que R_Z , o localizado de R em $Z(R)^*$, é um anel com divisão ou $R_Z = M_2(F)$ onde F é um corpo.

No caso em que $R_Z = M_2(F)$, R é uma ordem em R_Z , $\dim_{Z(R_Z)} R_Z = 4$ e temos o resultado que queríamos.

Suponhamos que R_Z é um anel com divisão. Se R_Z for comutativo então R_Z é um corpo e portanto R é comutativo, o que é absurdo. Se R_Z for não comutativo o lema 3.12, item (i), implica que existe uma derivação Δ em R_Z tal que $\Delta(rz^{-1})^n \in Z(R_Z)$, para todo $rz^{-1} \in R_Z$. Portanto R_Z e Δ estão nas condições do item (i) do teorema 3.18. Logo, concluimos que $\dim_{Z(R_Z)} R_Z = 4$, finalizando a demonstração do teorema.

//

Para finalizar este capítulo daremos um exemplo que mostra que, tanto no teorema 3.1 quanto no teorema 3.2, não podemos enfraquecer a hipótese de que $d(x)^{n(x)} \in Z_p(R)$, substituindo-a por $d(z)^{n(x)} \in Z(R)$.

3.20 - EXEMPLO. Seja R o anel das funções $f: R \rightarrow R$ com a soma e o produto usual de funções. Consideremos $M_2(R)$. Vamos provar que $M_2(R)$ não tem ideais à direita nil não nulos.

Seja L , um ideal à direita nil de $M_2(R)$ e

$$A = \begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix} \in L.$$

Então $AE_{ij} \in L$ $1 \leq i, j \leq 2$ e portanto AE_{ij} é nilpotente. Pela forma das matrizes AE_{ij} obtemos que f_1, f_2, f_3 e f_4 são nilpotentes e, como R não contém elementos nilpotentes não nulos, concluímos que $A=0$. Portanto $M_2(R)$ não contém ideais à direita nil não nulos e consequentemente $M_2(R)$ é semiprimo.

Consideremos agora a derivação interna em $M_2(R)$ dada pela matriz

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_2(R),$$

$$d \left(\begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix} \right) =$$

$$= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix} - \begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} f_3 & f_4 - f_1 \\ 0 & -f_3 \end{bmatrix},$$

para qualquer $\begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix} \in M_2(R)$. É claro que:

$$d\left(\begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix}\right)^2 = \begin{bmatrix} f_3^2 & 0 \\ 0 & f_3^2 \end{bmatrix} \in Z(M_2(R)).$$

Observamos que $d\left(\begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix}\right)$ pode não ser regular

basta para isto que f_3 não seja regular (isto é, basta que $\exists x_0 \in R$ tal que $f_3(x_0)=0$).

Vamos provar que todo elemento regular de $M_2(R)$ é

invertível. Ora, se $\begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix} \in M_2(R)$ é regular é fácil ver que f_1, f_2, f_3 e f_4 são regulares em R . Ainda, se existe $x_0 \in R$ tal que $f_1(x_0)f_4(x_0) - f_2(x_0)f_3(x_0) = 0$, tomando $g \in R$ dada por:

$$g(x) = \begin{cases} 0 & \text{se } x \neq x_0 \\ 1 & \text{se } x = x_0 \end{cases}$$

temos:

$$\begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix} \begin{bmatrix} f_4 g & f_4 g \\ -f_3 g & -f_3 g \end{bmatrix} = 0,$$

o que contradiz a hipótese $\begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix}$ regular, Portanto,

$f_1(x)f_4(x)-f_2(x)f_3(x)\neq 0 \quad \forall x \in R$ e conseqüentemente existe $h \in R$, $h=(f_1f_4-f_2f_3)^{-1}$. Neste caso,

$$\begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix} \begin{bmatrix} f_4h & -f_2h \\ -f_3h & f_1h \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

isto é, $\begin{bmatrix} f_1 & f_2 \\ f_3 & f_4 \end{bmatrix}$ é inversível em $M_2(R)$.

Concluimos então que $M_2(R)$ só pode ser uma ordem no próprio $M_2(R)$. Ainda, como R não é simples (por exemplo $I=\{f \in R \mid f(0)=0\}$ é ideal de R), então $M_2(R)$ também não é simples e portanto $M_2(R)$ não pode ser uma ordem numa álgebra simples.

Para finalizar, lembramos o resultado de Skolem-Nöether citado no capítulo zero: "Se A é uma álgebra simples de dimensão finita sobre seu centro F e d é uma derivação em A tal que $d(F)=0$, então d é uma derivação interna em A ".

Seria natural nos perguntarmos se, nas hipóteses

dos teoremas 3.1 e 3.2, quando concluímos que R é uma ordem numa álgebra simples de dimensão no máximo 4 sobre seu centro, teríamos que d é uma derivação interna?

Lembramos que, no caso em que R é um domínio e $Z(R)$ é não enumerável (no teorema 3.1) ou se R é um domínio e n é fixo, demonstramos que $d(Z(R))=0$ (lema 3.11).

Logo, a extensão $\Delta: R_Z \rightarrow R_Z$ dada por

$$\Delta(rz^{-1})=d(r)z^{-1}$$

para todo $rz^{-1} \in R_Z$ é uma derivação em R_Z e $\Delta(Z(R_Z))=0$. Portanto, o teorema de Skolem-Nöether implica que Δ é uma derivação interna em R_Z , isto é, existe $aw^{-1} \in R_Z$ tal que

$$\Delta(rz^{-1})=aw^{-1}rz^{-1}-rz^{-1}aw^{-1}=(ar-ra)z^{-1}w^{-1}$$

para todo elemento $rz^{-1} \in R_Z$.

Evidentemente concluímos que

$$d(r)=(ar-ra)w^{-1} \quad \forall r \in R.$$

Ainda, como existe um natural $n(r)>0$ tal que $d(r)^{n(r)} \in Z(R)$, é claro que $(ar-ra)^{n(r)} \in Z(R)$.

Portanto, nas condições do teorema 3.1, item (iii) ou nas condições do teorema 3.2 no caso em que R é um domínio, demonstramos que d é forma

$$d(r)=(ar-ra)w^{-1} \quad \forall r \in R,$$

onde $a \in R$ e $w \in Z(R)$.

No caso em que R é um domínio e $\text{car} R = p > 0$, pela demonstração do item (iv) do teorema 3.1, sabemos que $\dim_{\mathbb{Z}} RG_{\mathbb{Z}} \leq 4$ e, como RG é um domínio de centro não enumerável, temos que a derivação Δ em RG é tal que $\Delta(Z(RG)) = 0$. Mas Δ estende d e portanto $d(Z(R)) = 0$. Novamente, as mesmas considerações nos permitem concluir que existem $a \in R$ e $w \in Z(R)$ tais que

$$d(r) = (ar - ra)w^{-1} \quad \forall r \in R.$$

CAPÍTULO IV

Neste capítulo estudaremos basicamente derivações cujos valores são de alguma forma especiais. Serão analisados anéis com derivações cujos valores são de um dos tipos abaixo:

- 1 - nilpotentes ou inversíveis
- 2 - nilpotentes ou regulares
- 3 - nulos ou regulares
- 4 - nulos ou inversíveis

Iniciaremos o capítulo retomando dois resultados que foram utilizados no capítulo 3, mas que têm interesse independente.

O primeiro deles é uma pequena generalização de um resultado de Bergen, que aparece em [B.1]. A generalização só tem interesse no contexto do capítulo 3: é o resultado original de Bergen que nos interessará aqui. Neste trabalho é estudado um anel em uma derivação cujos valores são nilpotentes ou inversíveis. No capítulo 2 já expusemos condições sob as quais uma derivação não é nil; neste trabalho Bergen também trabalha sob estas condições, concluindo que:

- 1 - um anel sem ideais laterais nil não nulos com uma derivação cujos valores são nilpotentes ou inversíveis é D ou $M_2(D)$, onde D é um anel com divisão.

2 - um anel semiprimo com uma derivação cujos valores são nilpotentes de índice limitado ou inversíveis é D ou $M_2(D)$, onde D é um anel com divisão.

Mostraremos aqui estes dois resultados, fazendo uma pequena generalização: as condições sobre d se restringindo à um ideal não nulo de R . Também mostraremos que, no caso em que o anel é $M_2(D)$, e $\text{car} D \neq 2$, então a derivação é interna.

Outro resultado que já utilizamos, parcialmente, no capítulo anterior e que aparecerá aqui é o seguinte:

3 - se um anel tem uma derivação que não é nil em nenhum ideal não nulo e cujos valores sobre um certo ideal são nilpotentes ou regulares, então o anel é primo sem ideais nil não nulos.

Este resultado serviu para mostrar que a hipótese do anel ser primo nos resultados de Lanski, em [L.1], era supérflua, nos permitindo demonstrar o teorema 3.1. Também foi utilizado para generalizar o resultado de Herstein, substituindo a hipótese R primo por R semiprimo (teorema 3.2).

Seguindo o mesmo raciocínio que utilizamos na demonstração do resultado acima também provaremos que:

4 - um anel com uma derivação cujos valores num ideal não nulo são regulares ou nulos é um anel primo sem ideais nil não nulos.

Finalizando o capítulo, demonstraremos um resultado de Bergen, Herstein e Lanski que aparece em [B.4] onde é estudado um anel com uma derivação cujos valores são nulos ou inversíveis. Apesar da hipótese bastante especial, este

resultado tem a vantagem de dar uma resposta precisa e definitiva não só no que se refere ao anel mas também no que se refere à derivação. Conclui-se que, sob tais condições, uma das três situações seguintes ocorre:

- a) trata-se de um anel com divisão
- b) trata-se de um anel de matrizes 2×2 sobre um anel com divisão D .
- c) trata-se de um anel da forma $D[X]/(X^2)$ onde D é um anel com divisão. Além disto, neste caso, d não é uma derivação interna, $d(X)$ é da forma $d(X)=1+zX$ para algun $z \in Z(D)$, $d(D)=0$ e $\text{car} D=2$.

Conclui-se também que se $R=M_2(D)$ e $\text{car} R \neq 2$ então d é uma derivação interna e, se $\text{car} R \neq 2$ então $R=M_2(D)$ pode ocorrer se e somente se D não contém todas as extensões quadráticas de $Z(D)$.

Iniciaremos então, relembando o teorema 3.6 que já foi demonstrado no capítulo 3.

4.1 - TEOREMA. Seja R um anel primo tal que $R_Z, 0$ localizado de R em $Z(R)^*$, é um anel primitivo. Sejam ainda $d \neq 0$ uma derivação em R e $I \neq 0$ ideal de R tais que para todo $x \in I$ ou $d(x)$ é nilpotente ou $d(x)$ é inversível de R_Z . Então $R_Z=D$ ou $R_Z=M_2(D)$, onde D é um anel com divisão.

Já mencionamos que este resultado é uma generalização de um resultado de Bergen de [B.1]. Provaremos um corolário deste resultado que, com os dois lemas que se guem, implicam os resultados de Bergen (generalizados para ideais).

4.2 - COROLÁRIO. Sejam R um anel simples com unidade e $d \neq 0$ uma derivação em R . Suponhamos que para todo $x \in R$, $d(x)$ ou é inversível ou é nilpotente. Então $R = D$ ou $R = M_2(D)$, onde D é um anel com divisão.

DEMONSTRAÇÃO. Primeiramente observamos que se R é um anel simples, com unidade, então $Z(R)$ é um corpo. De fato, se $x \in Z(R)^*$ então Rx é um ideal (bilateral) não nulo de R o que implica $Rx = xR = R$. Neste caso, existe $x^{-1} \in R$ tal que $x^{-1}x = xx^{-1} = 1$ e portanto $Z(R)$ é corpo.

Ora, mas se $Z(R)$ é um corpo, todo elemento não nulo de $Z(R)$ é inversível e portanto $R_Z = R$. Logo, $R_Z = R$ é um anel primitivo e estamos nas condições do teorema 4.1. Concluimos, então que $R = R_Z = D$ ou $R = R_Z = M_2(D)$ para algum D anel com divisão.

//

4.3 - LEMA. Sejam R um anel com unidade, sem ideais laterais nil não nulos, $I \neq 0$ um ideal de R e d uma derivação em R tal que $d(I) \neq 0$ e $d(x)$ é nilpotente ou $d(x)$ é inversível para todo $x \in I$. Então R é um anel simples e consequentemente $I = R$.

DEMONSTRAÇÃO. Primeiramente vamos provar que $d(I^2) \neq 0$. De fato, como R não tem ideais laterais nil não nulos e $d(I) \neq 0$, o teorema 2.8 implica que d não é nil em I . Portanto existe $a \in I$ tal que $d(a)$ é inversível. Neste caso, se $d(I^2) = 0$ então:

$$0 = d(aI^2) = d(a)I^2,$$

o que implica, $I^2 = 0$ que é absurdo. Portanto $d(I^2) \neq 0$.

Ora, se $d(I^2) \neq 0$, novamente pelo teorema 2.8 temos que d não é nil em I^2 . Portanto existe $b \in I^2$ tal que $d(b)$ é inversível. Logo, $d(b) \in d(I^2) \subset I$ implica $I = R$.

Seja agora $J \neq 0$ um ideal de R . Vamos mostrar que $J = R$. De fato, tomando $a \in R$ tal que $d(a)$ é inversível e usando o mesmo raciocínio acima provamos que $d(J^2) = 0$ implica $0 = d(aJ^2) = d(a)J^2$, o que acarreta $J^2 = 0$, que é um absurdo. Portanto $d(J^2) \neq 0$ e, novamente pelo teorema 2.8, temos que d não é nil em J^2 . Logo, como $I = R$, existe $c \in J^2$ tal que $d(c)$ é inversível. Mas $d(c) \in d(J^2) \subset J$ o que implica $J = R$.

Provamos então que R é simples o que finaliza a demonstração.

//

4.4 - LEMA. Sejam R um anel semiprimo, $I \neq 0$ um ideal de R e $d \neq 0$ uma derivação em R tal que $d(I) \neq 0$ e para todo $x \in I$, ou $d(x)$ é inversível ou $d(x)^n = 0$ onde $n \geq 1$ é um inteiro fixado. Então R é um anel simples e consequentemente $I = R$.

DEMONSTRAÇÃO. A demonstração é a mesma do teorema anterior. O corolário 2.26 implica que d não é nil em I e o fato de R ser semiprimo implica $I^2 \neq 0$. Logo, da mesma forma que na demonstração acima provamos que $I = R$.

Dado $J \neq 0$ ideal de R , novamente o fato de R ser semiprimo implica $J^2 \neq 0$ e pelo mesmo raciocínio usado na demonstração do lema anterior, obtemos:

$$d(J^2) \neq 0.$$

Agora, o corolário 2.26 implica que d não é nil em J^2 e, usando que $I=R$, obtemos um elemento $c \in J^2$ tal que $d(c)$ é inversível. Mas $d(c) \in d(J^2) \subset J$ o que implica $J=R$.

Portanto R é simples e a demonstração está concluída.

//

Tanto nas hipóteses do lema 4.4 quanto naquelas do lema 4.3, o corolário 4.2 implica imediatamente que $R=D$ ou $R=M_2(D)$ onde D é um anel com divisão.

É claro que qualquer derivação em um anel com divisão D só toma valores inversíveis ou nulos. Vamos mostrar, através do seguinte exemplo, que em $M_2(D)$ temos, de fato, derivações cujos valores são nilpotentes ou inversíveis.

4.5 - EXEMPLO. Seja D um anel com divisão e consideremos, em $M_2(D)$, a derivação interna dada por

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = e_{12}.$$

Então, dado

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_2(D) \text{ temos:}$$

$$d \left(\begin{bmatrix} x & y \\ z & w \end{bmatrix} \right) = e_{12} \begin{bmatrix} x & y \\ z & w \end{bmatrix} - \begin{bmatrix} x & y \\ z & w \end{bmatrix} e_{12} =$$

$$= \begin{bmatrix} z & w-x \\ 0 & -z \end{bmatrix}.$$

É claro que se $z=0$ então

$$d \left(\begin{bmatrix} x & y \\ z & w \end{bmatrix} \right)^2 = 0$$

e, se $z \neq 0$

$$d \left(\begin{bmatrix} x & y \\ z & w \end{bmatrix} \right) \text{ é inversível.}$$

Vamos agora analisar o caso em que d é uma deri
vação em $M_2(D)$, $\text{car} D \neq 2$ e $d(A)$ é nilpotente ou $d(A)$ é inver
sível para toda matriz $A \in M_2(D)$.

A seguinte proposição mostra que a derivação é
interna no caso em que o anel é $M_2(D)$ e $\text{car} D \neq 2$.

4.6 - PROPOSIÇÃO. Sejam D um anel com divisão com $\text{card } D \neq 2$ e $d \neq 0$ uma derivação em $M_2(D)$ tal que para todo $A \in M_2(D)$ $d(A)$ é nilpotente ou $d(A)$ é inversível. Então d é uma derivação interna de $M_2(D)$.

DEMONSTRAÇÃO. Pelo lema 0.20, sabemos que existem $a, b, c \in D$ e f , uma derivação em D tais que:

$$d(e_{11}) = \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix}, \quad d(e_{12}) = \begin{bmatrix} -b & c \\ 0 & b \end{bmatrix},$$

$$d(e_{21}) = \begin{bmatrix} -a & 0 \\ -c & a \end{bmatrix} \quad \text{e} \quad d(e_{22}) = \begin{bmatrix} 0 & -a \\ -b & 0 \end{bmatrix};$$

e, para qualquer $x \in D$ temos:

$$d\left(\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} f(x) & xa \\ bx & 0 \end{bmatrix} \quad \text{e}$$

$$d\left(\begin{bmatrix} 0 & 0 \\ 0 & x \end{bmatrix}\right) = \begin{bmatrix} 0 & -ax \\ -xb & f(x)+xc-cx \end{bmatrix}.$$

Ainda, a demonstração do corolário 0.21 implica que d é uma derivação interna se e somente se f é uma derivação interna. Basta, portanto, provarmos que f é uma deri

vação interna.

Suponhamos, em primeiro lugar, que $a \neq 0$. Então, da do $x \in D$ temos,

$$\begin{aligned}
 d \left(\begin{bmatrix} x & 0 \\ a^{-1}f(x) & a^{-1}xa \end{bmatrix} \right) &= d \left(\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \right) + \\
 + d \left(\begin{bmatrix} 0 & 0 \\ 0 & a^{-1}f(x) \end{bmatrix} \right) \left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \right) + d \left(\begin{bmatrix} 0 & 0 \\ 0 & a^{-1}xa \end{bmatrix} \right) &= \\
 = \begin{bmatrix} f(x) & xa \\ bx & 0 \end{bmatrix} + \begin{bmatrix} -f(x) & 0 \\ -f(a^{-1}f(x)) - ca^{-1}f(x) & a^{-1}f(x)a \end{bmatrix} + \\
 + \begin{bmatrix} 0 & -xa \\ a^{-1}xab & f(a^{-1}xa) + a^{-1}xac - ca^{-1}xa \end{bmatrix} &= \\
 = \begin{bmatrix} 0 & 0 \\ u & v \end{bmatrix}, &
 \end{aligned}$$

onde

$$v = a^{-1}f(x)a + f(a^{-1}xa) + a^{-1}xac - ca^{-1}xa.$$

Como

$$\begin{bmatrix} 0 & 0 \\ u & v \end{bmatrix}$$

é nilpotente ou inversível, concluímos que $v=0$. Ainda, como f é uma derivação em D , temos que

$$0=f(1)=f(aa^{-1})=f(a)a^{-1}+af(a^{-1}),$$

isto é,

$$f(a^{-1})=-a^{-1}f(a)a^{-1}.$$

Logo,

$$\begin{aligned} 0=v=a^{-1}f(x)a-a^{-1}f(a)a^{-1}xa+a^{-1}f(x)a+a^{-1}xf(a)+ \\ +a^{-1}xac-ca^{-1}xa; \end{aligned}$$

portanto,

$$0=ava^{-1}=2f(x)-f(a)a^{-1}x+xf(a)a^{-1}+xaca^{-1}-aca^{-1}x.$$

Mas, $\text{car} D \neq 2$ implica que

$$f(x)=\frac{1}{2}[(f(a)a^{-1}+aca^{-1})x-x(f(a)a^{-1}+aca^{-1})],$$

e portanto f é uma derivação interna em D .

Por outro lado, se $a=0$, dado $x \in D$ qualquer, temos:

$$d \left(\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \right) = \begin{bmatrix} f(x) & 0 \\ bx & 0 \end{bmatrix},$$

que não é inversível. Logo,

$$\begin{bmatrix} f(x) & 0 \\ bx & 0 \end{bmatrix}$$

é nilpotente e temos que $f(x)=0$. Concluimos, portanto, que f é a derivação nula em D e, naturalmente, f é uma derivação interna em D .

Logo, d é uma derivação interna em $M_2(D)$.

//

Os lemas 4.3 e 4.4, o corolário 4.2 e a proposição 4.6 implicam imediatamente os seguintes teoremas:

4.7 - TEOREMA. Sejam R um anel sem ideais laterais nil não nulos, $I \neq 0$ um ideal de R e d uma derivação em R tal que $d(I) \neq 0$ e, para todo $x \in I$, $d(x)$ é nilpotente ou $d(x)$ é inversível. Então $R=D$ ou $R=M_2(D)$ para algum anel com divisão D . Ainda, se $R=M_2(D)$ e $\text{card } D \neq 2$ então d é uma derivação interna.

4.8 - TEOREMA. Sejam R um anel semiprimo, $I \neq 0$ um ideal de R e d uma derivação em R tal que $d(I) \neq 0$ e, para todo $x \in I$, $d(x)$ é inversível ou $d(x)^n = 0$, onde $n \geq 1$ é um inteiro fixado.

Então $R=D$ ou $R=M_2(D)$ onde D é um anel com divisão. Ainda, se $R=M_2(D)$ e $\text{car} D \neq 2$, então d é uma derivação interna.

Vamos agora estudar o caso em que os valores da derivação são nilpotentes ou regulares. Iniciaremos provando alguns lemas.

4.9 - LEMA. Sejam R um anel e d uma derivação em R tal que existe $a \in R$ com $d(a)$ regular. Então $d(L) \neq 0$ para todo L ideal lateral não nulo de R .

DEMONSTRAÇÃO. Seja L um ideal à esquerda de R . Vamos mostrar que $d(L)=0$ implica $L=0$. De fato, $d(L)=0$ implica

$$0 = d(aL) = d(a)L$$

e, como $d(a)$ é regular, temos $L=0$.

A demonstração para L , ideal à direita é análoga.

//

4.10 - LEMA. Sejam R um anel e d uma derivação em R . Seja ainda $J \neq 0$ um ideal de R tal que existe $a \in J$ com $d(a)$ regular. Então $J^2=0$ implica que R tem característica 2.

DEMONSTRAÇÃO. Se $J^2=0$ então $a^2=0$ e temos:

$$0 = d^2(a^2) = d^2(a)a + 2d(a)^2 + ad^2(a),$$

o que implica $2d(a)^2 \in J$. Consequentemente, temos:

$$0 = 2d(a)^2 J = d(a)^2 (2J);$$

como $d(a)^2$ é regular, concluímos que $2J = 0$.

Provaremos agora que $2J = 0$ implica $2R = 0$, o que finaliza a demonstração. De fato, dados $r \in R$ e $a \in J$ com $d(a)$ regular, temos que $ra \in J$ e, pelo parágrafo anterior, sabemos que $2ra = 0$. Ora, mas neste caso, temos:

$$0 = 2d(ra) = 2d(r)a + 2rd(a).$$

Ainda, $2d(r)a \in 2J = 0$ e portanto concluímos que $2rd(a) = 0$ e, consequentemente, que $2r = 0$. Como $r \in R$ é qualquer, temos $2R = 0$ o que finaliza a demonstração.

//

4.11 - LEMA. Sejam R um anel com $\text{car} R \neq 2$ e d uma derivação em R . Seja ainda $I \neq 0$ um ideal de R tal que para todo J ideal de R , $0 \neq J \subset I$, existe um elemento $a \in J$ com $d(a)$ regular. Então todo ideal não nulo de R contém um elemento regular.

DEMONSTRAÇÃO. Primeiramente vamos mostrar que I contém um elemento regular. De fato, pelo lema anterior, sabemos que $I^2 \neq 0$ e, como $I^2 \subset I$, existe $a \in I^2$ tal que $d(a)$ é regular. Mas,

$$d(a) \in d(I^2) \subset d(I)I + Id(I) \subset I$$

e portanto I contém um elemento regular.

Seja agora $K \neq 0$ um ideal de R . Como I contém um elemento regular, o ideal $IK \subset I$ é não nulo. Portanto, pelo lema anterior, temos $(IK)^2 \neq 0$ e consequentemente, existe $b \in (IK)^2$ tal que $d(b)$ é regular. Mas, $d(b) \in IK \subset K$, e concluimos que K contém um elemento regular, finalizando a demonstração do lema.

//

Estamos agora em condições de demonstrar as seguintes proposições:

4.12 - PROPOSIÇÃO. Sejam R um anel com $\text{car} R \neq 2$ e d uma derivação em R que não é nil em nenhum ideal não nulo de R . Seja ainda I um ideal não nulo de R tal que para todo $x \in I$, $d(x)$ é regular ou $d(x)$ é nilpotente. Então R é um anel primo sem ideais nil não nulos.

DEMONSTRAÇÃO. Vamos provar que R está nas condições do lema anterior. De fato, se $0 \neq J \subset I$ é um ideal de R , como d não é nil em J , então existe $a \in J \subset I$ tal que $d(a)$ não é nilpotente. Logo, $d(a)$ é regular.

Estamos então nas condições do lema 4.11 e concluimos que todo ideal não nulo de R tem um elemento regular. Segue então trivialmente que R é primo e $N(R) = 0$.

//

4.13 - PROPOSIÇÃO. Sejam R um anel com $\text{car} R \neq 2$ e d uma derivação em R . Seja ainda I , um ideal não nulo de R tal que $d(I) \neq 0$ e, para todo $x \in I$, $d(x)$ é regular ou $d(x) = 0$. Então R é um anel primo sem ideais nil não nulos.

DEMONSTRAÇÃO. Vamos mostrar que R , I e d estão nas condições do lema 4.11. De fato, se $0 \neq J \subset I$ é um ideal de R e $d(J) = 0$ então

$$0 = d(IJ) = d(I)J.$$

Mas, como $d(I) \neq 0$, existe $a \in I$ com $d(a)$ regular. Logo, da igualdade acima, obtemos $0 = d(a)J$ o que implica $J = 0$, que é uma contradição. Consequentemente, $d(J) \neq 0$. Ainda, $J \subset I$, portanto $d(J) \neq 0$ implica que existe $b \in J \subset I$ tal que $d(b)$ é regular.

Concluimos então que R, d e I satisfazem as hipóteses do lema 4.11 e, portanto, todo ideal não nulo de R tem um elemento regular. Segue trivialmente que R é primo e $N(R) = 0$.

//

É claro que, se R é um domínio, toda derivação em R só toma valores nilpotentes ou regulares. Vejamos um outro exemplo de um anel com uma derivação que só toma valores nilpotentes ou regulares.

4.14 - EXEMPLO. Seja R um domínio comunidade e d a derivação interna dada por

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

em $M_2(R)$. Dado

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_2(R)$$

temos:

$$d \left(\begin{bmatrix} x & y \\ z & w \end{bmatrix} \right) = e_{12} \begin{bmatrix} x & y \\ z & w \end{bmatrix} - \begin{bmatrix} x & y \\ z & w \end{bmatrix} e_{12} = \begin{bmatrix} z & w-x \\ 0 & -z \end{bmatrix}.$$

É claro que se $z=0$ então

$$d \left(\begin{bmatrix} x & y \\ z & w \end{bmatrix} \right)^2 = 0$$

e, se $z \neq 0$ então

$$d \left(\begin{bmatrix} x & y \\ z & w \end{bmatrix} \right)$$

é regular em $M_2(D)$.

Finalmente, estudaremos agora o caso em que os valores da derivação são inversíveis ou nulos. Mostraremos os

resultados de Bergen, Herstein e Lanski que aparecem em [B.4] . Primeiramente provamos alguns lemas.

Nos lemas que seguem R é um anel com unidade, d é uma derivação em R , e L é um ideal à esquerda de R tal que $d(L) \neq 0$ e $d(x)=0$ ou $d(x)$ é inversível para todo $x \in L$.

4.15 - LEMA. Se $0 \neq r \in R$ e $d(r)=0$ então r é inversível.

DEMONSTRAÇÃO. Seja $x \in L$ tal que $d(x)$ é inversível. Então $rx \in L$ e $d(rx)=rd(x)$. Como $r \neq 0$ e $d(x)$ é inversível, então $rd(x)=0$. Logo, $d(rx)=rd(x)$ é inversível e portanto r é inversível.

//

4.16 - LEMA. Se W é um ideal (à esquerda, à direita ou bilateral) de R e $d(W)=0$ então $W=0$.

DEMONSTRAÇÃO. Pelo lema anterior, se $d(W)=0$ então $W=0$ ou W contém um elemento inversível. Logo, $W=0$ ou $W=R$. Mas $d \neq 0$ e $d(W)=0$ implicam $W \neq R$ e portanto $W=0$.

//

4.17 - LEMA. Se $L \neq R$ então $L+d(L)=R$ e $L \cap d(L)=0$.

DEMONSTRAÇÃO. Primeiro observamos que $L+d(L)$ é um ideal à esquerda de R . De fato, se $a+d(b) \in L+d(L)$ com $a, b \in L$ então dado $r \in R$, $ra+rd(b)=ra+d(rb)-d(r)b \in L+d(L)$.

Como $d(L) \neq 0$, existe $a \in L$ com $d(a)$ inversível. Neste caso, $L+d(L)$ contém um elemento inversível e portanto $L+d(L)=R$.

Ainda, o lema 4.15 implica que se $0 \neq x \in L$ então $d(x) \neq 0$, isto é, $d(x)$ é inversível. Logo, $L \cap d(L)=0$.

//

4.18 - LEMA. Se $L \neq R$ então L é ideal à esquerda minimal e maximal.

DEMONSTRAÇÃO. Seja $W \neq R$ ideal à esquerda de R tal que $L \subset W$. Como $W \subset R=L+d(L)$, todo elemento $w \in W$ é da forma.

$$w=a+d(b) \quad \text{com } a, b \in L.$$

Portanto, $w-a=d(b) \in W \cap d(L)$. Mas os elementos não nulos de $d(L)$ são inversíveis, e $W \neq R$. Logo, $W \cap d(L)=0$ e concluímos que $w=a \in L$. Então $W=L$ e provamos que L é maximal.

Seja agora $K \neq 0$ ideal à esquerda de R tal que $K \subset L$. Como $K \neq 0$, o lema 4.16 implica $d(K) \neq 0$ e concluímos que K satisfaz as mesmas condições que L . Logo, $K+d(K)=R$ e, da mesma forma que no parágrafo anterior, concluímos que K é maximal. Portanto $L=K$ e provamos que L é minimal.

//

4.19 - LEMA Se $L \neq R$ e R não é simples então $\text{car} R = 2$, $L^2 = 0$ e L é o único ideal (bilateral) de R .

DEMONSTRAÇÃO. Consideremos $\text{Anl}(L) = \{x \in R / xL = 0\}$. É claro que $\text{Anl}(L)$ é um ideal à esquerda de R . Ainda, como $L + d(L) = R$, $1 \in R$ é da forma:

$$1 = a + d(b) \quad \text{com } a \text{ e } b \in L.$$

Logo, se $x \in \text{Anl}(L)$, então $xa = xb = 0$ e temos:

$$x = x(a + d(b)) = xd(b) = d(xb) - d(x)b = -d(x)b \in L.$$

Portanto, $\text{Anl}(L) \subset L$ e, pelo lema anterior, temos que

$$\text{Anl}(L) = 0 \quad \text{ou} \quad \text{Anl}(L) = L.$$

Suponhamos, primeiramente, que $\text{Anl}(L) = 0$. Vamos mostrar que neste caso, chegaremos ao absurdo: R é simples. Seja $I \neq 0$ um ideal de R . Como $\text{Anl}(L) = 0$, temos que $0 \neq IL \subset L$ e portanto, $IL = L$. Neste caso, se $I^2 L = 0$, então:

$$0 = I^2 L = I(IL) = IL$$

o que é absurdo. Concluimos, portanto, que $I^2 L \neq 0$.

Temos, então, um ideal à esquerda de R , $I^2 L$, tal que $0 \neq I^2 L \subset L$. Novamente, pelo lema anterior, concluímos que $I^2 L = L$. Portanto, temos que:

$$0 \neq d(L) = d(I^2 L) \subset d(I^2) \cap d(L) \subset I \cap d(L).$$

Ora, mas $d(L)$ só contém elementos inversíveis ou nulos; então, do que foi feito acima, concluímos que I contém um elemento inversível, isto é, $I=R$. Logo, R é simples, o que é absurdo.

Concluímos, então que $\text{Anl}(L)=L$. Vamos agora provar que L é o único ideal (bilateral) próprio de R . Seja, então I um ideal (bilateral) de R . Consideremos o ideal à esquerda IL . É claro que $IL \subset L$. Pelo lema anterior, temos que $IL=L$ ou $IL=0$. Mas se $IL=L$, então $L=IL \subset I \cap L$, o que implica $L \subset I$; por outro lado, se $IL=0$, então $I \subset \text{Anl}(L)=L$. Logo, usando novamente o lema anterior, temos:

$$L=I \quad \text{ou} \quad I=R \quad \text{ou} \quad I=0,$$

e portanto L é o único ideal (bilateral) próprio de R .

Vamos agora mostrar que, se $\text{Anl}(L)=L$ então $\text{car} R=2$. Seja $a \in L$ tal que $d(a)$ é inversível. Como $\text{Anl}(L)=L$, então $a^2 \in L^2=0$ e consequentemente:

$$0=d(a^2)=d^2(a)a+2d(a)d(a)+ad^2(a).$$

Já vimos que L é um ideal (bilateral) de R , portanto, $d^2(a)a+ad^2(a) \in L$ e, da igualdade acima, concluímos que $2d(a)^2 \in L$. Consequentemente, $4d(a)^4 \in L^2=0$. Em suma, concluímos que existe $x=d(a)^4$ um elemento inversível tal que $2x \in L$ e $4x=0$.

Vamos analisar várias possibilidades: se $2x=0$ então $2R=2xx^{-1}R=0$ e provamos o que queríamos; se $2x \neq 0$ e $d(2x)=0$ então, pelo lema 4.15, $2x$ é inversível, mas $2x \in L$ e $L \neq R$ o que nos leva a um absurdo; finalmente, se $2x \neq 0$ e

$d(2x)$ é inversível, então $4x=0$ implica $2d(2x)=0$ e temos:

$$2R=2d(2x)d(2x)^{-1}R=0$$

e provamos o que queríamos.

//

O próximo lema nos dará toda a informação que necessitamos para analisar o caso em que R não é simples.

4.20 - LEMA. Se R não é simples e $L \neq R$, então $\text{car} R = 2$ e $R = D[X]/(X^2)$ onde D é um anel com divisão. Além disso, d não é uma derivação interna e $d(X) = 1 + zX$ para algum $z \in Z(D)$.

DEMONSTRAÇÃO. Em primeiro lugar, relembramos que, pelos lemas que acabamos de provar, já sabemos que: $L^2 = 0$, $L + d(L) = R$, $L \cap d(L) = 0$, L é o único ideal (bilateral) próprio de R e $\text{car} R = 2$.

Consideremos agora $D = \{u \in R / d(u) \in L\}$. Vamos provar as seguintes afirmações sobre D :

Afirmção 1. D é um subanel de R que é um anel com divisão.

De fato, como L é um ideal (bilateral) de R , da dos u e $v \in D$ temos:

$$d(u+v) = d(u) + d(v) \in L$$

e,

$$d(uv) = d(u)v + ud(v) \in Lv + uL \subset L.$$

É óbvio, portanto, que D é um subanel de R .

Ainda, dados $u \in D$ e $a \in L$ tal que $d(a)$ é inversível, então $d(u)a \in L^2 = 0$ e $ua \in L$. Logo, $d(ua) = ud(a)$ é inversível ou zero. Se $ud(a)$ é inversível, como $d(a)$ é inversível, temos que u é inversível. Por outro lado, se $ud(a) = 0$ então $u = ud(a)d(a)^{-1} = 0$. Portanto, concluímos que dado $u \in D$, ou $u = 0$ ou u é inversível em R . Mas $d(u^{-1}) = u^{-1}d(u)u^{-1}$. Portanto, $d(u^{-1}) \in L$ e concluímos que D é um anel com divisão.

Afirmção 2. Se $a \in L$ e $a \neq 0$ então $R = D + Da$.

Ora, sabemos que $R = L + d(L)$. Portanto, dado $r \in R$, existem b e c elementos de L tais que

$$d(r) = b + d(c).$$

Logo, $d(r - c) = b \in L$ e $r = (r - c) + c \in D + L$. Concluímos, então, que

$$R = D + L.$$

Seja agora $0 \neq a \in L$. Como $a \in L$ então $La \subset L^2 = 0$; como R tem unidade e L é um ideal à esquerda minimal, então $0 \neq Ra = L$. Logo,

$$L=Ra=(D+L)a=Da$$

e, do parágrafo anterior, concluímos que $R=D+Da$, o que demonstra a afirmação 2.

Vamos agora mostrar que existe $b \in L$ tal que $d(b)=1+zb$ para algum $z \in D$. Seja $0 \neq a \in L$ qualquer. Então, pela afirmação 2, sabemos que $d(a)$ é da forma:

$$d(a)=u+va, \quad \text{com } u, v \in D.$$

Se $u=0$, então $d(a)=va \in L \cap d(L)=0$ e, o lema 4.15 implica que a é inversível, o que é absurdo, pois $a \in L \setminus R$. Logo, temos que $u \neq 0$ e portanto, como $u \in D$, u é inversível em D . Neste caso, $d(u^{-1})a \in L^2=0$ e $u^{-1}a \in L$. Consequentemente,

$$d(u^{-1}a)=u^{-1}d(a)=u^{-1}(u+va)=1+(u^{-1}v)u^{-1}a$$

e, tomando $b=u^{-1}a$, temos que $d(b)=1+zb$ para algum $z \in D$.

Nosso objetivo agora é mostrar que, se $b \in L$ é tal que $d(b)=1+zb$ para algum $z \in D$, então $b \in Z(R)$. De fato, seja $r \in R$ qualquer. Então $brb=bd(r)b \in L^2=0$ e portanto,

$$0=d(brb)=d(b)rb+brd(b)=(1+zb)rb+br(1+zb)=rb+br.$$

Como $\text{car} R=2$, da igualdade acima, concluímos que $b \in Z(R)$.

É óbvio então que d não é uma derivação interna, pois se assim fosse, teríamos $0=d(b)=1+zb$ o que implica

que $1=zb \in L$, que é um absurdo.

O fato de que $R \cong D[X]/(X^2)$ também decorre imediatamente de $b \in Z(R)$. Basta tomarmos o homeomorfismo $\psi : D[X] \rightarrow R$ dado por: $\psi(p(X)) = p(b) \quad \forall p(X) \in D[X]$. Do fato de que $R = D + Db$ temos que ψ é um epimorfismo; observando que $\text{Anl}(L) = L$ e $D \cap Db = D \cap L = 0$ é fácil ver que $\text{Ker}(\psi) = (X^2)$. Logo, $R \cong D[X]/(X^2)$.

Resta-nos demonstrar que se $d(b) = 1 + zb$ com $b \in L$ e $z \in D$, então $z \in Z(D)$. De fato, se $v \in D$, como $b \in Z(R)$, temos que $d(v)b = bd(v) \in L^2 = 0$. Logo,

$$0 = bv + vb = d(bv + vb) = d(b)v + vd(b) = (1 + zb)v +$$

$$+v(1 + zb) = zbv + vzb = (zv + vz)b.$$

Ora, mas $zv + vz \in D$ e portanto $zv + vz = 0$ ou $zv + vz$ é inversível. Se $zv + vz$ é inversível, então, da igualdade acima, temos que $b = 0$ o que contradiz $d(b) = 1 + zb$. Logo $zv + vz = 0$ e portanto $z \in Z(D)$.

//

Estamos agora, condições de provar um dos resultados de Bergen, Herstein e Lanski que aparece em [B.4].

4.21 - TEOREMA. Sejam R um anel com unidade e L um ideal à esquerda próprio de R . Seja ainda uma derivação d em R tal que $d(L) \neq 0$ e, para todo $a \in L$, ou $d(a) = 0$ ou $d(a)$ é inversível. Então ou $R = M_2(D)$ ou $R = D[X]/(X^2)$ e $\text{car} R = 2$, para algum D , anel com divisão. Além disto, se $R = D[X]/(X^2)$ e $\text{car} R = 2$ então

$d(X)=1+zX$ para algum $z \in Z(D)$.

DEMONSTRAÇÃO. Se R não é simples, o lema 4.20 implica que $\text{car} R=2$, $R=D[X]/(X^2)$, $d(X)=1+zX$ para algum $z \in Z(D)$ e d não é uma derivação interna.

Resta-nos demonstrar que, se R é simples então $R=M_2(D)$, para algum anel com divisão D . De fato, pelo lema 4.18, sabemos que L é um ideal à esquerda minimal e maximal. Em [H.8] está demonstrado que um anel simples com unidade que tem um ideal à esquerda minimal é artiniano. Logo, R é simples e artiniano e o teorema de Artin-Wedderburn implica que $R \cong M_n(D)$ para algum anel com divisão D .

Mas se $n \geq 3$ então $M_n(D)$ não tem ideal lateral que seja minimal e maximal. Logo, $n \leq 2$. Ainda, como L é um ideal à esquerda próprio, temos que $n \neq 1$ e concluímos que $R \cong M_2(D)$.

//

Se no teorema anterior, tem-se que $L=R$, então Bergen, Herstein e Lanski demonstram que obtemos mais informações sobre a derivação e sobre o anel, no caso em que $R=M_2(D)$ e $\text{car} R \neq 2$. O lema que segue estuda este caso específico.

4.22 - LEMA. Sejam D um anel com divisão tal que $\text{car} D \neq 2$. Uma condição necessária e suficiente para que exista $d \neq 0$, uma derivação em $M_2(D)$, tal que para todo $A \in M_2(D)$, $d(A)=0$ ou $d(A)$ é inversível é que D não contenha todas as exten -

sões quadráticas de $Z(D)$. Ainda, se existe $d \neq 0$, uma derivação em $M_2(D)$ satisfazendo as condições acima, então d é uma derivação interna.

DEMONSTRAÇÃO. Suponhamos que exista d , uma derivação em $M_2(D)$ satisfazendo as condições acima. Então, pela proposição 4.6 sabemos que d é uma derivação interna. Vamos provar que podemos supor que d é uma derivação interna dada por uma matriz da forma

$$\begin{bmatrix} 0 & \alpha \\ 1 & \beta \end{bmatrix} \in M_2(D).$$

Seja

$$B = \begin{bmatrix} a & b \\ c & e \end{bmatrix} \in M_2(D)$$

tal que $d(A) = BA - AB$ para todo $A \in M_2(D)$. Vamos provar que $c \neq 0$. Ora, se $c = 0$ então para qualquer $x \in D$, temos:

$$\begin{aligned} d \left(\begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} \right) &= \begin{bmatrix} a & b \\ 0 & e \end{bmatrix} \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & e \end{bmatrix} = \\ &= \begin{bmatrix} 0 & ax - xe \\ 0 & 0 \end{bmatrix}. \end{aligned}$$

Mas

$$d\left(\begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}\right)$$

é inversível ou zero; portanto, concluímos que $ax - xe = 0$
 $\forall x \in D$. Logo, $a = e \in Z(D)$. Ainda, se $c = 0$, então

$$d(e_{22}) = \begin{bmatrix} a & b \\ 0 & e \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & e \end{bmatrix} = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$$

e portanto $b = 0$. Logo, se $c = 0$, concluímos que

$$B = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$$

com $a \in Z(D)$, isto é, $B \in Z(D)$ e conseqüentemente, $d = 0$, o que é absurdo.

Então $c \neq 0$. Consideremos

$$U = \begin{bmatrix} 1 & a \\ 0 & c \end{bmatrix}$$

e

$$U^{-1} = \begin{bmatrix} 1 & -ac^{-1} \\ 0 & c^{-1} \end{bmatrix}$$

Tomando $C = U^{-1}BU$, é claro que C é da forma

$$\begin{bmatrix} 0 & \alpha \\ 1 & \beta \end{bmatrix}$$

e, para qualquer $A \in M_2(D)$ temos:

$$AC - CA = AU^{-1}BU - U^{-1}BUA = U^{-1}d(UAU^{-1})U.$$

Logo, a derivação interna dada por C também só toma valores inversíveis ou nulos.

Podemos então supor que d é uma derivação interna dada por uma matriz da forma

$$\begin{bmatrix} 0 & \alpha \\ 1 & \beta \end{bmatrix} \in M_2(D).$$

Neste caso, se $x \in D$, temos que:

$$\begin{aligned} d \left(\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \right) &= \begin{bmatrix} 0 & \alpha \\ 1 & \beta \end{bmatrix} \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} - \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \begin{bmatrix} 0 & \alpha \\ 1 & \beta \end{bmatrix} = \\ &= \begin{bmatrix} 0 & \alpha x - x \alpha \\ 0 & \beta x - x \beta \end{bmatrix}, \end{aligned}$$

que não é inversível. Logo, $\alpha x - x \alpha = \beta x - x \beta = 0 \quad \forall x \in D$, isto é,

$\alpha, \beta \in Z(D)$.

Pelo lema 4.15, sabemos que

$$d\left(\begin{bmatrix} 0 & \alpha \\ 1 & \beta \end{bmatrix}\right) = 0$$

implica que

$$\begin{bmatrix} 0 & \alpha \\ 1 & \beta \end{bmatrix}$$

é inversível e portanto $\alpha \neq 0$. Por este mesmo lema, temos que para todo $x \in D$,

$$d\left(\begin{bmatrix} x & 0 \\ 1 & 0 \end{bmatrix}\right) \neq 0$$

uma vez que

$$\begin{bmatrix} x & 0 \\ 1 & 0 \end{bmatrix}$$

não é inversível. Logo,

$$d\left(\begin{bmatrix} x & 0 \\ 1 & 0 \end{bmatrix}\right) = \begin{bmatrix} \alpha & -\alpha x \\ x + \beta & \alpha \end{bmatrix}$$

é inversível e portanto $\alpha x^2 + \alpha \beta x + \alpha^2 \neq 0 \ \forall x \in D$. Concluimos, en tão, que D não contém todas as extensões quadráticas de $Z(D)$.

Reciprocamente, se D não contém todas as extensões quadráticas de $Z(D)$ então existem $\alpha \in \beta Z(D)$, com $\alpha \neq 0$, tais que $\alpha x^2 - \beta x - 1$ não tem solução em D . Consideremos d , a derivação interna em $M_2(D)$ dada por

$$\begin{bmatrix} 0 & 1 \\ \alpha & \beta \end{bmatrix}.$$

Vamos mostrar que $d(A)=0$ ou $d(A)$ é inversível para todo $A \in M_2(D)$. De fato, dados x, y, z e $w \in D$ temos:

$$d\left(\begin{bmatrix} x & y \\ z & w \end{bmatrix}\right) = \begin{bmatrix} z - \alpha y & w - x - \beta y \\ \alpha(x - w) + \beta z & \alpha y - z \end{bmatrix}.$$

Sejam $a = z - \alpha y$ e $b = w - x - \beta y$. Então:

$$\alpha(x - w) + \beta z = -\alpha b + \beta a,$$

e portanto,

$$d\left(\begin{bmatrix} x & y \\ z & w \end{bmatrix}\right) = \begin{bmatrix} a & b \\ -\alpha b + \beta a & -a \end{bmatrix}.$$

Se $a=0$, é claro que

$$d\left(\begin{bmatrix} x & y \\ z & w \end{bmatrix}\right)$$

ou é zero ou é inversível pois $\alpha \neq 0$. Se $a \neq 0$ então:

$$\begin{bmatrix} a & b \\ -\alpha b + \beta a & -a \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & a^{-1}b \\ -\alpha a^{-1}b + \beta & -1 \end{bmatrix}$$

e portanto,

$$d \left(\begin{bmatrix} x & y \\ z & w \end{bmatrix} \right)$$

é inversível se e somente se

$$-1 - (a^{-1}b)(-\alpha a^{-1}b + \beta) = \alpha(a^{-1}b)^2 - \beta(a^{-1}b) - 1 \neq 0.$$

Mas pela escolha de α e β é claro que

$$\alpha(a^{-1}b)^2 - \beta(a^{-1}b) - 1 \neq 0.$$

Concluimos, então que $d(A) \neq 0$ ou $d(A)$ é inversível qualquer que seja $AGM_2(D)$.

//

Estamos agora em condições de provar o seguinte teorema, que é o resultado principal de [B.4]:

4.23 - TEOREMA. Sejam R um anel com unidade e $d \neq 0$ uma derivação em R tal que para todo $r \in R$, ou $d(r) = 0$ ou $d(r)$ é inversível. Então R satisfaz uma das seguintes condições:

(i) R é um anel com divisão.

(ii) $R=M_2(D)$ onde D é um anel com divisão.
 Além disto se $\text{card} D \neq 2$ este caso ocorre se e somente se D não contém todas as extensões quadráticas de $Z(D)$.

(iii) $R=D[X]/(X^2)$ onde D é um anel com divisão, $\text{card} D=2$, $d(D)=0$ e $d(X)=1+zX$ para algum $z \in Z(D)$.

DEMONSTRAÇÃO. Suponhamos que R não é um anel com divisão. Neste caso, existe L um ideal à esquerda próprio de R . O lema 4.15 e $L \neq R$ implicam $d(L) \neq 0$. Estamos, portanto, nas condições do teorema 4.21 e concluimos que $R=M_2(D)$ ou $R=D[X]/(X^2)$, $\text{card} R=2$ e $d(X)=1+zX$ para algum $z \in Z(D)$.

Se $R=M_2(D)$ então o lema 4.22 implica que R satisfaz (ii).

Se $R=D[X]/(X^2)$ para mostrarmos que R satisfaz (iii) só falta provar que $d(D)=0$. Ora, mas pelo lema 4.20 sabemos que $D=\{u \in R/d(u) \in L\}$. Como $L \neq R$, L não tem elementos inversíveis; logo, $d(u) \in L$ implica $d(u)=0$. Concluimos então que $D=\{u \in R/d(u)=0\}$ e, portanto, que $d(D)=0$.

//

O teorema que acabamos de demonstrar nos diz que se $R=M_2(D)$ é possível obtermos uma derivação d em R tal que os elementos não nulos de $d(R)$ são inversíveis se e somente se D não contém todas as extensões quadráticas de $Z(D)$. A seguinte proposição nos dá uma condição suficiente para que tenhamos uma derivação, $d \neq 0$, em $M_2(D)$ tal que os elementos não nulos de $d(L)$ são inversíveis, onde L é um ideal à esquerda de $M_2(D)$.

4.24 - PROPOSIÇÃO. Seja D um anel com divisão e

$$L = \left\{ \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \mid x, y \in D \right\}$$

ideal à esquerda de $M_2(D)$. Se existe $a \in D$, tal que a não é um quadrado em D então existe uma derivação d em $M_2(D)$ tal que todo elemento não nulo de $d(L)$ é inversível.

DEMONSTRAÇÃO. Seja d a derivação interna em $M_2(D)$ dada por

$$\begin{bmatrix} 0 & a \\ 1 & 0 \end{bmatrix}.$$

Dado

$$\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}$$

qualquer temos:

$$d\left(\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}\right) = \begin{bmatrix} ay & -xa \\ x & -ya \end{bmatrix} = \begin{bmatrix} ay & x \\ x & y \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -a \end{bmatrix}.$$

Como

$$\begin{bmatrix} 1 & 0 \\ 0 & -a \end{bmatrix}$$

é inversível em $M_2(D)$, temos que

$$d\left(\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}\right)$$

é inversível se e somente se

$$\begin{bmatrix} ay & x \\ x & y \end{bmatrix}$$

também o é. Ainda

$$d\left(\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}\right)=0$$

se e somente se

$$\begin{bmatrix} ay & x \\ x & y \end{bmatrix} = 0.$$

Ora, mas se $x=y=0$, então

$$\begin{bmatrix} ay & x \\ x & y \end{bmatrix} = 0$$

e portanto

$$d \left(\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \right) = 0.$$

Se, por outro lado, $x \neq 0$ ou $y \neq 0$ e

$$\begin{bmatrix} ay & x \\ x & y \end{bmatrix}$$

é não inversível, então existem r e $s \in D$ não ambos nulos tais que:

$$\begin{bmatrix} ay & x \\ x & y \end{bmatrix} \begin{bmatrix} r \\ s \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Logo,

$$ayr + xs = 0 \quad \text{e} \quad xr + ys = 0.$$

É fácil ver que se $r=0$, como $a \neq 0$ e $x \neq 0$ ou $y \neq 0$ temos que $s=0$. Portanto, $r \neq 0$ e obtemos:

$$ay = -xsr^{-1} \quad \text{e} \quad x = -ysr^{-1}.$$

Se $y=0$, então $x=0$ o que contradiz $x \neq 0$ ou $y \neq 0$. Portanto $y \neq 0$ e concluímos que:

$$a = -xsr^{-1}y^{-1} = -(-ysr^{-1})sr^{-1}y^{-1} = y(sr^{-1})^2y^{-1} =$$

$$=(ysr^{-1}y^{-1})^2,$$

o que contradiz a hipótese de que a não é um quadrado em D . Logo, se $x \neq 0$ ou $y \neq 0$ concluímos que

$$\begin{bmatrix} ay & x \\ x & y \end{bmatrix}$$

é inversível e, consequentemente, que

$$d \left(\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \right)$$

é inversível.

Portanto, todo elemento não nulo de $d(L)$ é inversível e provamos a proposição.

//

Finalizando o capítulo, mostraremos que podemos ter uma derivação em $M_2(D)$ tal que todo elemento não nulo de $d(L)$ seja inversível para um ideal lateral L e, no entanto, não existir nenhuma derivação δ em $M_2(D)$ tal que todo elemento de não nulo de $\delta(M_2(D))$ seja inversível.

Pela proposição 4.24 e pelo lema 4.22, basta tomarmos um anel com divisão D tal que $Z(D)$ é algebricamente fechado, mas D contém um elemento que não é um quadrado. Um anel deste tipo é o que nos dá o exemplo a seguir:

4.25 - EXEMPLO. Seja F o corpo de frações do anel de polinômios $\mathbb{C}[X]$, onde $\mathbb{C}$ é o conjunto dos números complexos. Consideremos D o conjunto das séries de Laurent.

$$\sum_{i=-n}^{+\infty} \frac{p_i(X)}{q_i(X)} Y^i$$

na variável Y com

$$\frac{p_i(X)}{q_i(X)} \in F.$$

Definimos a soma em D da forma usual e o produto induzido por:

$$Y \frac{p(X)}{q(X)} = \frac{p(2X)}{q(2X)} Y.$$

O conjunto D , munido de soma e produto é um anel com divisão e $Z(D) = \mathbb{C}$. Porém, é fácil verificar que $Y \notin D$ não é um quadrado em D .

BIBLIOGRAFIA

- [B.1] J.Bergen, "Lie ideals with regular and nilpotent elements and a result on derivations", a ser publi cado.
- [B.2] J.Bergen, "Prime rings and derivations", Thesis University of Chicago, 1981.
- [B.3] J.Bergen, I.N.Herstein e J.W.Kerr, "Lie ideals and derivations of prime rings", J.Algebra 71 (1981), 259-267.
- [B.4] J.Bergen, I.N.Herstein e C.Lanski, "Derivations with invertible values", Canad.J.Math. 35 (2) (1983), 300-310.
- [F.1] B.Falzenszwalb, "On a result of Levitzki", Canad. Math.Bull. 21 (2) (1978), 241-242.
- [F.2] B.Felzenszwalb, "Derivations in prime rings", Proc. Amer.Math.Soc. 84 (1) (1982), 16-20.
- [F.3] B.Felzenszwalb e A.Giambruno, "A commutativity theorem for rings with derivations", Pac.J.Math. 102 (1) (1982).
- [F.4] B.Felzenszwalb e C.Lanski, "On the centralizers of ideals and nil derivations", J.Algebra 83 (2)(1983), 520-530.

- [G.1] A.Giambruno e I.N.Herstein, "Derivations with nilpotent values", Rend.Circ.Mat.Palermo 30 (1981), 199-206.
- [H.1] I.N.Herstein, "A note on derivations", Canad.Math. Bull. 21 (1978), 369-370.
- [H.2] I.N.Herstein, "A note on derivations II", Canad. Math.Bull. 22 (1979), 509-511.
- [H.3] I.N.Herstein, "Center-like elements in prime rings", J.Algebra 60 (1979), 567-574.
- [H.4] I.N.Herstein, "Derivations in prime rings having power-central values", Contemp.Math. 13, Amer. Math. Soc., Providence, R.I. (1982), 163-171.
- [H.5] I.N.Herstein, "Invariant subrings of a certain kind", Israel J.Math. 26 (1977), 205-208.
- [H.6] I.N.Herstein, "Noncommutative rings", Carus Monograph 15, Math.Assoc.of Amer., 1968.
- [H.7] I.N.Herstein, "On the hypercenter of a ring", J. Algebra 36 (1975), 151-157.
- [H.8] I.N.Herstein, "Rings with involution", Univ.of Chicago Press, 1976.
- [H.9] I.N.Herstein, "Topics in ring theory", Univ.of Chicago Press, 1969.

- [J.1] N.Jacobson, "Structure of rings", Amer.Math.Soc. Colloquium Publications, 1956.
- [L.S] S.Lang, "Algebra", Addison-Wesley Publ.Comp.Inc., 1965.
- [L.1] C.Lanski, "Derivations with algebraic values", Communic. in Algebra 11 (20) (1983), 2349-2379.
- [P.M] F.C.Polcino Milies, "Derivations of full matrix rings", a ser publicado.
- [P.1] E.C.Posner, "Derivations in prime rings", Proc.Amer. Math.Soc. 8 (1957), 1.093-1.100.