SUA APLICAÇÃO EM EXTENSÕES

DE CORPOS

MARLY MANDIA

TESE APRESENTADA AO

*INSTITUTO DE MATEMÁTICA E ESTATÍSTICA*

DA

*UNIVERSIDADE DE SÃO PAULO*

PARA OBTENÇÃO DO GRAU DE MESTRE EM

MATEMÁTICA

ORIENTADOR: *Prof. Dr. LUIZ HENRIQUE JACY MONTEIRO*

Durante a elaboração deste trabalho, a autora recebeu apoio financeiro do BNDE, contratos FUNTEC nº 100 e 154 e FINEP convênio 184/C.T.

JULHO DE 1974

SÃO PAULO

à

Nininha

## AGRADECIMENTOS

Agradeço

ao Prof. Luiz Henrique Jacy Monteiro, pela orientação, estímulo e dedicação constantes, que fundamentalmente fizeram com que este trabalho existisse;

ao Prof. Alberto Azevedo, pela essencial contribuição matemática na execução deste trabalho;

ao Prof. Alésio João De Caroli, por me ter despertado o gosto pela matemática;

aos amigos, colegas e a todas as pessoas que de algum modo, me incentivaram neste início de carreira;

ao CNPq, ao BNDE e à FINEP que possibilitaram minha dedicação ao estudo da matemática;

ao Sr. João Baptista Esteves de Oliveira, pelo serviço de datilografia, e

ao Sr. Armando Garcia Segura, pelo trabalho de impressão.

*São Paulo, julho de 1974*

*Marly Mandia*

# P R E F Á C I O

A origem deste trabalho se deve aos seminários sobre *"Módulos das Diferenciais"* ministrados por Alberto Azevedo, segundo tratamento atribuído a R. Berger, quando da realização do III Curso de Verão, durante os meses de janeiro e fevereiro de 1974, no Instituto de Matemática e Estatística da Universidade de São Paulo.

Através da noção do conceito de diferencial em anéis comutativos, introduzido por P. Cartier, em [3],se iniciou e se desenvolveu a teoria sobre *"o módulo das diferenciais"* cuja aplicação, de modo geral, é usada no estudo de extensões de corpos e na teoria do ponto simples de variedades algébricas (Critério Jacobiano).

Neste presente trabalho, nos atemos ao estudo dos módulos das diferenciais e suas aplicações em extensões de corpos do tipo finito, e no problema de extensões de corpos que admitem prolongamento de derivações, aqui chamadas de extensões separáveis.

No capítulo I, encontramos resultados básicos para o desenvolvimento deste trabalho: apresentamos o conceito de derivação e suas propriedades fundamentais, e desenvolvemos um pequeno estudo sobre o prolongamento de uma derivação definida num corpo.

No capítulo II, introduzimos o conceito de "*derivação universal*" de um anel comutativo A, e, consequentemente, o conceito de "*módulo das diferenciais*". Mostramos a existência e unicidade (a menos de A-isomorfismos) do módulo das diferenciais (proposições 2.1.1 e 2.1.2) e damos exemplos básicos de derivações universais. A seguir, desenvolvemos um estudo sobre extensões universais de derivações, com o objetivo maior de recairmos numa nova prova de existência do módulo das diferenciais (teorema 2.5.1), através da qual, uma nova expressão para o módulo das diferenciais se apresenta e se justifica por sua utilidade prática na obtenção de resultados que apresentamos nos capítulos que seguem.

Como aplicação do módulo das diferenciais, desenvolvemos, no capítulo III, um estudo sobre extensões de corpos do tipo finito. Introduzimos, inicialmente, o conceito de inseparabilidade de uma extensão do tipo finito, seguindo de perto o tratamento dado por P. Cartier, em [3], e por S. Suzuki, em [9] . Obtemos, a seguir, critérios que caracterizam as extensões algébricas separáveis do tipo finito (teorema 3.2.1) e, mais geralmente, extensões algébricas separavel mente geradas do tipo finito (teorema 3.2.2). Damos uma caracterização dos corpos perfeitos (teorema 3.2.3) e apresentamos um resultado que determina a dimensão do módulo das diferenciais quando se trabalha com extensões de corpos do tipo finito e de característica diferente de zero (teorema 3.2.4). Fazemos um estudo sobre o número mínimo de geradores de uma extensão do tipo finito (teorema 3.2.5) e concluimos esta parte do trabalho, com um resultado (teorema 3.2.6) que nos dá condições necessárias e suficientes para que uma extensão de corpos do tipo finito seja separavelmente gerada.

No capítulo IV, seguindo o tratamento dado por Y. Nakai, em [7], resolvemos o problema geral do prolongamento de derivações (teorema 4.1.1). Desenvolvemos, em seguida, um estudo sobre extensões separáveis de corpos, e conseguimos, através do teorema 4.2.2, relacionar nosso trabalho com resultados obtidos por S. MacLane, em [6].

*Marly Mandia*

# Í N D I C E

CAPÍTULO I

# DERIVAÇÕES

Em todo este trabalho, todos os anéis serão supostos comutativos com elemento unidade denotado por 1, e todos os módulos serão unitários.

## 1.1 - *Definições*

Seja A um anel e seja M um A-módulo.

1.1.1 - Uma aplicação D: A $\longrightarrow$ M diz-se uma derivação de A a valores em M, se D satisfaz às seguintes propriedades:

$$\text{D1: } (\forall x,y \in A)(D(x+y) = Dx+Dy)$$

$$\text{D2: } (\forall x,y \in A)(D(x+y) = xDy+yDx)$$

Uma vez fixado o A-módulo M, nos referiremos a uma derivação de A a valores em M, como simplesmente uma derivação de A.

1.1.2 - Uma derivação de A a valores em M que se anula num subanel P de A, diz-se uma P-derivação de A.

Escreveremos:

$Der(A,M) = \{D: A \longrightarrow M : D \text{ é uma derivação}\}$

$Der_P(A,M) = \{D: A \longrightarrow M : D \text{ é uma P-derivação}\}$

## 1.2 - *Propriedades das Derivações*

1.2.1 - Se $D: A \longrightarrow M$ é uma derivação, o conjunto dos elementos de A anulados por D é um subanel de A com elemento unidade 1.

A demonstração é trivial. □

1.2.2 - Se $D: A \longrightarrow M$ é uma derivação, então $(\forall n \in \mathbb{N}, n>0)$ $(\forall x \in A)(D(x^n) = nx^{n-1}Dx)$.

A demonstração segue facilmente por indução sobre o natural n. □

1.2.3 - Sejam $D_1: A \longrightarrow M$, $D_2: A \longrightarrow M$ duas P-derivações e $\lambda: M \longrightarrow N$ um homomorfismo de A-módulos. Então:

a) $D_1 + D_2: A \longrightarrow M$ definida por $(\forall x \in A)((D_1+D_2)(x)=D_1x+D_2x)$ é uma P-derivação.

b) Se $a \in A$, $aD_1: A \longrightarrow M$ definida por $(\forall x \in A)((aD_1)(x)=aD_1x)$ é uma P-derivação.

c) $\lambda \circ D_1: A \longrightarrow N$ é uma P-derivação.

A demonstração segue trivialmente das definições. □

## 1.3 - *Observações*

1.3.1 - Toda P-derivação $D: A \longrightarrow M$ é P-linear.

1.3.2 - Se A é um anel primo, então a única derivação de A a valores num A-módulo M, é a derivação trivial, isto é, a derivação que leva todo elemento de A, no elemento zero de M.

1.3.3 - Se P é o subanel primo de A, então toda derivação $D: A \longrightarrow M$ é uma P-derivação.

1.3.4 - Se a característica de A é $p \neq 0$, então toda derivação $D: A \longrightarrow M$ é uma $[A^p]$-derivação.

1.3.5 - $Der(A,M)$ com as operações definidas em 1.2.3, a) e b), é um A-módulo e $Der_P(A,M)$ é um submódulo do A-módulo $Der(A,M)$.

1.3.6 - A definição de uma P-derivação pode ser generalizada do seguinte modo:

Seja $\phi: P \longrightarrow A$ um homomorfismo de anéis com $\phi(1) = 1$ e M um A-módulo. Uma derivação $D: A \longrightarrow M$ diz-se uma P-derivação de A se $(\forall x \in P)(D(\phi(x)=0)$.

Notemos que A é uma P-álgebra se definirmos $x.a = \phi(x)a$ para todo x em P e todo a em A.

Usaremos de agora em diante esta definição. Se $x \in P$, escreveremos Dx significando $D(\phi(x))$. Também, sempre que escrevermos "o anel A é uma P-álgebra", estaremos supondo a existência de um homomorfismo de anéis $\phi: P \longrightarrow A$ tal que $\phi(1) = 1$.

Logo, uma derivação $D: A \longrightarrow M$ é uma P-derivação de A em M, se D é P-linear.

## 1.4 - *Exemplos de Derivações*

1.4.1 - Seja $D: A \longrightarrow A$ uma derivação, e $R = A[X_1,\dots,X_n]$ o anel de polinômios a n indeterminadas. Sendo $\alpha$ a ênupla $(i_1,i_2,\dots,i_n)$ com $i_j \in \mathbb{N}$ para todo $j=1,\dots,n$, e $M_\alpha(X) = X_1^{i_1},\dots X_n^{i_n}$, seja $f = \sum_\alpha a_\alpha M_\alpha(X) \in R$. Denotaremos por $f^D$ o polinômio $\sum_\alpha D(a_\alpha) M_\alpha(X) \in R$.

Um cálculo direto nos mostra que a aplicação $\bar{D}:R\longrightarrow R$ definida por $(\forall f\in R)(\bar{D}f=f^D)$, é uma derivação que estende D, isto é, tal que $\bar{D}|_A = D$.

1.4.2 - Sejam A um anel e $R = A[\{X_i\}_{i\in I}]$ o anel de polinômios nas indeterminadas $X_i$ indexadas por um conjunto de índices I. Para cada $i\in I$, denotemos por $S_i = \{X_j: \ j\in I \text{ e } j\neq i\}$, e por $R_i = A[S_i]$. Então $R = R_i[X_i]$ é um anel de polinômios a uma indeterminada sobre o anel $R_i$. Se $f = \sum_j a_j X_i^j \in R_i[X_i]$, denotaremos por $f_{X_i}$ ou $\frac{\partial f}{\partial X_i}$ o polinômio $\sum_j a_j X_i^{j-1} \in R$. Um cálculo direto nos mostra que a aplicação $D: R \longrightarrow R$ definida por $(\forall f\in R)(Df = \frac{\partial f}{\partial X_i})$ é uma $R_i$-derivação. Denotaremos tal derivação por $D_i$ ou $\frac{\partial}{\partial X_i}$. Tem-se que $D_i(X_j) = \delta_{ij}$. Também, D1 e D2 nos mostram que $D_i$ $(i\in I)$ é unicamente determinada pelas condições de que é trivial em A e de que satisfaz $D_i(X_j) = \delta_{ij}$ para $j\in I$.

No caso particular de $R = A[X]$ tem-se que $D_1 f = f'$, onde $f'$ indica a derivada usual de um polinômio.

1.4.3 - Seja $D: A \longrightarrow M$ uma derivação e seja S um sistema multiplicativo de A. Sendo $A_S$ o anel das frações de A a denominadores em S, e $M_S$ o $A_S$-módulo das frações de A a denominadores em S, a aplicação $\Delta: A_S \longrightarrow M_S$ definida por $(\forall x\in A)(\forall s\in S)(\Delta(\frac{x}{s}) = \frac{sDx-xDs}{s^2})$ é uma derivação.

Mostraremos que $\Delta$ está bem definida. Sejam $x,x'\in A$, $s,s'\in S$ com $\frac{x}{s} = \frac{x'}{s'}$; logo existe $s''\in S$ tal que $s''(s'x-sx') = 0$; portanto $0 = D(0) = D(s''(s'x-sx')) = (s'x-sx')Ds''+s''(s'Dx+xDs'-sDx'-x'Ds)$; multiplicando-se por $ss's''$ temos que:

$0=s''(ss's''s'Dx+s(s''s'x)Ds' - ss's''sDx' - s'(s''sx')Ds$; desde que $s''s'x = s''sx'$, vem que $0 = s''(ss's''s'Dx + s(s''sx')Ds' - ss's''sDx' - s'(s''s'x)Ds)$, isto é, $0 = (s'')^2((s')^2(sDx-xDs) - s^2(s'Dx' - x'Ds'))$; como $(s'')^2 \in S$ segue que $\frac{sDx-xDs}{s^2} = \frac{s'Dx'-x'Ds'}{(s')^2}$, isto é, $\Delta(\frac{x}{s}) = \Delta(\frac{x'}{s'})$.

Um cálculo direto nos mostra que $\Delta$ satisfaz D1 e D2.

No caso particular em que A é um domínio de integridade, e M é um k-módulo onde k é o corpo de frações de A, então $\Delta: k \longrightarrow M$ definida por $(\forall x \in A)(\forall y \in A^*)(\Delta(\frac{x}{y}) = \frac{yDx-xDy}{y^2})$ é uma derivação de k que prolonga D. Mais ainda, $\Delta$ é a única derivação de k que estende D. De fato, seja $\Delta': k \longrightarrow M$ uma extensão de D; logo $(\forall x \in A)(\forall y \in A^*)$ vale: $Dx = \Delta' x = \Delta'(y\frac{x}{y}) = Dx + \frac{x}{y}\Delta' y = y\,\Delta'(\frac{x}{y}) + \frac{x}{y} Dy$; portanto $y\,\Delta'(\frac{x}{y}) = Dx - \frac{x}{y} Dy$, de onde segue que $\Delta'(\frac{x}{y}) = \frac{yDx-xDy}{y^2} = \Delta(\frac{x}{y})$; logo $\Delta' = \Delta$.

## 1.5 - *Derivações no Anel de Polinômios*

*Teorema 1.5.1* - Seja A um anel e seja $R = A[\{X_i\}_{i \in I}]$ o anel de polinômios nas indeterminadas $X_i$, $i \in I$. Sendo $D: R \longrightarrow M$ uma derivação de R a valores num R-módulo M, vale: $(\forall f \in R)(Df = f^D + \sum_i \frac{\partial f}{\partial X_i} DX_i)$.

*Demonstração:*

Seja $f \in R$; logo existe um número finito de indeterminadas que notaremos por $X_1, \ldots, X_n$ tal que $f \in A[X_1, \ldots, X_n]$. Seja $g = a\, X_1^{q_1}, \ldots, X_n^{q_n}$ um monômio de f, onde $a \in A$ e $q_i \in \mathbb{N}$ pa ra $i=1,2,\ldots,n$. Então

$$Dg = D(a)X_1^{q_1}\cdot\ldots\cdot X_n^{q_n} + aD(X_1^{q_1}\cdot\ldots\cdot X_n^{q_n}) =$$

$$= g^D + a\sum_{i=1}^{n} X_1^{q_1}\cdot\ldots\cdot \widehat{X_i^{q_i}}\cdot\ldots\cdot X_n^{q_n}D(X_i^{q_i}) =$$

$$= g^D + \sum_{i=1}^{n} a\, q_i\, X_1^{q_1}\ldots X_i^{q_i-1}\ldots X_n^{q_n}DX_i$$

$$= g^D + \sum_{i=1}^{n} \frac{\partial g}{\partial X_i} DX_i$$

Estendendo por linearidade vem a tese. □

Uma consequência imediata deste teorema é dada pelo

*Corolário 1.5.1* - Seja $D_0\colon A \longrightarrow M$ uma derivação de A a valores num R-módulo M, onde $R = A[\{X_i\}_{i\in I}]$. Seja $\{m_i\}_{i\in I}$ uma família de elementos de M. Então existe uma única derivação $D\colon R \longrightarrow M$ que prolonga $D_0$, isto é, tal que $D_0 = D|_A$, e tal que $(\forall i\in I)(DX_i = m_i)$. Ela é dada por $(\forall f\in R)(Df=f^{D_0} + \sum_i \frac{\partial f}{\partial X_i}m_i)$.

## 1.6 - *Prolongamento de Derivação Definidas Num Corpo*

*Teorema 1.6.1* - Sejam k um corpo, $K = k(x_1,\ldots,x_n)$ uma extensão de k do tipo finito, $D\colon k \longrightarrow M$ uma derivação de k a valores num K-espaço vetorial M, e $m_1,\ldots, m_n$ elementos de M. Seja ainda, $\{f_\lambda\}$ um sistema de geradores do ideal das relações algébricas satisfeitas por $x_1,\ldots,x_n$ sobre k. Então, existe uma derivação $\Delta\colon K \longrightarrow M$ que estende D se, e somente se

(1) $$f_\lambda^D(x_1,\ldots,x_n) + \sum_{i=1}^{n} \frac{\partial f_\lambda}{\partial x_i}\cdot m_i = 0 \text{ para todo } \lambda.$$

($\frac{\partial f_\lambda}{\partial x_i}$ indica $\frac{\partial f_\lambda}{\partial X_i}(x_1,\dots,x_n)$). Ainda mais , se (1) for satisfeita, $\Delta$ é determinada de modo único.

*Demonstração:*

Seja $\Delta$: K $\longrightarrow$ M uma derivação de K que estende D nas condições exigidas. Então, procedendo-se analogamente à demonstração do teorema 1.5.1, vale:

$$(\forall g \in k[X_1,\dots,X_n])(\Delta(g(x_1,\dots,x_n)) = g^D(x_1,\dots,x_n) + \sum_{i=1}^{n} \frac{\partial g}{\partial x_i}\ \Delta x_i)$$

Como $\Delta 0=0$, $f_\lambda(x_1,\dots,x_n) = 0$ para todo $\lambda$, e $\Delta x_i = m_i$ para $i=1,\dots,n$, vem que

$$f_\lambda^D(x_1,\dots,x_n) + \sum_{i=1}^{n} \frac{\partial f_\lambda}{\partial x_i}\cdot m_i = 0 \text{ para todo } \lambda.$$

Reciprocamente, suponhamos que valha (1). Definamos $\Delta'$: $k[x_1,\dots,x_n] \longrightarrow M$ por

$$(\forall g \in k[X_1,\dots,X_n])(\Delta'(g(x_1,\dots,x_n)) = g^D(x_1,\dots,x_n) + \sum_{i=1}^{n} m_i \frac{\partial g}{\partial x_i})$$

$\Delta'$ está bem definida pois se $g,f \in k[X_1,\dots,X_n]$ com $g(x_1,\dots\dots,x_n) = f(x_1,\dots,x_n)$, toma-se $h=g-f$ e tem-se que $h(x_1,\dots\dots,x_n) = 0$; da hipótese (1) vem que $h^D(x_1,\dots,x_n) + \sum_{i=1}^{n} m_i \frac{\partial h}{\partial x_i} = 0$, e imediatamente segue que

$$g^D(x_1,\dots,x_n) + \sum_{i=1}^{n} m_i \frac{\partial g}{\partial x_i} = f^D(x_1,\dots,x_n) + \sum_{i=1}^{n} m_i \frac{\partial g}{\partial x_i} ,$$

isto é, $\Delta'(g(x_1,\dots,x_n)) = \Delta'(f(x_1,\dots,x_n))$. Claramente $\Delta'$ é uma derivação de $k[x_1,\dots,x_n]$ que estende D e é tal que $\Delta' x_i = m_i$ para todo $i=1,\dots,n$. Também, $\Delta'$ é única nestas condições, já que toda derivação $\Delta''$ de $k[x_1,\ldots,x_n]$ que estende $D$ é dada por $(\forall g \in k[x_1,\ldots,x_n])(\Delta''(g(x_1,\ldots,x_n)) = g^D(x_1,\ldots,x_n) + \sum \frac{\partial g}{\partial x_i}\Delta'' x_i)$ e, portanto, $(\forall g \in k[X_1,\ldots,X_n])(\Delta''(g(x_1,\ldots,x_n)) = g^D(x_1,\ldots,x_n) + \sum \frac{\partial g}{\partial x_i} m_i = \Delta'(g(x_1,\ldots,x_n))$, isto é, $\Delta'' = \Delta'$.

Do exemplo 1.4.3 segue que existe uma única derivação $\Delta\colon K \longrightarrow M$ que estende $\Delta'$. Logo existe uma única derivação $\Delta\colon k \longrightarrow M$ que estende $D$ nas condições pedidas. □

*Proposição 1.6.1* - Sejam $k$ um corpo, $K=k(x)$ uma extensão simples de $k$, $D\colon k \longrightarrow M$ uma derivação de $k$ a valores num $K$-espaço vetorial $M$.

(a) se $x$ é transcendente sobre $k$, existe uma derivação de $K$ em $M$ que estende $D$; mais precisamente, para cada $m \in M$ existe uma única derivação $\Delta$ de $K$ em $M$ que estende $D$ e tal que $\Delta x = m$.

(b) Se $x$ é algébrico separável sobre $k$, existe uma única derivação de $K$ em $M$ que estende $D$.

(c) se $k$ tem característica $p \neq 0$, e se $x$ é puramente inseparável sobre $k$, então, sendo $n$ o menor natural $(n \geq 1)$ tal que $x^{p^n} \in k$, $D$ admite uma derivação $\Delta$ de $K$ em $M$ que estende $D$ se, e somente se, $D(x^{p^n}) = 0$; neste caso $\Delta x$ pode ser tomado arbitrariamente em $M$.

*Demonstração:*

(a) Como $x$ é transcendente sobre $k$, então se $g \in k[X]$ é tal que $g(x) = 0$, tem-se que $g = 0$.

Para cada $m \in M$, tem-se trivialmente que $0^D(x)+m\frac{\partial 0}{\partial x} = 0$ e o resultado segue imediatamente do teorema 1.6.1.

(b) Seja $f \in k[X]$ o polinômio minimal de x sobre k. Neste caso, f gera o ideal das relações algébricas satisfeitas por x. Como $f'(x) \neq 0$, a expressão $f^D(x)+mf'(x)$ se anula para um único $m \in M$, precisamente para $m=-\frac{f^D(x)}{f'(x)}$. Do teorema 1.6.1 segue facilmente que existe uma única derivação $\Delta: K \longrightarrow M$ que estende D e é tal que $\Delta x = m$.

(c) Sendo $y = x^{p^n}$, sabe-se que o polinômio minimal de x sobre k é $f = X^{p^n} - y \in k[X]$ e tem-se que f gera o ideal das relações algébricas satisfeitas por x. Também, $f^D(x) = Dy$ e $f'(x) = 0$; logo a expressão $f^D(x)+mf'(x) = 0$ é satisfeita se, e só se, $Dy = 0$ e, neste caso m pode ser tomado arbitrariamente. O resultado segue então, imediatamente do teorema 1.6.1. □

*Teorema 1.6.2* - Sejam k um corpo, K uma extensão de k, $M \neq (0)$ um K-espaço vetorial e $D: k \longrightarrow M$ uma derivação.

(a) Se k tem característica zero, existe $\Delta: K \longrightarrow M$ derivação de K que estende D de tal modo que se x é transcendente sobre k, $\Delta x \neq 0$.

(b) Se k tem característica $p \neq 0$, e se $K^p \subset k$, existe derivação $\Delta: K \longrightarrow M$ que estende D de tal modo que se $x \notin k$, $\Delta x \neq 0$.

*Demonstração:*

(a) Considerando $\eta = \{(K',D') : K'$ é um corpo intermediário entre k e K, $D': K' \longrightarrow M$ derivação que estende D$\}$, vemos que

$\eta \neq \phi$ e $\eta$ é indutivo por prolongamento. Logo, pelo lema de Zorn, existe $(\bar{K}, \bar{D})$ elemento maximal de $\eta$. Se $\bar{K} \neq K$, seja $y \in K$, $y \notin \bar{K}$. Considerando a extensão $\bar{K}(y)$ de $\bar{K}$, e observando que a característica de $\bar{K}$ é zero, segue pela proposição anterior que existe $\bar{\bar{D}}: \bar{K}(y) \longrightarrow M$ derivação que prolonga $\bar{D}$ e que, portanto, prolonga $D$. Chegamos a um absurdo já que $(\bar{K}, \bar{D})$ é maximal. Logo $K = \bar{K}$. Da parte (a) da proposição acima, é claro que podemos tomar uma derivação $\Delta: K \longrightarrow M$ que estende $D$ e tal que $\Delta x \neq 0$ se $x \in K$ é transcendente sobre $k$.

(b) Do mesmo modo que em (a), consideremos o conjunto $\eta$ e seja $(\bar{K}, \bar{D})$ um elemento maximal de $\eta$. Se $K \neq \bar{K}$, seja $x \in K$, $x \notin \bar{K}$ e tomemos a extensão $\bar{K}(x)$ de $\bar{K}$. Como $K^p \subset k$, $x^p \in k \subset \bar{K}$ e, portanto $x$ é puramente inseparável sobre $\bar{K}$. Como $\bar{D}(x^p)=0$ já que a característica de $k$ é $p$, segue pela parte (c) da proposição anterior que existe $\bar{\bar{D}}: \bar{K}(x) \longrightarrow M$ derivação que prolonga $\bar{D}$ e que portanto estende $D$. Chegamos a um absurdo e, logo, $K = \bar{K}$. Se $y \in K$ é tal que $y \notin k$, como $y^p \in k$, temos que o polinômio minimal de $y$ sobre $k$ é $X^p - y^p$; logo pela demonstração da parte (c) da proposição anterior, segue que uma derivação $\Delta: K \longrightarrow M$ que estende $D$, pode ser tomada de tal modo que $\Delta y \neq 0$. □

*Corolário 1.6.1* - Sejam $K$ um corpo com características $p \neq 0$ e $M \neq (0)$ um $K$-espaço vetorial. O conjunto de todos os elementos de $K$ tais que $Dx = 0$ para toda derivação $D: K \longrightarrow M$ é exatamente $K^p$.

*Demonstração:*

Obviamente $(\forall x \in K^p)(Dx=0)$. Suponhamos então que exis te $x \in K-K^p$ com $Dx=0$ para toda derivação de $K$. Consideremos $L = K^p(x)$; temos $x$ puramente inseparável sobre $K^p$ pois $x^p \in K^p$ e temos $x \notin K^p$; logo, pela parte (b) do teorema 1.6.2, existe $\bar{D}$ derivação de $L$ tal que $\bar{D}y = 0$ para todo $y \in K^p$ e tal que $\bar{D}x \neq 0$. Chegamos a um absurdo já que $Dx=0$ para toda derivação de $K$. E o corolário está provado. □

*Corolário 1.6.2* - Sejam $k$ um corpo, $K$ uma extensão de $k$, e $M \neq (0)$ um $K$-espaço vetorial.

(a) Se a característica de $k$ é zero, o conjunto dos elementos de $K$ tais que $Dx=0$ para toda $k$-derivação $D: K \longrightarrow M$, é o fecho algébrico de $k$ em $K$.

(b) Se a característica é $p \neq 0$, o conjunto dos elementos de $K$ anulados por toda $k$-derivação $D: K \longrightarrow M$ é $k(K^p)$.

*Demonstração:*

(a) Seja $x \in K$ algébrico sobre $k$ e seja $f \in k[X]$ o polinômio minimal de $x$ sobre $k$; pela proposição 1.6.1 segue que $Dx = -\frac{f^D(x)}{f'(x)}$ para toda $k$-derivação $D: K \longrightarrow M$. Como $Dy=0$ para todo $y \in k$, vem que $f^D(x)=0$ e, portanto, $Dx=0$ para todo $k$-derivação de $K$.

Reciprocamente, seja $x \in K$ com $Dx=0$ para todo $k$-derivação $D$ de $K$. Se $x$ for transcendente sobre $k$, pela parte (a) do teorema 1.6.2, existe $\bar{D}: K \longrightarrow M$ uma $k$-derivação de $K$ tal que $\bar{D}x \neq 0$, o que é absurdo já que $Dx = 0$ para toda $k$-derivação de K.

(b) a demonstração é análoga a do corolário 1.6.1. □

*Proposição 1.6.2* - Sejam $k$ um corpo, $K = k(\{x_\lambda\}_{\lambda\in\Lambda})$, $K/k$ uma extensão transcendente pura, $D: k \longrightarrow M$ uma derivação de $k$ a valores num $K$-espaço vetorial $M$, e $\{m_\lambda\}_{\lambda\in\Lambda}$ uma família de elementos de $M$. Então existe uma única derivação $\Delta: K \longrightarrow M$ que estende $D$ tal que $(\forall\lambda\in\Lambda)(\Delta x_\lambda = m_\lambda)$.

*Demonstração:*

O resultado vem de modo análogo à demonstração do teorema 1.6.2, usando-se o lema de Zorn e a proposição 1.6.1, parte (a). □

*Proposição 1.6.3* - Se $K/k$ é uma extensão de corpos algébrica separável, então, para todo $K$-espaço vetorial $M$, toda derivação de $k$ a valores em $M$ pode ser prolongada a uma derivação de $K$ a valores em $M$.

*Demonstração:*

Usando-se o lema de Zorn e a proposição 1.6.1, parte (b), a demonstração é análoga a do teorema 1.6.2. □

## CAPÍTULO II

## MÓDULOS DAS DIFERENCIAIS

### 2.1 - *Derivações Universais*

Sejam A,P anéis, A uma P-álgebra, M um A-módulo.

*Definição 2.1.1* - Uma derivação universal de A sobre P é uma P-derivação de A, $d: A \longrightarrow M$, tal que para todo A-módulo N, se $D: A \longrightarrow N$ é uma P-derivação de A, então existe um único homomorfismo $\lambda: M \longrightarrow N$ de A-módulos que torna o diagrama, ao lado, comutativo, isto é, $D = \lambda o d$.

$$\begin{tikzcd} & N \\ A \arrow[ur, "D"] \arrow[r, "d"'] & M \arrow[u, "\lambda"'] \end{tikzcd}$$

*Definição 2.1.2* - Diz-se que $d: A \longrightarrow M$ é uma derivação universal de A, se d é uma derivação universal de A sobre P, onde P é o anel primo de A.

*Proposição 2.1.1* - Se $d: A \longrightarrow M$ e $\partial: A \longrightarrow N$ são duas derivações universais de A sobre P, então existe um isomorfismo $\lambda: M \longrightarrow N$ de A-módulos tal que $\lambda o d = \partial$.

*Demonstração:*

Da definição 2.1.1, existem dois homomorfismos de A-módulos, $\lambda$ e $\lambda'$ tai que $\lambda o d=\partial$ e $\lambda' o \partial = d$; portanto $\partial = (\lambda o \lambda') o d$

$$\begin{tikzcd} & N \arrow[d, shift left, "\lambda'"] \\ A \arrow[ur, "\partial"] \arrow[r, "d"'] & M \arrow[u, shift left, "\lambda"] \end{tikzcd}$$

e $d=(\lambda' o \lambda) o d$; como $1_M$ e $1_N$ são os únicos homomorfismos de A-módulos tais que $d=1_M o d$ e $\partial=1_N o \partial$, segue que $\lambda' o \lambda = 1_M$ e $\lambda o \lambda' = 1_N$, isto é, $\lambda$ é um isomorfismo de A-módulos. $\square$

*Proposição 1.2.1* - Existe uma derivação universal de A sobre P.

*Demonstração:*

Consideremos o A-módulo $M_1 = A \underset{P}{\otimes} A$ ($M_1$ é um A-módulo se definirmos $a\cdot(x\otimes y) = ax\otimes y$ para quaisquer $a,x,y\in A$), e $M_2$ o A-submódulo de $M_1$ gerado pelos elementos do tipo $1\otimes xy - x\otimes y - y\otimes x$ para todo $x,y$ em A. Seja $M = M_1/M_2$ e seja $d: A \longrightarrow M$ definida por $(\forall x\in A)(dx=\overline{1\otimes x}$ = classe módulo $M_2$ determinada pelo elemento $1\otimes x$ de $M_1$).

d é uma derivação universal de A sobre P. Temos que

$(\forall x,y\in A)(d(x+y) = \overline{1\otimes(x+y)} = \overline{1\otimes x+1\otimes y} = \overline{1\otimes x}+\overline{1\otimes y} = dx+dy)$;

$(\forall x,y\in A)(dxy = \overline{1\otimes xy} = \overline{x\otimes y+y\otimes x} = \overline{x\otimes y}+\overline{y\otimes x} = \overline{x(1\otimes y)} +$

$+ \overline{y(1\otimes x)} = x(\overline{1\otimes y}) + y(\overline{1\otimes x}) = xdy + ydx)$;

$(\forall x\in P)(dx = \overline{1\otimes x} = \overline{x(1\otimes 1)} = x(\overline{1\otimes 1}) = xd1 = 0)$;

logo d é uma P-derivação. Seja agora $D: A \longrightarrow N$ uma P-derivação a valores num A-módulo N; a aplicação $\Psi: A\times A \longrightarrow N$ definida por $(\forall x,y\in A)(\Psi(x,y) = xDy)$ é P-bilinear já que D é P-linear; logo pela propriedade universal do produto tensorial, exis te um único homomorfismo de P-módulos $\lambda': A\underset{P}{\otimes}A \longrightarrow N$ tal que $(\forall x,y\in A)(\lambda'(x\otimes y)=xDy)$; $\lambda'$ é também um homomorfismo de A-módulos já que $(\forall a,x,y\in A)(\lambda'(a(x\otimes y) = \lambda'(ax\otimes y) = (ax)Dy = a(xDy) = a\lambda'(x\otimes y))$; como $(\forall x,y\in A)(\lambda'(1\otimes xy-x\otimes y-y\otimes x) = Dxy-xDy-yDx=0)$, segue que $M_2\subseteq Ker(\lambda')$ e, portanto, $\lambda'$ induz o homomorfismo de

$$\begin{tikzcd} & N \\ A \arrow[ur, "D"] \arrow[r, "d"'] & M \arrow[u, "\lambda"'] \end{tikzcd}$$

A-módulos $\lambda: M \longrightarrow N$ definido por $(\forall m\in M_1)(\lambda\bar{m}=\lambda'm)$; $\lambda$ satisfaz as condições exigidas pois, $(\forall x\in A)((\lambda o d)(x) = \lambda(\overline{1\otimes x}) = \lambda'(1\otimes x) = Dx)$, isto é, $\lambda o d = D$; também, sendo $\lambda_1: M \longrightarrow N$ um homomorfismo de A-módulos tal que $\lambda_1 od=\lambda od = D$, temos que $(\forall x,y\in A)(\lambda_1(\overline{x\otimes y}) = \lambda_1(x(\overline{1\otimes y})) = x\lambda_1(\overline{1\otimes y}) = x\lambda_1(dy) = x(\lambda_1 od)(y) = x(\lambda od)(y) = x\lambda(dy) = x\lambda(\overline{1\otimes y}) = \lambda(x(\overline{1\otimes y})) = \lambda(\overline{x\otimes y}))$, isto é, $\lambda_1 = \lambda$.

E a proposição está provada. □

*Definição 2.1.3* - Se $d: A \longrightarrow M$ é uma derivação universal de A sobre P, o elemento da é denominado "diferencial de a", e M é denominado "módulo das diferenciais de A sobre P", ou "módulo das P-diferenciais de A" e será denotado por $D(A|P)$. Se P é o subanel primo de A, diz-se simplesmente que M é um "módulo das diferenciais de A".

As proposições acima nos mostram que o módulo das diferenciais pode ser caracterizado, a menos de isomorfismos, por uma propriedade universal.

*Proposição 2.1.3* - Se $d: A \longrightarrow D(A|P)$ é uma derivação universal de A sobre P, então $D(A|P)$ é gerado por $dA = \{dx : x \in A\}$, isto é, $D(A|P) = AdA$.

*Demonstração:*

Seja $M^* = AdA$ e seja $d^*: A \longrightarrow M^*$ definida por $(\forall x \in A)(d^*a = da)$; pela propriedade universal de d, existe um único homomorfismo de A-módulos $\lambda: M \longrightarrow M^*$ tal que $\lambda o d = d^*$; sendo $i: M^* \longrightarrow M$ a inclusão canônica, então $d = i o d^* = i o(\lambda o d) = (i o \lambda) o d$; como $1_M$ é o único homomorfismo de A-módulos tal que $d = 1_M o d$, segue que $i o \lambda = 1_M$, e, portanto, i é também sobrejetora; logo $M = M^*$. □

*Observação 2.1.1* - Sendo M, N, A-módulos, e denotando por $Hom(M,N) = \{\delta : M \longrightarrow N : \delta \text{ é A-linear}\}$, então, $d: A \longrightarrow M$ é uma derivação universal de A sobre P se, e somente se, a aplicação $\phi: Hom(M,N) \longrightarrow Der_P(A,N)$ definida por $(\forall \lambda \in Hom(M, N))$ $(\phi(\lambda) = \lambda \circ d)$ é um isomorfismo de A-módulos. Logo, temos que $Hom(D(A|P), N) \approx Der_P(A, N)$ como A-módulos.

*Observação 2.1.2* - Um caso particular da observação anterior é dado quando $N = K$ é um corpo, e $D(K|P)$ é um K-espaço vetorial de dimensão finita. Temos então que $Der_P(K,K) \approx D(K|P)^*$ onde $D(K|P)^*$ indica o dual do K-espaço vetorial $D(K|P)$. Neste caso, $Der_P(K,K)^* = D(K|P)$, isto é, se $a \in K$, a diferencial de a, da, se identifica a um elemento do espaço dual das P-derivações de K que assumem valores em K; assim se $D: K \longrightarrow K$ é uma P-derivação de K, $Da = < da, D >$. Usualmente o conceito de di ferencial é introduzido desta maneira; por exemplo, se V é uma variedade diferenciável, a diferencial local num ponto de V é o espaço dual do espaço dos vetores tangentes à variedade no dado ponto. Daí ser atribuído a $D(A|P)$ o nome de módulo das diferenciais.

*Observação 2.1.3* - Se k é um corpo e K é uma extensão de k, então uma derivação universal de K sobre k tem como núcleo, o fecho algébrico de k em K, se a característica de k é zero; se a característica de k é $p \neq 0$, então o núcleo de uma derivação universal de K sobre k, é $k(K^p)$. Este resultado segue do corolário 1.6.2.

## 2.2 - *Exemplos de Derivações Universais*

*Proposição 2.2.1* - Seja P um anel e $A = P[\{X_i\}_{i \in I}]$ o anel de polinômios nas indeterminadas $X_i$, $i \in I$. Então $D(A|P)$ é um A-módulo livre cujas bases têm a mesma cardinalidade de I.

*Demonstração:*

Seja M um A-módulo livre com "I" geradores e seja $\{\Delta X_i\}_{i \in I}$ uma base de M.

Consideremos a aplicação $d: A \longrightarrow M$ definida por: se $f = \sum_{\alpha} a_\alpha M_\alpha(X) \in A$, então $df = \sum_{i \in I} \frac{\partial f}{\partial X_i} \Delta X_i$.

Um cálculo direto nos mostra que d é uma P-derivação. Mais ainda, d é uma derivação universal sobre P; de fato, se $D: A \longrightarrow N$ é uma P-derivação de A a valores num A-módulo N, então $(\forall f\in A)(Df = f^D + \sum_i \frac{\partial f}{\partial X_i}\Delta X_i)$; como D é trivial em P, segue que $(\forall f\in A)(Df=\sum \frac{\partial f}{\partial X_i}\Delta X_i)$; ora, existe um único homomorfismo $\lambda$ de A-módulos tal que $\lambda(\Delta X_i) = DX_i$ para todo $i\in I$ e, claramente $\lambda\circ d = D$.

$$\begin{tikzcd} & N \\ A \arrow[ur, "D"] \arrow[r, "d"'] & M=\bigoplus_{i\in I} A\Delta X_i \arrow[u, "\lambda"'] \end{tikzcd}$$

Desse modo temos que $D(A|P)$ é um A-módulo livre tendo por base $\{dX_i\}_{i\in I}$ uma vez que $(\forall i\in I)(dX_i=\Delta X_i)$. □

O teorema que segue nos dá um resultado que vem facilmente da proposição acima.

*Teorema 2.2.1* - Seja P um anel. Então, $P[\{X_i\}_{i\in I}] \approx P[\{Y_j\}_{j\in J}]$ como P-álgebras se, e somente se, I e J têm a mesma cardinalidade.

*Demonstração:*

Chamemos $A=P[\{X_i\}_{i\in I}]$ e $B=P[\{Y_j\}_{j\in J}]$. Num sentido a demonstração é trivial. Suponhamos então que $A\approx B$ e tomemos $\phi: A \longrightarrow B$ um isomorfismo. Sejam d e $\partial$ derivações universais e observemos que A é um B-módulo através de $\phi$ e B é um A-módulo através de $\phi^{-1}$. Pela propriedade universal de d e $\partial$,

$$\begin{tikzcd} B \arrow[r, "\partial"] & D(B|P) \arrow[d, shift left, "\lambda'"] \\ A \arrow[u, "\phi"] \arrow[r, "d"'] & D(A|P) \arrow[u, shift left, "\lambda"] \end{tikzcd}$$

segue que existe $\lambda$ homomorfismo de A-módulos, e existe $\lambda'$ homomorfismo de B-módulos tais que $\lambda\circ d=\partial\circ\phi$ e $\lambda'\circ\partial=d\circ\phi^{-1}$; logo $(\lambda\circ\lambda')\circ\partial=\partial$ e $(\lambda'\circ\lambda)\circ d=d$; como $1_{D(B|P)}$ e $1_{D(A|P)}$ são os únicos isomorfismos tais que $1_{D(B|P)}\circ\partial=\partial$ e $1_{D(A|P)}\circ d=d$ segue que

$\lambda\circ\lambda' = 1_{D(B|P)}$ e $\lambda'\circ\lambda = 1_{D(A|P)}$ e, portanto, $D(A|P) \simeq D(B|P)$. Da proposição temos que $D(A|P)$ e $D(B|P)$ são módulos livres, $D(A|P) = \bigoplus_{i\in I} AdX_i$ e $D(B|P) = \bigoplus_{j\in J} B\partial Y_j = \bigoplus_{j\in J} A\partial Y_j$ já que $A\simeq B$; também, $D(A|P) \simeq D(B|P)$ como A-módulos; então, a cardinalidade de suas bases como A-módulos é a mesma, isto é, I e J têm a mesma cardinalidade. □

<u>*Proposição 2.2.2*</u> - Sejam P, A, R anéis, A uma P-álgebra, R uma A-álgebra (consequentemente uma P-álgebra), $d: R \longrightarrow D(R|P)$ uma derivação universal, RdA o R-submódulo de $D(R|P)$ gerado pelos elementos do tipo da com $a\in A$, e $\phi: D(R|P) \longrightarrow D(R|P)/RdA$ o homomorfismo canônico de R-módulos. Então $D(R|A)=D(R|P)/RdA$ e $\partial=\phi\circ d$ é uma derivação universal de R sobre A.

<u>*Demonstração:*</u>

$$\begin{tikzcd} & M & \\ R \arrow[ur, "\Delta"] \arrow[r, "d"'] \arrow[d, dash] & D(R|P) \arrow[u, "\lambda'"'] \arrow[r, "\phi"'] & D(R|P)/RdA \arrow[ul, "\lambda"'] \\ A \arrow[d, dash] & & \\ P & & \end{tikzcd}$$

Claramente $\partial=\phi\circ d$ é uma A-derivação de R. Mostremos que $\partial$ satisfaz a propriedade universal. Para isto, seja $\Delta$ uma A-derivação de R a valores num R-módulo M; como $\Delta$ é também uma P-derivação de R, então existe um único homomorfismo $\lambda'$ de R-módulos tal que $\lambda'\circ d = \Delta$; como $(\forall a\in A)(\lambda'(da)=(\lambda'\circ d)(a)=\Delta a = 0)$, segue que $RdA\subset Ker(\lambda')$ e, portanto, $\lambda'$ induz um homomorfismo de R-módulos $\lambda$ tal que $(\forall x\in D(R|P))(\lambda\bar{x}=\lambda' x)$, isto é, $\lambda'=\lambda\circ\phi$. $\lambda$ satisfaz as condições exigidas pois $\phi\circ\partial=\lambda\circ(\phi\circ d) = (\lambda\circ\phi)\circ d = \lambda'\circ d = \Delta$; também, sendo $\lambda_1: D(R|P)/RdA \longrightarrow M$ um homo morfismo de R-módulos tal que $\lambda_1\circ\partial=\lambda\circ\partial=\Delta$, tem-se que $(\lambda_1\circ\phi)\circ d)=$ $=(\lambda\circ\phi)\circ d$; como d é uma derivação universal então $\lambda_1\circ\phi=\lambda\circ\phi$ e, portanto, $(\forall x\in D(R|P))$ $(\lambda_1\bar{x}=(\lambda_1\circ\phi)(x)=(\lambda\circ\phi)x=\lambda\bar{x})$, isto é $\lambda_1=\lambda$.$\square$

Uma observação interessante é que dados os anéis $P\subset A\subset R$ e $d: R \longrightarrow D(R|P)$, uma derivação universal de R sobre P, não é verdade que $d|_A: A \longrightarrow AdA$ seja uma derivação universal de A sobre P, como mostra o seguinte exemplo: Sejam $P=\mathbb{Z}_p$: corpo dos inteiros módulo p (p>1 primo), $R=P[X]$ e $A=P[X^p]=R^p$. Sendo $d: R \longrightarrow D(R|P)$ uma derivação universal de R sobre P, temos que $(\forall f\in A)(df=0)$ já que dado $f\in A$, existe $g\in R$ um $f=g^p$; logo $d|_A\equiv 0$. Mas, se $\partial: A \longrightarrow D(A|P)$ é uma derivação universal de A sobre P, temos pela proposição 2.2.1 que $D(A|P)$ é um A-módulo livre de posto 1. Logo $d|_A\neq\partial$.

Um caso particular da proposição é dado quando se considera o A-módulo $(A\otimes_{\mathbb{Z}} A)/A_1$ onde $\mathbb{Z}$ é o anel dos inteiros e $A_1$ é o A-submódulo de $A\otimes_{\mathbb{Z}} A$ gerado pelos elementos do tipo $1\otimes xy - x\otimes y - y\otimes x$ para x,y em A. Pela proposição 2.1.2, $D(A)=$ $=(A\otimes_{\mathbb{Z}} A)/A_1$. A proposição acima nos diz que se P é um anel e A uma P-álgebra, então $D(A|P) = D(A)/AdP$ onde d é uma derivação universal de A.

## 2.3 - *Extensões Universais de Derivações*

Faremos agora um pequeno estudo sobre extensões universais de derivações que culminará numa nova prova da existên cia do módulo das diferenciais. Esta prova, embora bastante sofisticada tem como vantagem obter uma expressão para o módulo das diferenciais que será de grande utilidade em aplicações futuras, como veremos no próximo capítulo.

<u>*Definição 2.3.1*</u> - Sejam $A, R$ anéis, $M$ um $A$-módulo, e $\phi: A \longrightarrow R$ um homomorfismo de anéis. Uma extensão universal de $\delta$ a $R$ é uma derivação $\Delta: R \longrightarrow N$ de $R$ a valores num $R$-módulo $N$, com as propriedades:

$$\begin{tikzcd} & Q \\ R \arrow[ur, "D"] \arrow[r, "\Delta"] & N \arrow[u, "\xi"'] \\ A \arrow[u, "\phi"] \arrow[r, "\delta"] & M \arrow[u, "\lambda"'] \end{tikzcd}$$

E1: $\Delta$ é uma extensão de $\delta$, isto é, existe um homomorfismo $\lambda: M \longrightarrow N$ de $A$-módulos tal que $\lambda \circ \delta = \Delta \circ \phi$.

E2: Se $Q$ é um $R$-módulo e $D: R \longrightarrow Q$ é uma derivação de $R$ que é uma extensão de $\delta$ a $R$, então existe um único homomorfismo $\xi: N \longrightarrow Q$ de $R$-módulos tal que $\xi \circ \Delta = D$.

É conveniente observar que o $R$-módulo $N$ é também um $A$-módulo através de $\phi$, definindo-se $(\forall a \in A)(\forall n \in N)(a.n = \phi(a)n)$.

<u>*Proposição 2.3.1*</u> - Sejam $A, R$ anéis, $M$ um $A$-módulo, $\bar{N}$, $N$, $R$-módulos , $\phi: A \longrightarrow R$ homomorfismo de anéis, $\delta: A \longrightarrow M$ uma derivação de $A$. Se $\Delta: R \longrightarrow N$ e $\bar{\Delta}: R \longrightarrow \bar{N}$ são duas extensões universais de $\delta$ a $R$, então existe um isomorfismo $\xi: N \longrightarrow \bar{N}$ de $R$-módulos tal que $\bar{\Delta} = \xi \circ \Delta$. Consequentemente $N \simeq \bar{N}$.

<u>*Demonstração*</u>:

A demonstração é análoga à da proposição 2.1.1. $\square$

A proposição acima nos mostra que no caso de existir tensão de $\delta$.

Seja agora $D: S \longrightarrow Q$ uma derivação de $S$ num $S$-módulo $Q$, que seja uma extensão de $\delta$ a $S$; logo existe $\alpha$ homomorfismo de $A$-módulos tal que $\alpha o \delta = D o \theta$; portanto $\alpha o \delta = (D o \Psi) o \phi$, isto é, $D o \Psi$ é uma derivação de $R$ que estende $\delta$; como $\Delta$ é uma extensão universal de $\delta$ a $R$, segue que existe um único $\beta$, homomorfismo de $R$-módulos tal que $\beta o \Delta = D o \Psi$, isto é, $D$ é também uma extensão de $\Delta$ a $S$; mas $\bar{\Delta}$ é uma extensão universal de $\Delta$ a $S$; logo existe um único $\gamma$, homomorfismo de $S$-módulos tal que $\gamma o \bar{\Delta} = D$, e a demonstração está concluída. □

*Proposição 2.3.4* - Sejam $A, R$ anéis, $R$ uma $A$-álgebra e $\delta: A \longrightarrow (0)$ a derivação trivial. Então, $d: R \longrightarrow RdR$ é uma extensão universal de $\delta$ a $R$ se, e somente se, $d$ é uma derivação universal de $R$ sobre $A$.

*Demonstração:*

A demonstração segue imediatamente se observarmos que toda derivação de $R$ a valores num $R$-módulo, que é uma extensão da derivação trivial de $A$, é uma $A$-derivação de $R$, e reciprocamente. □

*Proposição 2.3.5* - Sejam $A$, $R$, $S$ anéis, $R$ uma $A$-álgebra, $S$ uma $R$-álgebra. Se $\Delta$ é uma extensão universal de uma derivação universal $d$ de $R$ sobre $A$, então $\Delta$ é uma derivação universal de $S$ sobre $A$.

$$\begin{array}{ccc} S & \xrightarrow{\Delta} & S\Delta S \\ | & & \\ R & \xrightarrow{d} & D(R/A) \\ | & & \\ A & \longrightarrow & (0) \end{array}$$

*Demonstração:*

O resultado segue facilmente das proposições 2.3.3 e

2.3.4. □

## *2.4 - Exemplos de Extensões Universais de Derivações*

*Proposição 2.4.1* - Sejam $A$ um anel, $\delta: A \longrightarrow A\delta A$ uma derivação de $A$ e $R = A[\{X_i\}_{i\in I}]$. Tomemos $N^* = \bigoplus_{i\in I} R\Delta X_i$ um $R$-módulo livre com base $\{\Delta X_i\}_{i\in I}$, e consideremos o $R$-módulo

$$\begin{tikzcd} R \arrow[r, "\Delta"] & N \\ A \arrow[u, "i"] \arrow[r, "\delta"] & A\delta A \end{tikzcd}$$

$N=(R \underset{A}{\otimes} A\delta A)\oplus N^*$. A aplicação $\Delta: R \longrightarrow N$ definida por, se $f = \sum_\alpha a_\alpha M_\alpha(X) \in R$, então $\Delta f = \left( \sum_\alpha (M_\alpha(X)\otimes\delta a_\alpha), \sum_i \frac{\partial f}{\partial X_i}\Delta X_i\right)$ é uma extensão universal de $\delta$ a $R$.

*Demonstração*:

(a) $\Delta$ é uma derivação de $R$:

i) Sejam $f = \sum_\alpha a_\alpha M_\alpha(X)$ e $g = \sum_\alpha b_\alpha M_\alpha(X)$, $f,g \in R$. Logo

$$\Delta(f+g) = \left(\sum_\alpha (M_\alpha(X)\otimes\delta(a_\alpha+b_\alpha)), \sum_i \frac{\partial(f+g)}{\partial X_i}\Delta X_i\right) =$$

$$= \left( \sum_\alpha (M_\alpha(X)\otimes\delta a_\alpha) + \sum_\alpha (M_\alpha(X)\otimes\delta b_\alpha), \sum_i \frac{\partial f}{\partial X_i}\Delta X_i + \right.$$

$$\left. + \sum \frac{\partial g}{\partial X_i}\Delta X_i\right) = \left(\sum_\alpha (M_\alpha(X)\otimes\delta a_\alpha), \sum_i \frac{\partial f}{\partial X_i}\Delta X_i\right) +$$

$$+ \left(\sum_\alpha (M_\alpha(X)\otimes\delta b_\alpha), \sum_i \frac{\partial g}{\partial X_i}\Delta X_i\right) = \Delta f + \Delta g.$$

ii) Sendo $f = aX_1^{a_1}\dots X_n^{a_n}$ e $g = bX_1^{b_1}\dots X_n^{b_n}$ $a,b\in A$, vem que

$$\Delta(f.g) = \Delta(abX_1^{a_1+b_1}\dots X_n^{a_n+b_n}) =$$

$$= (X_1^{a_1+b_1}\dots X_n^{a_n+b_n} \otimes \delta ab, \sum_i \frac{\partial fg}{\partial X_i}\Delta X_i) =$$

$$= (X_1^{a_1+b_1}\dots X_n^{a_n+b_n} \otimes (a\delta b+b\delta a), \sum_i f\frac{\partial g}{\partial X_i} +$$

$$+ g\frac{\partial f}{\partial X_i}) \Delta X_i) = (aX_1^{a_1}\ldots X_n^{a_n}\, X_1^{b_1}\ldots X_n^{b_n} \otimes \delta b +$$

$$+ bX_1^{b_1}\ldots X_n^{b_n}\, X_1^{a_1}\ldots X_n^{a_n} \otimes \delta a,\ f \sum_i \frac{\partial g}{\partial X_i} \Delta X_i +$$

$$+ g \sum_i \frac{\partial f}{\partial X_i} \Delta X_i) = f(X_1^{b_1}\ldots X_n^{b_n} \otimes \delta b,\ \sum_i \frac{\partial g}{\partial X_i} \Delta X_i) +$$

$$+ g(X_1^{a_1}\ldots X_n^{a_n} \otimes \delta a,\ \sum_i \frac{\partial f}{\partial X_i} \Delta X_i) = f\Delta g + g\Delta f.$$

Por linearidade segue que $(\forall f,g \in R)(\Delta(fg) = f\Delta g + g\Delta f)$.

(b) $\Delta$ é uma extensão de $\delta$ a $R$.

$$\begin{tikzcd}
R \arrow[r, "\Delta"] & N \\
A \arrow[u, "i"] \arrow[r, "\delta"] & A\delta A \arrow[u, "\lambda"']
\end{tikzcd}$$

Sendo $i: A \longrightarrow R$ a inclusão canônica, e $\lambda$ definida por $(\forall x \in A\delta A)(\lambda x = (1\otimes x, o))$, temos que $\lambda$ é um homomorfismo de $A$-módulos e que $\lambda\circ\delta = \Delta\circ i$ já que $(\forall x \in A)((\lambda\circ\delta)(x) = \lambda(\delta x) = (1\otimes \delta x\ , 0))$ e que $(\forall x \in A)((\Delta\circ i)(x) = \Delta x = (1\otimes\delta x, o))$.

(c) $\Delta$ satisfaz a propriedade universal.

$$\begin{tikzcd}
 & & Q \\
R \arrow[r, "\Delta"] \arrow[urr, "D"] & N \arrow[ur, "\xi"'] & \\
A \arrow[u, "i"] \arrow[r, "\delta"] & A\delta A \arrow[u, "\lambda"'] \arrow[uur, "\theta"'] &
\end{tikzcd}$$

Seja $D$ uma derivação de $R$ num $R$-módulo $Q$ que é uma extensão de $\delta$ a $R$; logo existe $\theta$ homomorfismo de $A$-módulos tal que $\theta\circ\delta =$ $= D\circ i$. Consideremos a aplicação $\bar{\theta}: R\times A\delta A \longrightarrow Q$ definida por $(\forall f \in R)(\forall x \in A\delta A)(\bar{\theta}(f,x) = f\theta x)$; verifica-se facilmente que $\bar{\theta}$ é $A$-bilinear; logo existe um homomorfismo de $A$-módulos $\mu: R \otimes_A A\delta A \longrightarrow Q$ tal que $(\forall f \in R)(\forall x \in A\delta A)(\mu(f\otimes x) = f\theta x)$; $\mu$ é também um homomorfismo de $R$-módulos pois $(\forall f,r \in R)(\forall x \in A\delta A)(\mu(r(f\otimes x)) = \mu(rf\otimes x) = (rf)\theta x =$ $= r(f\theta x) = r\mu(f\otimes x))$.

Por outro lado seja $\Psi: N^* = \underset{i}{\oplus} R\Delta X_i \longrightarrow Q$ o único homomorfismo de R-módulos tal que $(\forall i \in I)(\Psi(\Delta X_i) = DX_i)$. Desse modo obtemos o homomorfismo de R-módulos $\xi: N \longrightarrow Q$ definido por $(\forall f \in R)(\forall x \in A\delta A)(\forall (r_i)_{i\in I}$ família quase nula de elementos de R) $(\xi(f \otimes x, \sum_i r_i \Delta X_i) = f\theta x + \sum_i r_i DX_i)$.

$\xi$ satisfaz as condições exigidas. De fato, se

$f = \sum_\alpha a_\alpha M_\alpha(X) \in R$, temos $Df = f^D + \sum_i \frac{\partial f}{\partial X_i} \Delta X_i$; logo

$$(\xi o \Delta)(f) = \xi(\sum_\alpha (M_\alpha(X) \otimes \delta a_\alpha), \sum_i \frac{\partial f}{\partial X_i} \Delta X_i) = \sum_\alpha (M_\alpha(X) \cdot (\theta o \delta)(a_\alpha)) +$$

$$+ \sum_i \frac{\partial f}{\partial X_i} DX_i = \sum_\alpha (M_\alpha(X) Da_\alpha) + \sum \frac{\partial f}{\partial X_i} DX_i = f^D + \sum_i \frac{\partial f}{\partial X_i} DX_i = Df;$$

portanto $\xi o \Delta = D$. Mostremos agora a unicidade de $\xi$; para isto, seja $\bar{\xi}: N \longrightarrow Q$ um homomorfismo de R-módulos tal que $\bar{\xi} o \Delta = \xi o \Delta = D$; ora, se $(f \otimes x, \sum_i r_i \Delta X_i) \in N$ com $f \in R$, $x \in A\delta A$ e $(r_i)_{i\in I}$ família quase nulas de elementos de R, temos que existem $(\alpha_i)_{i\in I}$, $(\beta_i)_{i\in I}$ famílias quase nulas de elementos de A tal que $\lambda(\sum_i \beta_i \delta\alpha_i) = (f \otimes x, \sum_i r_i \Delta X_i)$; logo $\bar{\xi}(f \otimes x, \sum_i r_i \Delta X_i) =$

$$= \bar{\xi} o \lambda (\sum_i \beta_i \delta \alpha_i) = \sum_i \beta_i (\bar{\xi} o \lambda o \delta)(\alpha_i) = \sum_i \beta_i (\bar{\xi} o \Delta o i)(\alpha_i) = \sum_i \beta_i (D o i)(\alpha_i) =$$

$$= \sum_i \beta_i D\alpha_i = \sum_i \beta_i (\xi o \Delta)(\alpha_i) = \sum_i \beta_i (\xi o \Delta o i)(\alpha_i) = \sum_i \beta_i (\xi o \lambda o \delta)(\alpha_i) =$$

$$= \sum_i \beta_i (\xi o \lambda)(\delta \alpha_i) = \xi o \lambda (\sum_i \beta_i \delta \alpha_i) = \xi(f \otimes x, \sum_i r_i \Delta X_i);$$ portanto, $\bar{\xi} = \xi$.

E a proposição está provada. □

Notemos agora que das proposições 2.3.5 e 2.4.1 decorre imediatamente a proposição 2.2.1, que nos diz que $d: R = A[\{X_i\}_{i\in I}] \longrightarrow \underset{i}{\oplus} R dX_i$ definida por $(\forall f \in R)(df = \sum_i \frac{\partial f}{\partial X_i} dX_i)$ é uma derivação universal de R sobre A.

<u>*Proposição 2.4.2*</u> - Sejam A um anel, S um sistema multiplicativo de A, $D: A \longrightarrow M = ADA$ uma derivação e $\phi: A \longrightarrow A_S$ o homomorfismo canônico de anéis, isto é, $(\forall a \in A)(\phi a = \frac{a}{1})$. Então, a derivação $\Delta: A_S \longrightarrow M_S$ definida por $(\forall x \in A)(\forall s \in S)(\Delta(\frac{x}{s}) = \frac{sDx - xDs}{s^2})$ é uma extensão universal de D a $A_S$.

<u>*Demonstração:*</u>

$\Delta$ é uma extensão de D. De fato, seja $\lambda$ o homomorfismo canônico de módulos, isto é, $(\forall m \in M)(\lambda m = \frac{m}{1})$;

$$\begin{tikzcd} A_S \arrow[r, "\Delta"] & M_S \\ A \arrow[u, "\phi"] \arrow[r] & M \arrow[u, "\lambda"'] \end{tikzcd}$$

temos que $(\forall a \in A)(\lambda o D)(a) = \lambda Da = \frac{Da}{1})$ e que $(\forall a \in A)((\Delta o \phi)(a) = \Delta(\phi a) = \Delta(\frac{a}{1}) = \frac{Da}{1}$; logo $\lambda o D = \Delta o \phi$.

$\Delta$ satisfaz a propriedade universal das extensões universais. Para isto, seja $\bar{D}$ uma derivação de $A_S$ a valores num $A_S$-módulo N, $\bar{D}$ uma extensão de D a $A_S$;

$$\begin{tikzcd} & & N \\ A_S \arrow[r] \arrow[urr, "\bar{D}"] & M_S \arrow[ur, "\xi"'] & \\ A \arrow[u, "\phi"] \arrow[r, "D"] & M \arrow[u, "\lambda"'] \arrow[uur, "\theta"'] & \end{tikzcd}$$

logo, existe $\theta$ homomorfismo de A-módulos tal que $\theta o D = \bar{D} o \phi$; observemos que $(\forall a \in A)(\forall m \in M)(\theta(am) = a.\theta m = \phi(a).\theta m = \frac{a}{1}\theta m)$. Também, se $m, m' \in M$ e $s, s' \in S$ com $\frac{m}{s} = \frac{m'}{s'}$, então existe $s'' \in S$ tal que $s''(s'm - sm') = 0_M$; aplicando $\theta$ segue que $\frac{s''}{1}\theta(s'm - sm') = 0_N$; logo $0_N = \frac{s''}{1}(\frac{s'}{1}\theta m - \frac{s}{1}\theta m')$; multiplicando por $\frac{1}{ss's''}$ vem que $0_N = \frac{1}{s}\theta m - \frac{1}{s'}\theta m'$, isto é, $\frac{1}{s}\theta m = \frac{1}{s'}\theta m'$. Podemos então definir a aplicação $\xi$ por $(\forall m \in M)(\forall s \in S)(\xi(\frac{m}{s}) = \frac{1}{s}\theta m)$ e é fácil

ver que $\xi$ é um homomorfismo de $A_S$-módulos. Temos que $\xi o\Delta=\bar{D}$. De fato, observando-se que $(\forall s\in S)(\bar{D}\frac{1}{s} = -\frac{1}{s^2}D(\frac{s}{1}))$, segue que $(\forall a\in A)(\forall s\in S)$ vale $\bar{D}(\frac{a}{s})=\bar{D}(\frac{a}{1}\cdot\frac{1}{s}) = \frac{a}{1}\bar{D}(\frac{1}{s})+\frac{1}{s}\bar{D}(\frac{a}{1}) = \frac{1}{s}\bar{D}(\frac{a}{1})-(\frac{a}{1})\frac{1}{s^2}\bar{D}(\frac{1}{s}) = \frac{1}{s}(Do\phi)(a)-(\frac{x}{1})\frac{1}{s^2}(\bar{D}o\phi)(s) =$
$= \frac{1}{s}(\theta oD)(a)-\frac{a}{s^2}(\theta oD)(s) = \xi(\frac{Da}{s}-\frac{aDs}{s^2}) = \xi(\frac{sDa-aDs}{s^2}) =$
$= \xi(\Delta(\frac{a}{s})) = (\xi o\Delta)(\frac{a}{s})$.

$\xi$ é o único homomorfismo de $A_S$-módulos tal que $\bar{D} = \xi o\Delta$. De fato, seja $\bar{\xi}: M_S \longrightarrow N$ um $A_S$-homomorfismo de módulos tal que $\bar{\xi}o\Delta=\xi o\Delta=\bar{D}$, e mostremos que $\xi=\bar{\xi}$. Para isto, basta mostrarmos que $(\forall m\in M)(\bar{\xi}(\frac{m}{1}) = \xi(\frac{m}{1}))$. Seja $m\in M = ADA$; logo existem $x_1,\dots,x_t$, $y_1,y_2,\dots,y_t\in A$ tais que $m = \sum_{i=1}^{t} x_iDy_i$; então

$$\bar{\xi}(\frac{m}{1}) = (\bar{\xi}o\lambda)(m) = \sum_{i=1}^{t} x_i(\bar{\xi}o\lambda)(Dy_i) = \sum_{i=1}^{t} x_i(\bar{\xi}o\lambda oD)(y_i) =$$
$$= \sum_{i=1}^{t} x_i(\bar{\xi}o\Delta o\phi)(y_i) = \sum_{i=1}^{t} x_i(\bar{\xi}o\Delta)(\frac{y_i}{1}) = \sum_{i=1}^{t} x_i\bar{D}(\frac{y_i}{1}) =$$
$$= \sum_{i=1}^{t} x_i(\bar{D}o\phi)(y_i) = \sum_{i=1}^{t} x_i(\theta oD)(y_i) = \sum_{i=1}^{t} x_i\theta(Dy_i) = \theta(\sum_{i=1}^{t} x_iDy_i) =$$

$= \theta(m) = \xi(\frac{m}{1})$; logo $\xi = \bar{\xi}$ e a proposição está provada. □

*Corolário 2.4.2* - Sejam $A,P$ anéis, $A$ uma $P$-álgebra e $S$ um sistema multiplicativo de $A$. Então $\{D(A|P)\}_S$ é um módulo das diferenciais de $A_S$ sobre $P$. Precisamente, $D(A_S|P) \simeq \{D(A|P)\}_S$.

*Demonstração:*

$$\begin{array}{ccc} A_S & \xrightarrow{\Delta} & \{D(A|P)\}_S \\ \phi\uparrow & & \\ A & \xrightarrow{d} & D(A|P) \\ \uparrow & & \\ P & \longrightarrow & (0) \end{array}$$

Sendo $d$ uma derivação universal de $A$ sobre $P$, $\Delta$ uma extensão universal de $d$ a $A_S$, e $\phi$ o homomorfismo canônico de anéis, o resultado segue imediatamente através da proposição 2.3.5. □

## 2.5 - *Uma nova "expressão" para os módulos das diferenciais*

*Lema 2.5.1* - Sejam A,R,S anéis, $A \subset R$, $A \subset S$, $\phi$ um homomorfismo

$$\begin{array}{ccc} S & \xrightarrow{\bar{\Delta}} & \bar{N} \\ \phi \uparrow & & \\ R & \xrightarrow{\Delta} & N \\ i \uparrow & & \\ A & \xrightarrow{\delta} & M \end{array}$$

sobrejetor de anéis tal que $\phi|_A = 1_A$, e $\delta$ uma derivação de A a valores num A-módulo M. Assumamos que $\Delta: R \longrightarrow N = R\Delta R$ seja uma extensão universal de $\delta$ a R. Sendo $\eta=\mathrm{Ker}(\phi)$ e $\bar{N}=N/R\Delta\eta$, então,

a) $\bar{N}$ é um S-módulo;

b) A aplicação $\bar{\Delta}: S \longrightarrow \bar{N}$ definida por: (se $s \in S$ e $\phi(r)=s$ para $r \in R$, então $\bar{\Delta}s = \bar{\Delta}(\phi(r)) = \overline{\Delta r}$ = classe resídua de $\Delta r$ módulo $R\Delta\eta$) é uma extensão universal de $\delta$ a S.

*Demonstração*:

Observemos primeiramente que $\bar{\Delta}$ está bem definida pois se $r, r_1 \in R$ são tais que $\phi(r) = \phi(r_1)$, então $r-r_1 \in \eta$ e, portanto, $\Delta(r-r_1) \in R\Delta\eta$, isto é, $\overline{\Delta r} = \overline{\Delta r_1}$.

a) Sejam $r, r_1 \in R$ e $x, x_1 \in N$ tais que $\phi(r) = \phi(r_1)$ e $\bar{x} = \bar{x_1}$; temos então que $r-r_1 \in \eta$ e $x-x_1 \in R\Delta\eta$. De $x-x_1 \in R\Delta\eta$ segue que existem $y_1,\ldots,y_n \in \eta$ e $\alpha_1,\ldots,\alpha_n \in R$ tais que $x-x_1 = \sum_{i=1}^{n} \alpha_i \Delta y_i$; logo $rx-r_1x_1 = r(x-x_1)+(r-r_1)x_1 = r\sum_{i=1}^{n} \alpha_i \Delta y_i + (r-r_1)x_1$. Sendo $x_1 = \sum_{i=1}^{n} \beta_i \Delta z_i \in N$ onde $(\forall i=1,\ldots,n)(\beta_i, z_i \in R)$, $(r-r_1)x_1 = (r-r_1)\sum_{i=1}^{n} \beta_i \Delta z_i = \sum_{i=1}^{n} \Delta[(r-r_1)\beta_i z_i] - \sum_{i=1}^{n} z_i \Delta[(r-r_1)\beta_i]$ já que $\Delta$ é uma derivação de R. Portanto $rx-r_1x_1 = r\sum_{i=1}^{n} \alpha_i \Delta y_i +$

. $+ \sum_{i=1}^{n} \Delta[(r-r_1)\beta_i z_i] - \sum_{i=1}^{n} z_i \Delta[(r-r_1)\beta_i]$, de onde vem que

$rx - r_1 x_1 \in R\Delta\eta$, isto é, $\overline{rx} = \overline{r_1 x_1}$.

Com isto tudo, mostramos que tem sentido se definir uma operação.,de $S\times\bar{N}$ em $\bar{N}$ por: (se $n\in N$ e $s\in S$, sendo $r\in R$ tal que $\phi(r) = s$, então $s.\bar{n} = \overline{rn}$). Vem agora facilmente que com esta operação, $\bar{N}$ é um S-módulo.

b) Indicaremos por $i: A \longrightarrow R$ a inclusão canônica, e por $q: N \longrightarrow \bar{N}$ o homomorfismo canônico.

i) $\bar{\Delta}$ é uma derivação de S pois:

$(\forall x,y\in R)\ \bar{\Delta}(\phi(x)+\phi(y)) = \bar{\Delta}(\phi(x+y)) = \overline{\Delta(x+y)} = \overline{\Delta x} + \overline{\Delta y} =$
$= \bar{\Delta}(\phi(x)) + \bar{\Delta}(\phi(y))$, e

$(\forall x,y\in R)\ \bar{\Delta}(\phi(x)\phi(y)) = \bar{\Delta}(\phi(xy)) = \overline{\Delta xy} = \overline{x\Delta y + y\Delta x} =$
$= \overline{x\Delta y} + \overline{y\Delta x} = \phi(x)\overline{\Delta y} + \phi(y)\overline{\Delta x} = \phi(x)\bar{\Delta}(\phi(y)) + \phi(y)\bar{\Delta}(\phi(x))$.

ii) $\bar{\Delta}$ é uma extensão de $\delta$ a S.

$$\begin{tikzcd}
S \arrow[r, "\bar{\Delta}"] & \bar{N} \\
R \arrow[u, "\phi"] \arrow[r, "\Delta"] & N \arrow[u, "q"'] \\
A \arrow[u, "i"] \arrow[r, "\delta"] & M \arrow[u, "\lambda"']
\end{tikzcd}$$

Como $\Delta$ é uma extensão de $\delta$ a R, vem que existe $\lambda$ homomorfismo de A-módulos tal que $\lambda o\delta = \Delta oi$. Definimos $\bar{\lambda}: M \longrightarrow \bar{N}$ por $(\forall m\in M)$ $(\bar{\lambda}m = \overline{\lambda m})$, isto é, $\bar{\lambda} = qo\lambda$; evidentemente $\bar{\lambda}$ é um homomorfismo de A-módulos. Também, $(\forall a\in A)$ vale $(\bar{\lambda}o\delta)(a) = \bar{\lambda}(\delta a) = \overline{\lambda(\delta a)} = \overline{(\lambda o\delta)(a)} = \overline{(\Delta oi)(a)} = \overline{\Delta a} = \bar{\Delta}(\phi(a)) = (\bar{\Delta}o(\phi oi))(a)$, isto é, $\bar{\lambda}o\delta = \bar{\Delta}o(\phi oi)$ e, portanto $\bar{\Delta}$ é uma extensão de $\delta$ a S.

iii) $\bar{\Delta}$ satisfaz a propriedade universal das extensões universais.

$$\begin{tikzcd}
& & Q \\
S \arrow[urr, "D"] \arrow[r, "\bar{\Delta}"] & \bar{N} \arrow[ur, "\bar{\xi}"] & \\
R \arrow[u, "\phi"] \arrow[r, "\Delta"] & N \arrow[u, "q"] \arrow[uur, "\xi"'] & \\
A \arrow[u, "i"] \arrow[r, "\delta"] & M \arrow[uuur, "\gamma"'] &
\end{tikzcd}$$

Seja D uma derivação de S a valores em um S-módulo Q que é uma extensão de $\delta$ a S; logo, existe $\gamma$ um homomorfismo de A-módulos tal que $\gamma o \delta = Do(\phi o i)$. Daqui vem imediatamente que a derivação $Do\phi$ é uma extensão de $\delta$ a R. Como $\Delta$ é uma extensão universal de $\delta$ a R, seja $\xi$ o único homomorfismo de R-módulos tal que $\xi o \Delta = Do\phi$. Seja $x \in R\Delta\eta$, isto é, $x = \sum_{i=1}^{n} r_i \Delta x_i$ onde $(\forall i=1,\dots,n)(r_i \in R)(x_i \in N)$; temos então que $\xi(x) = \sum_{i=1}^{n} r_i(\xi o \Delta)(x_i) = \sum_{i=1}^{n} r_i(Do\phi)(x_i) = \sum_{i=1}^{n} r_i D(\phi(x_i))=0$; logo $R\Delta\eta \subset Ker(\xi)$ e, portanto, podemos definir a aplicação $\bar{\xi}: \bar{N} \longrightarrow Q$ por $(\forall n \in N)(\bar{\xi}\bar{n} = \xi n)$, isto é, $\bar{\xi} o q = \xi$. Já que $(\forall r \in R)(\bar{\xi}(\phi(r).\bar{n}) = \bar{\xi}(\overline{rn}) = \xi(rn) = r\xi n = r.\bar{\xi}\bar{n} = \phi(r)\bar{\xi}(\bar{n})$, segue facilmente que $\bar{\xi}$ é um homomorfismo de S-módulos.

$\bar{\xi} o \bar{\Delta} = D$ pois $(\forall r \in R)(D(\phi(r)) = (Do\phi)(r) = (\xi o \Delta)(r) = \xi(\Delta r) = \bar{\xi}(\overline{\Delta r}) = \bar{\xi}(\bar{\Delta}(\phi(r)) = (\bar{\xi} o \bar{\Delta})(\phi(r)))$.

$\bar{\xi}$ é o único homomorfismo de S-módulos tal que $\bar{\xi} o \bar{\Delta} = D$. De fato, seja $\mu: \bar{N} \longrightarrow Q$ um homomorfismo de S-módulos tal que $\mu o \bar{\Delta} = \bar{\xi} o \bar{\Delta} = D$; logo $\mu o \bar{\Delta} o \phi = \bar{\xi} o \bar{\Delta} o \phi = Do\phi$; como $\bar{\Delta} o \phi = q o \Delta$, vem que $(\mu o q) o \Delta = (\bar{\xi} o q) o \Delta = Do\phi$; mas $Do\phi$ é uma extensão de $\delta$ a R, e $\Delta$ é uma extensão universal de $\delta$ a R; logo, $\mu o q = \bar{\xi} o q$ e, portanto, $\mu = \bar{\xi}$. □

*Proposição 2.5.1* - Sejam A, R anéis, $A \subset R$ e $\delta: A \longrightarrow M = A\delta A$ uma derivação de A. Então, existe uma extensão universal de $\delta$ a R.

*Demonstração:*

$$\begin{tikzcd}
R \arrow[r, "\bar{\Delta}"] & R\bar{\Delta}R \\
S \arrow[u, "\phi"] \arrow[r, "\Delta"] & S\Delta S \\
A \arrow[u, "i"] \arrow[r, "\delta"] & M
\end{tikzcd}$$

Seja $\{x_i\}_{i\in I}$ um conjunto de geradores para R sobre A, isto é, $R=A[\{x_i\}_{i\in I}]$. Sendo $S=A[\{X_i\}_{i\in I}]$, consideremos $\phi:S \longrightarrow R$ o único homomorfismo de A-módulos tal que $(\forall i\in I)(\phi(X_i)=x_i)$. Pela proposição 2.4.1 sabemos que a derivação $\Delta: S \longrightarrow ((S\otimes_A\delta A)\oplus(\bigoplus_{i\in I} R\Delta X_i))$ definida por: (se $f = \sum_\alpha a_\alpha M_\alpha(X)\in S$ então $\Delta f=(\sum_\alpha (M_\alpha(X)\otimes\delta a_\alpha), \sum_i \frac{\partial f}{\partial X_i}\Delta X_i))$ é uma extensão universal de $\delta$ a S; lembremos que $\bigoplus_{i\in I} R\Delta X_i$ indica um R-módulo livre com base $\{\Delta X_i\}_{i\in I}$.

Seja agora $\eta=\mathrm{Ker}\phi$ e $N=((S\otimes_A\delta A)\oplus(\bigoplus_{i\in I} RX_i))\ /\ S\Delta\eta$ e indiquemos por $f(x)=\sum_\alpha a_\alpha M_\alpha(x)\in R$ se $f=\sum_\alpha a_\alpha M_\alpha(X)\in S$. Pelo lema, segue que N é um R-módulo e que $\bar{\Delta}: R \longrightarrow N$ definida por $(\forall f(x)\in R)$ $(\bar{\Delta}(f(x)) = \overline{\Delta f}$ = classe resídua de $f\in S$ módulo $S\Delta\eta)$ é uma extensão universal de $\delta$ a R. □

*Lema 2.5.2* - Sejam $D:A \longrightarrow M$ uma derivação, $\eta$ um ideal de A, e $\{f_\lambda\}_{\lambda\in\Lambda}$ um sistema de geradores de $\eta$. Então $AD\eta=\eta DA + \sum_\lambda ADf_\lambda$.

*Demonstração:*

Sejam $f\in\eta$ e $(a_\lambda)_{\lambda\in\Lambda}$ uma família quase nula de elementos de A tal que $f = \sum_\lambda a_\lambda f_\lambda$. Como $Df = \sum_\lambda a_\lambda Df_\lambda + \sum_\lambda f_\lambda Da_\lambda$, então $Df \in (\eta DA + \sum_\lambda ADf_\lambda)$; portanto $D\eta \subset (\eta DA + \sum_\lambda ADf_\lambda)$ e, logo $AD\eta \subset (\eta DA + \sum_\lambda ADf_\lambda)$.

Por outro lado, é claro que $\sum_\lambda ADf_\lambda \subset AD\eta$; também,

$(\forall a\in A)(\forall\lambda)(f_\lambda Da = D(f_\lambda a) - aDf_\lambda)\in AD\eta$ e, portanto, $(\forall a\in A)fDa =$ $= \sum_\lambda a_\lambda(f_\lambda Da)\in\eta DA$, isto é, $\eta DA\subset AD\eta$; logo $(\eta DA + \sum_\lambda ADf_\lambda)\subset AD\eta$. E o lema está provado. □

*Teorema 2.5.1* - Sejam $A,R$ anéis com $R=A[\{x_i\}_{i\in I}]$, $S=A[\{X_i\}_{i\in I}]$, $\phi: S\longrightarrow R$ o homomorfismo de A-álgebras tal que $(\forall i\in I)(\phi(X_i) = x_i)$, $\eta=\operatorname{Ker}(\phi)$, $\{f_\lambda\}_{\lambda\in\Lambda}$ um sistema de geradores de $\eta$, $\bigoplus_{i\in I} R\Delta X_i$ um R-módulo livre com base $\{\Delta X_i\}_{i\in I}$ e $\Delta: S\longrightarrow\bigoplus_{i\in I} R\Delta X_i$ a derivação de S definida por $(\forall f\in S)(\Delta f = \sum_{i\in I}\frac{\partial f}{\partial x_i}\Delta X_i)$. Então vale

$$D(R/A) = (\bigoplus_{i\in I} R\Delta X_i)/\sum_\lambda R\Delta f_\lambda$$

*Demonstração:*

$$\begin{tikzcd}
R \arrow[r, "\partial"] & (\bigoplus_i S\bar{\Delta}X_i)/S\bar{\Delta}\eta \\
S \arrow[u, "\phi"] \arrow[r, "\bar{\Delta}"] & \bigoplus_i S\bar{\Delta}X_i \\
A \arrow[u, "i"] \arrow[r, "\delta"] & (0)
\end{tikzcd}$$

Pela proposição anterior sabemos que $\partial$ definida por $(\forall f(x)\in R)(\partial(f(x)) = \overline{\bar{\Delta}f}$ = classe residua de $\bar{\Delta}f$ módulo $S\bar{\Delta}\eta)$ é uma extensão universal de $\delta$ a R; aqui $\bigoplus_{i\in I} S\bar{\Delta}X_i$ é um S-módulo livre com base $\{\bar{\Delta}X_i\}_{i\in I}$, e $\bar{\Delta}$ definida por $(\forall f\in S)(\bar{\Delta}f = \sum_i\frac{\partial f}{\partial X_i}\bar{\Delta}X_i)$ é uma extensão universal de $\delta$ a S. Como $\delta$ é a derivação trivial de A, segue da proposição 2.3.5 que $\partial$ é uma derivação universal de R sobre A.

Seja $\theta$ o homomorfismo sobrejetor de S-módulos tal que $(\forall i\in I)(\theta(\bar{\Delta}X_i) = \Delta X_i)$, isto é, se $(s_i)_{i\in I}$ é uma família quase nula de elementos de S, então, $\theta(\sum_i s_i\bar{\Delta}X_i) = \sum_i s_i\cdot\Delta X_i = \sum_i\phi(s_i)\Delta X_i$ ; logo

$$\begin{tikzcd}
S \arrow[r, "\Delta"] \arrow[dr, "\bar{\Delta}"'] & \bigoplus_{i\in I} R\bar{\Delta}X_i \\
& \bigoplus S\bar{\Delta}X_i \arrow[u, "\theta"']
\end{tikzcd}$$

$\theta o\bar{\Delta} = \Delta$.

Temos que:

(i) $Ker(\theta) = \eta\bar{\Delta}S$.

Observemos que $\eta\bar{\Delta}S=\{\sum_i \alpha_i\bar{\Delta}X_i : (\alpha_i)_{i\in I}$ é uma família quase nula de $\eta\}$, já que $\eta$ é um ideal de $S$. Se $x = \sum_i s_i\bar{\Delta}X_i \in Ker(\theta)$, então $\sum_i \phi(s_i)\Delta X_i = 0$; logo $(\forall i\in I)$ $\phi(s_i)=0$, isto é, $(\forall i\in I)$ $(s_i \in Ker(\phi)=\eta)$ e, portanto, $x\in\eta\bar{\Delta}S$. Mostramos com isso que $Ker(\theta) \subset \eta\bar{\Delta}S$. É claro que vale $\eta\bar{\Delta}S \subset Ker(\theta)$. Logo $\eta\bar{\Delta}S = Ker(\theta)$.

(ii) $\eta\bar{\Delta}S \subset S\bar{\Delta}\eta$

Esta inclusão vem imediatamente do lema 2.5.2 já que $\eta$ é um ideal de $S$, $\bar{\Delta}$ é uma derivação de $S$ e, portanto $S\bar{\Delta}\eta=\eta\bar{\Delta}S+\sum_\lambda S\bar{\Delta}f_\lambda$.

(iii) $\theta(S\bar{\Delta}\eta) = \sum_\lambda R\Delta f_\lambda$

Seja $x\in S\bar{\Delta}\eta$; como $S\bar{\Delta}\eta=\eta\bar{\Delta}S + \sum_\lambda S\bar{\Delta}f_\lambda$, vem que $x = x_1 + x_2$ com $x_1\in Ker(\theta) = \eta\bar{\Delta}S$ e $x_2 = \sum_\lambda \alpha_\lambda\bar{\Delta}f_\lambda$ onde $(\alpha_\lambda)_{\lambda\in\Lambda}$ é uma família quase nula de elementos de $S$. Então

$$\theta(x) = \theta(\sum_\lambda \alpha_\lambda\bar{\Delta}f_\lambda) = \sum_\lambda \phi(\alpha_\lambda)\theta(\bar{\Delta}f_\lambda) = \sum_\lambda \phi(\alpha_\lambda)\theta(\sum \frac{\partial f_\lambda}{\partial X_i}\bar{\Delta}X_i) =$$
$$= \sum_\lambda [\phi(\alpha_\lambda)(\sum_i \frac{\partial f_\lambda}{\partial x_i}\Delta X_i)] = \sum_\lambda \phi(\alpha_\lambda)\Delta f_\lambda.$$ Logo, se $x\in S\bar{\Delta}\eta$, $\theta(x)\in\sum_\lambda R\Delta f_\lambda$, isto é, $\theta(S\bar{\Delta}\eta) \subset \sum_\lambda R\Delta f_\lambda$.

Por outro lado, se $y = \sum_\lambda r_\lambda\Delta f_\lambda \in \sum_\lambda R\Delta f_\lambda$, onde $(r_\lambda)_{\lambda\in\Lambda}$ é uma família quase nula de elementos de $R$, sendo $(s_\lambda)_{\lambda\in\Lambda}$ em $S$

tal que $\phi(s_\lambda) = r_\lambda$ para todo $\lambda$, e $s_\lambda = 0$ se $r_\lambda = 0$, então, se $x = \sum_\lambda s_\lambda \bar{\Delta} f_\lambda$, vem que $\theta x = y$. Como $x \in \sum_\lambda S\bar{\Delta} f_\lambda \subset S\bar{\Delta}\eta$ segue que $\sum_\lambda R\Delta f_\lambda \subset \theta(S\bar{\Delta}\eta)$ e o resultado está provado.

Desse modo, podemos definir $\bar{\theta} : (\bigoplus_{i\in I} S\bar{\Delta}X_i)/S\bar{\Delta}\eta \longrightarrow (\bigoplus_{i\in I} R\Delta X_i)/\sum_\lambda R\Delta f_\lambda$ por $(\forall x \in \bigoplus_i S\Delta X_i)(\bar{\theta}\bar{x}) = \overline{\overline{\theta x}}$ = classe de $x$ módulo $\sum_\lambda R\Delta f_\lambda$). Vem facilmente que $\bar{\theta}$ é um isomorfismo de S-módulos. Observando-se que, pelo lema 2.5.1, $\bigoplus_{i\in I} S\bar{\Delta}X_i/S\bar{\Delta}\eta$ é um R-módulo, onde, se $r\in R$ e $s\in S$ é tal que $\phi(s)=r$, então $(\forall x \in \bigoplus_{i\in I} S\bar{\Delta}X_i)$ $(r\cdot\bar{x} = \overline{sx})$, segue que $(\forall x \in \bigoplus_{i\in I} S\bar{\Delta}X_i)(\bar{\theta}(r\cdot\bar{x}) = \bar{\theta}(\overline{sx}) = \bar{\theta}(s\bar{x}) =$ $= s.\bar{\theta}(\bar{x}) = \phi(s)\bar{\theta}(\bar{x}) = r(\bar{\theta}(\bar{x}))$, isto é, $\bar{\theta}$ é um isomorfismo de R-módulos.

Finalmente, sendo $d: R \longrightarrow (\bigoplus_{i\in I} R\Delta X_i)/\sum_\lambda R\Delta f_\lambda$ a derivação definida por $(\forall f\in S)(d(f(x)) = \overline{\overline{\Delta f}}$ = classe resídua de $f$ módulo $\sum_\lambda R\Delta f_\lambda$), temos que $\bar{\theta}\circ\partial = d$, já que $(\forall f\in S)(\bar{\theta}\circ\partial)(f(x)) = \bar{\theta}(\overline{\bar{\Delta}f}) =$ $= \overline{\overline{\theta(\bar{\Delta}f)}} = \overline{\overline{(\theta\circ\bar{\Delta})(f)}} = \overline{\overline{\Delta f}} = d(f(x))$. Como $\partial$ é uma derivação universal de R sobre A, então vem imediatamente que d também é uma derivação universal de R sobre A e, portanto $D(R/A) = (\bigoplus_{i\in I} R\Delta X_i)/\sum_\lambda R\Delta f_\lambda$. □

$$\begin{tikzcd}
 & (\bigoplus_i R\Delta X_i)/\sum_\lambda R\Delta f_\lambda \\
R \arrow[ur, "d"] \arrow[r, "\partial"] & (\bigoplus_i S\bar{\Delta}X_i)/S\bar{\Delta}\eta \arrow[u, "\bar{\theta}"'] \\
S \arrow[u, "\phi"] \arrow[r, "\bar{\Delta}"] \arrow[dr, "\Delta"'] & \bigoplus_i S\bar{\Delta}X_i \arrow[d, "\theta"] \\
 & \bigoplus_i R\Delta X_i
\end{tikzcd}$$

*Corolário 2.5.1* - Sejam A, R anéis com $R = A[\{x_i\}_{i\in I}]$, $T = A[\{X_i\}_{i\in I}]$, $\phi$ o homomorfismo de A-álgebras tal que $(\forall i\in I)(\phi(X_i) = x_i)$,

$$\begin{tikzcd} R_S \arrow[r, "d"] & D(R_S|A) \\ R \arrow[u] \arrow[r] & (\bigoplus_i R\Delta X_i)/\sum_\lambda R\Delta f_\lambda = N \\ T \arrow[u, "\phi"] \arrow[r, "\Delta"] & \bigoplus_{i\in I} R\Delta X_i \\ A \arrow[u, "i"] \arrow[r] & (0) \end{tikzcd}$$

$\{f_\lambda\}_{\lambda\in\Lambda}$ um sistema de geradores de $\eta = \mathrm{Ker}(\phi)$, S um sistema multiplicativo de R e $\bigoplus_{i\in I} R\Delta X_i$ um R-módulo livre com base $\{\Delta X_i\}_{i\in I}$. Então

$$D(R_S|A) = (\bigoplus_{i\in I} R_S\Delta X_i)/\sum_\lambda R_S\Delta f_\lambda$$

onde, $\bigoplus_{i\in I} R_S\Delta X_i$ significa

$$\bigoplus_{i\in I} R_S(1\underset{R}{\otimes}\Delta X_i) = R_S\underset{R}{\otimes}(\bigoplus_i R\Delta X_i),$$

$\sum_\lambda R_S\Delta f_\lambda$ significa $\sum_\lambda R_S(1\otimes\Delta f_\lambda) = R_S\underset{R}{\otimes}\sum_\lambda R\Delta f_\lambda$, e $\Delta$ é a derivação de T definida por $(\forall f\in T)$ $(\Delta f = \sum_\lambda \frac{\partial f}{\partial X_i}\Delta X_i)$.

*Demonstração*:

Pelo teorema sabemos que $\partial: R \longrightarrow N$ definida por $(\forall f\in T)(\partial(f(x)) = \overline{\Delta f}$ = classe residua de $\Delta f$ módulo $\sum_\lambda R\Delta f_\lambda)$ é uma derivação universal de R sobre A.

Das proposições 2.4.2 e 2.3.5 temos que $D: R_S \longrightarrow N_S$ definida por $(\forall f,g\in T$ com $f(x)\in R$ e $g(x)\in S)(D(\frac{f(x)}{g(x)}) = \frac{g(x)\overline{\Delta f} - f(x)\overline{\Delta g}}{g(x)^2}$ é uma derivação universal de $R_S$ sobre A.

Como $R_S\underset{R}{\otimes} N \simeq N_S$ através do isomorfismo $\theta: N_S \longrightarrow R_S\underset{R}{\otimes}N$ tal que $(\forall n\in N)(\forall s\in S)(\theta(\frac{n}{s}) = \frac{1}{s}\otimes n)$, segue imediatamente que a derivação $\bar{D}: R_S \longrightarrow R_S\underset{R}{\otimes} N$ definida por $\theta\circ D = \bar{D}$, isto é, tal que $(\forall f,g\in T$ com $f(x)\in R$ e $g(x)\in S)\ (\bar{D}(\frac{f(x)}{g(x)})=\frac{1}{g(x)^2}\otimes\left[g(x)\overline{\Delta f}-f(x)\overline{\Delta g}\right])$ é também uma derivação universal de $R_S$ sobre A.

Considerando-se a sequência exata

$$(0)\longrightarrow \sum_\lambda R\Delta f_\lambda \xrightarrow{i} \bigoplus_{i\in I} R\Delta X_i \xrightarrow{q} (\bigoplus_i R\Delta X_i)/\sum_\lambda R\Delta f_\lambda \longrightarrow (0)$$

onde i é a inclusão canônica e q o homomorfismo canônico, segue que também é exata a sequência

$$R_S \otimes_R \sum_\lambda R\Delta f_\lambda \xrightarrow{1\otimes i} R_S \otimes_R (\bigoplus_{i\in I} R\Delta X_i) \xrightarrow{1\otimes q} R_S \otimes_R N \longrightarrow (0)$$

e portanto,

$$D(R_S/A) = R_S \otimes_R N \approx (R_S \otimes_R (\bigoplus_{i\in I} R\Delta X_i))/(R_S \otimes_R \sum_\lambda R\Delta f_\lambda)$$

através do isomorfismo $\bar{\theta}$ definido por $(\forall r\in R)(\forall s\in S)(\forall (r_i)_{i\in I}$ família quase nula de elementos $R)(\bar{\theta}(\frac{r}{s}\otimes \overline{\sum_{i\in I} r_i\Delta X_i}) = \overline{\frac{r}{s}\otimes \sum_i r_i\Delta X_i}$.

Logo, o corolário está provado; mais ainda, uma derivação universal de $R_s$ sobre A é dada por

$$d: R_s \longrightarrow (\bigoplus_{i\in I} R_s\Delta X_i)/\sum_\lambda R_s\Delta f_\lambda ,$$

definida por $d = \bar{\theta}o\bar{D}$. Com a identificação de $1\otimes\Delta X_i$ com $\Delta X_i$, $i\in I$, temos que $(\forall f(x)\in R)(\forall g(x)\in S)\ (d(\frac{f(x)}{g(x)}) = \frac{\overline{g(x)\Delta f-f(x)\Delta g}}{(g(x))^2}$. □

Um caso particular deste corolário é dado quando R é um anel de integridade e K seu corpo de frações. Neste caso $S = R-\{0\}$ e $D(K|A) = (\bigoplus_i K\Delta X_i)/\sum_\lambda K\Delta f_\lambda$; também, uma derivação universal $d: K \longrightarrow D(K|A)$ é dada por

$$(\forall f,g\in T \text{ com } f(x),g(x)\in R \text{ e } g(x)\neq 0)\ (d(\frac{f(x)}{g(x)}) = \frac{g(x)\Delta f - f(x)\Delta g}{(g(x))^2}$$

Assumamos que $K/k$ seja uma extensão de corpos, $k$ com característica $p\neq 0$, e recordemos a noção de p-base de $K/k$. Diz-se que $X\subset K$ é um conjunto p-independente de $K$ sobre $k$, se todo subconjunto finito $\{x_1,\ldots,x_n\}\subset X$ é p-independente sobre $k$, isto é, os $p^n$ monômios $x_1^{i_n}\cdot\ldots\cdot x_n^{i_n}$ $(0 \leq i_q < p,\ q=1,\ldots,n)$ são linearmente independentes sobre $k(K^p)$; ainda mais, $X\subset K$ é p-independente de $K$ sobre $k$ se, e somente se para todo $X' \subsetneqq X$, $k(K^p)(X') \subsetneqq k(K^p)(X)$. Diz-se que $X$ é uma p-base de $K$ sobre $k$, se $X$ é p-independente sobre $k$ e $K = k(K^p)(X)$.

<u>*Corolário 2.5.2*</u> - Seja $K/k$ uma extensão de corpos, $k$ com característica $p\neq 0$. Sendo $\{x_i\}_{i\in I}$ uma p-base de $K$ sobre $k$, e $d$ uma derivação universal de $K$ sobre $k$, então $D(K/k)$ é um $K$-espaço vetorial com base $\{dx_i\}_{i\in I}$.

<u>*Demonstração*</u>:

Temos que $D(K/k) \simeq D(K/k(K^p))$ pois $d(k(K^p)) = (0)$ e, pela proposição 2.2.2, $D(K/k(K^p)) = D(K/k)/Kd(k(K^p))$. Chamemos $S = k(K^p)[\{X_i\}_{i\in I}]$ um anel de polinômios nas indeterminadas $\{X_i\}_{i\in I}$ e observemos que $K = k(K^p)[\{x_i\}_{i\in I}] = k(K^p)(\{x_i\}_{i\in I})$ já que $\{x_i\}_{i\in I}$ é uma p-base de $K$ sobre $k$ e que para todo $i\in I, x_i$ é algébrico sobre $k(K^p)$.

Pelo teorema 2.5.1, temos que $D(K/k(K^p)) = (\bigoplus_{i\in I} K\Delta X_i)/\sum_{\lambda} K\Delta f_{\lambda}$

onde $\bigoplus_{i\in I} K\Delta X_i$ indica um K-espaço vetorial com base $\{\Delta X_i\}_{i\in I}$, $\Delta: S \longrightarrow \bigoplus_{i\in I} K\Delta X_i$ é a derivação de S definida por:

$$(\forall f\in S)(\Delta f = \sum_i \frac{\partial f}{\partial x_i}\Delta X_i)), \quad \text{e} \quad \{f_\lambda\}_{\lambda\in\Lambda} \quad \text{é}$$

um sistema de geradores de $\mathrm{Ker}(\phi)$ onde $\phi: S \longrightarrow K$ é o homomorfismo de $k(K^p)$-álgebras tal que $(\forall i\in I)(\phi(X_i)=x_i)$. Ora, é fácil ver que $\mathrm{Ker}\,\phi$ é gerado por $\{f_i\}_{i\in I}$ onde $f_i=X_i^p-x_i^p\in S$. Mas temos que

$$\Delta f_i = \sum_{j\in I} \frac{\partial f_i}{\partial x_j}\Delta X_j = \frac{\partial(X_i^p-x_i^p)}{\partial x_i}\Delta X_i = 0$$

Logo, temos que $D(K/k(K^p)) \approx \bigoplus_{i\in I} K\Delta X_i$ e, portanto, $D(K/k)$ é um K-espaço vetorial com base de cardinalidade igual à cardinalidade de I. Como $\{dx_i\}_{i\in I}$ gera $D(K/k)$ como K-espaço vetorial, segue que $\{dx_i\}_{i\in I}$ constitui uma base de $D(K/k)$. $\square$

## CAPÍTULO III

## APLICAÇÕES DOS MÓDULOS DAS DIFERENCIAIS A EXTENSÕES DE CORPOS DO TIPO FINITO

### 3.1 - *Inseparabilidade de uma Extensão de Corpos do Tipo Finito*

Sendo k um corpo e $f: V \longrightarrow W$ um homomorfismo de k-espaços vetoriais, indicaremos por $N_f$ e $C_f$ o núcleo e o conúcleo de f, respectivamente. Se $N_f$ e $C_f$ tiverem dimensão finita sobre k, escreveremos $\delta(f) = [C_f:k] - [N_f:k]$.

*Lema 3.1.1* - Sejam k um corpo, $f: V \longrightarrow W$, $g: W \longrightarrow T$ homomorfismos de k-espaços vetoriais tais que $N_f$, $N_g$, $C_f$ e $C_g$ tenham dimensão finita. Se $h = gof$ então $N_h$ e $C_h$ são k-espaços vetoriais de dimensão finita e $\delta(h) = \delta(g) + \delta(f)$.

*Demonstração:*

É fácil ver que $N_f \subset N_h$ e que $f(N_h) \subset f(V)$. Seja $\pi: N_g \longrightarrow C_f$ o homomorfismo de k-espaços vetoriais definido por $(\forall n \in N_g)(\pi(n) = n + f(V))$; então $Ker(\pi) = f(V) \cap N_g$ e $\pi(N_g) = N_g/f(V)$.

Sendo $w,w'\in W$ com $(w-w')\in f(V)$, vem imediatamente que $(gw-gw')\in$ $\in h(V)$; logo podemos definir o homomorfismo de k-espaços vetoriais, $\gamma: C_f \longrightarrow C_h$ por $(\forall w\in W)(\gamma(w+f(V))=gw+h(V))$; é fácil ver que $Ker(\gamma)=N_g/f(V)$ e que $\gamma(C_f)=g(W)/h(V)$. É claro que se $t,t'\in$ $\in T$ com $(t-t')\in h(V)$, então $(t-t')\in g(W)$; logo podemos definir o epimorfismo de k-espaços vetoriais $\rho: C_h \longrightarrow C_g$ por $(\forall t\in T)$ $(\rho(t+h(V))=t+g(W)$; vem facilmente que $Ker(\rho)=g(W)/h(V)$. Logo, indicando por i a inclusão canônica, temos que é exata a sequência de k-espaços vetoriais

$$(0) \longrightarrow N_f \xrightarrow{i} N_h \xrightarrow{f} N_g \xrightarrow{\pi} C_f \xrightarrow{\gamma} C_h \xrightarrow{\rho} C_g \longrightarrow (0)$$

Como $N_h/N_f \approx f(N_h) \subset N_g$ e $N_g$ e $N_f$ têm dimensão finita sobre k, então $N_h$ é um k-espaço vetorial de dimensão finita; também $C_h$ é um k-espaço vetorial de dimensão finita já que $C_h/\gamma(C_f) \approx \rho(C_h) \subset C_g$ e que $C_g$ e $C_f$ têm dimensão finita sobre k.

Logo, a sequência exata de k-espaços vetoriais de dimensões finitas, acima, nos diz imediatamente que

$$[N_f:k]-[N_h:k]+[N_g:k]-[C_f:k]+[C_h:k]-[C_g:k] = 0$$

isto é, $\delta(h) = \delta(f) + \delta(h)$. □

*Lema 3.1.2* - Se k é um corpo, e $f: V \longrightarrow W$ é um homomorfismo de k-espaços vetoriais, com $N_f$ e $C_f$ de dimensões finitas sobre k, então $\delta(f)$ é invariante por extensão de escalares.

*Demonstração:*

Consideremos a sequência exata:

$$(0) \longrightarrow N_f \xrightarrow{i} V \xrightarrow{f} W \xrightarrow{q} C_f \longrightarrow (0)$$

onde i é inclusão canônica e q o homomorfismo canônico de k-espaços vetoriais.

Sendo K um corpo com k⊂K, temos que também é exata a sequência de K-espaços vetoriais:

$$K \underset{k}{\otimes} N_f \xrightarrow{1\otimes i} K \underset{k}{\otimes} V \xrightarrow{1\otimes f} K \underset{k}{\otimes} W \xrightarrow{1\otimes q} K \underset{k}{\otimes} C_f \longrightarrow (0)$$

Logo, $(K \underset{k}{\otimes} W)/(K \underset{k}{\otimes} f(V)) \simeq K \underset{k}{\otimes} C_f$, isto é, $C_{1\otimes f} \simeq K \underset{k}{\otimes} C_f$. Também, $N_{1\otimes f} = K \underset{k}{\otimes} N_f$. Como $[K \underset{k}{\otimes} N_f : K] = [N_f : k]$ e $[K \underset{k}{\otimes} C_f : K] = [C_f : k]$, segue que $\delta(f) = \delta(1\otimes f)$ e o lema está provado. □

Sejam $P \subset K \subset L$ corpos onde P é o corpo primo de K. Indicaremos $D(K) = D(K/P)$ e $D(L) = D(L/P)$.

Sendo $d_K : K \longrightarrow D(K)$ e $D_L : L \longrightarrow D(L)$ duas derivações universais, consideremos a aplicação L-bilinear $\Phi : L\times D(K) \longrightarrow D(L)$ definida por: (se $(\ell, d_K k) \in L\times D(K)$, então $\Phi(\ell, d_K k) = \ell d_L k$). Logo existe um homomorfismo de L-espaços vetoriais que será denotado por $\phi_{K,L}$, definido por: (se $(\ell \otimes d_K k) \in L \underset{K}{\otimes} D(K)$, então:

$$\begin{tikzcd} L\times D(K) \arrow[r, "\Phi"] \arrow[d] & D(L) \\ L \underset{k}{\otimes} D(K) \arrow[ur, "\phi_{K,L}"'] & \end{tikzcd}$$

$$\phi_{K,L}(\ell \otimes d_K k) = \ell d_L k).$$

Indicaremos por $N_{K,L}$ o núcleo de $\phi_{K,L}$.

*Lema 3.1.3* - Sejam $K \subset L \subset M$ corpos, P o corpo primo de L e suponhamos que $C_{\phi_{K,L}}$ e $N_{K,L}$ sejam espaços vetoriais de dimensão finita sobre L, e que $C_{\phi_{L,M}}$, $N_{L,M}$ sejam espaços vetoriais de dimensão finita sobre M. Então:

a) $\delta(\phi_{K,L}) = [D(L/K):L] - [N_{K,L}:L]$

b) $\delta(\phi_{K,L}) + \delta(\phi_{L,M}) = \delta(\phi_{K,M})$.

*Demonstração:*

a) O resultado é imediato se observarmos que $Im(\phi_{K,L})=KdL$, e que, pela proposição 2.2.2, temos $D(L/K)=D(K)/KdL$.

b) Lembremos que $M \otimes_L (L \otimes_K D(K)) \simeq M \otimes_K D(K)$ e consideremos

$$M \otimes_K D(K) \xrightarrow{1\otimes\phi_{K,L}} M \otimes_L D(L) \xrightarrow{\phi_{L,M}} D(M).$$

Temos pelo lema 3.1.2 que $\delta(1\otimes\phi_{K,L}) = \delta(\phi_{K,L})$; também, $\phi_{L,M}\circ(1\otimes\phi_{K,L}) = \phi_{K,M}$. Aplicando-se o lema 3.1.1, o resultado segue imediatamente. □

*Teorema 3.1.1* - Se L/K é uma extensão de corpos de dimensão finita, então $N_{K,L}$ e $D(L/K)$ têm posto finito como L-espaços vetoriais e vale

$$[D(L/K):L]-[N_{K,L}:L] = gr._K\ tr.\ L$$

onde $gr._K$ tr. L indica o grau de transcedência da extensão L/K.

*Demonstração:*

Assumindo que o teorema seja verdadeiro para duas extensões do tipo finito, M/L, L/K, o lema 3.1.3 nos diz que

$$[D(M/K):M]-[N_{K,M}:M]=([D(L/K):L]-[N_{K,L}:L])+([D(M/L):M]-[N_{L,M}:M]).$$

Como $gr._K tr.M = gr._K tr.L + gr._L tr.M$, então temos que o teorema também é verdadeiro para M/K. Logo, a prova deste teorema se reduz ao caso em que L/K é uma extensão simples, $L = K(x)$.

Se x for transcendente ou algébrico separável sobre K, então $N_{K,L}=(0)$. De fato, seja $z = \sum_{i=1}^{n} \ell_i \otimes d_K k_i \in L \otimes_K D(K)$ com $\phi_{K,L}(z) = 0$, isto é, $\sum_{i=1}^{n} \ell_i d_L k_i = 0$; como $d: K \longrightarrow L \otimes_K D(K)$ definida por $(\forall k \in K)(dx = 1 \otimes d_K k)$ é uma derivação de $K$ a valores no $L$-espaço vetorial $L \otimes_K D(K)$, então, pela proposição 1.6.1, existe uma derivação $\bar{d}: L \longrightarrow L \otimes_K D(K)$ que estende $d$; seja $\alpha$ o homomorfismo de $L$-espaços vetoriais tal que $\alpha o d_L = \bar{d}$; temos então que

$$\begin{tikzcd} & L \otimes_K D(K) \\ L \arrow[ur, "\bar{d}"] \arrow[dr, "d_L"'] & \\ & D(L) \arrow[uu, "\alpha"'] \\ & L \otimes_K D(K) \arrow[u, "\phi_{K,L}"'] \end{tikzcd}$$

$$0 = \alpha\Big(\sum_{i=1}^{n} \ell_i d_L k_i\Big) = \sum_{i=1}^{n} \ell_i (\alpha o d_L)(k_i) =$$

$$= \sum_{i=1}^{n} \ell_i \bar{d} k_i = \sum_{i=1}^{n} \ell_i d k_i = \sum_{i=1}^{n} \ell_i (1 \otimes d_K k_i) =$$

$= \sum_{i=1}^{n} \ell_i \otimes d_K k_i$; logo $z=0$ e, portanto $N_{K,L} = (0)$.

Se $x$ for transcendente sobre $K$, temos que $N_{K,L} = (0)$ e $\mathrm{gr.}_K \mathrm{tr.}\ L = 1$; também, $[D(K(x)/K):K(x)] = 1$, pelo corolário 2.5.1; logo o teorema é satisfeito.

Se $x$ for algébrico sobre $K$, como $K[x]=K(x)=L$, pela proposição 2.5.1 temos que $D(L/K) = L\Delta X/L\Delta f$, onde $L\Delta X$ indica um $L$-espaço vetorial de dimensão 1, $\Delta: K[X] \longrightarrow L\Delta X$ é a $K$-derivação de $K[X]$ definida por $(\forall g \in K[X])(\Delta g = g'(x)\Delta X)$, e $f$ é o polinômio minimal de $x$ sobre $K$.

Se $x$ for algébrico separável sobre $K$, temos que $D(L/K) = (0)$ já que $f'(x) \neq 0$, $N_{K,L} = (0)$ e $\mathrm{gr.}_K \mathrm{tr.} L = 0$; logo o teorema é satisfeito.

Se $L/K$ for uma extensão algébrica inseparável, sabemos existir $y \in L$ tal que $K(y)/K$ é algébrica separável ( e portanto nesta extensão o teorema é verdadeiro) e $L/K(y)$ é uma extensão do tipo finito puramente inseparável. Podemos, portanto, supor $x$ puramente inseparável sobre $K$ e tal que $x \notin K$ e $x^p \in K$, onde $p$ indica a característica de $K$. Temos que $D(L/K) \approx L\Delta X$ já que $f'(x) = (X^p - x^p)'(x) = 0$, e que $gr._K tr.L = 0$. Mostremos então que $[N_{K,L} : L] = 1$. Para isto, seja $\{x_\lambda\}_{\lambda \in \Lambda}$ uma p-

$$\begin{array}{c} L \\ | \\ K \\ | \\ L^p \\ | \\ K^p \end{array}$$

base de $K/L^p$; logo $\{x_\lambda, x\}_{\lambda \in \Lambda}$ é uma p-base de $L/L^p$ já que $x \notin K$ e que $L = K^p(x, \{x_\lambda\}_{\lambda \in \Lambda})$; desde que $L^p = K^p(x^p)$ e que $x^p \notin K^p$, $\{x_\lambda, x^p\}_{\lambda \in \Lambda}$ é uma p-base de $K/K^p$. Aplicando-se o corolário 2.5.2, temos que $D(L)$ ($\approx D(L/L^p)$) é um $L$-espaço vetorial com uma base dada por $\{d_L x_\lambda, d_L x\}_{\lambda \in \Lambda}$ e que $D(K)$ ($\approx D(K/K^p)$) é um $K$-espaço vetorial com uma base dada por $\{d_K x_\lambda, d_K x^p\}_{\lambda \in \Lambda}$; desde que $\phi_{K,L} : L \otimes_K D(K) \longrightarrow D(L)$ é tal que $\phi_{K,L}(1 \otimes d_k x_\lambda) = d_L x_\lambda$ para todo $\lambda$, e que $\phi_{K,L}(1 \otimes d_K x^p) = d_L x^p = 0$, temos que $N_{K,L} = L(1 \otimes d_k x^p)$ e, portanto, $[N_{K,L} : L] = 1$.

E o teorema está provado. □

*Definição 3.1.1* - Se $L/K$ é uma extensão de corpos do tipo finito, chama-se inseparabilidade de $L/K$, e indica-se por $InsL/K$, à dimensão de $N_{K,L}$ como $L$-espaço vetorial.

*Corolário 3.1.1* - Seja $L/K$ uma extensão de corpos do tipo finito. Então vale:

a) $0 \leq \text{Ins } L/K < \infty$

b) $\text{Ins } L/K = [D(L/K):L] - \text{gr.}_K \text{ tr. } L$

*Demonstração:*

É uma consequência imediata do teorema 3.1.1. □

*Corolário 3.1.2* - Sejam $K \subset L \subset M$ corpos e $M/K$ uma extensão do tipo finito. Então $\text{Ins } L/K \leq \text{Ins } M/K$ e, consequentemente $[D(L/K):L] \leq [D(M/K):M]$.

*Demonstração:*

Temos que $M/K$ é do tipo finito,e portanto $M/L$ e $L/K$ são também do tipo finito. Logo, o teorema 3.1.1 nos diz que $D(M/L)$, $D(M/K)$, $N_{K,M}$, $N_{L,M}$ são $M$-espaços vetoriais de dimensão finita, e que $D(L/K)$, $N_{K,L}$ são $L$-espaços vetoriais de dimensão finita. Consideremos então:

$$M \underset{K}{\otimes} D(K) \xrightarrow{1 \otimes \phi_{K,L}} M \underset{L}{\otimes} D(L) \xrightarrow{\phi_{L,M}} D(M)$$

Como $\phi_{K,M} = \phi_{L,M} \circ (1 \otimes \phi_{K,L})$, temos que $N_{1 \otimes \phi_{K,L}} \quad N_{K,M}$; também, $N_{1 \otimes \phi_{K,L}} = M \underset{K}{\otimes} N_{K,L}$, pela demonstração do lema 3.1.2,isto é, $M \underset{K}{\otimes} N_{K,L} \subset N_{K,M}$ ; mas $[M \underset{K}{\otimes} N_{K,L} : M] = [N_{K,L} : K]$; logo $[N_{K,L} : L] \leq [N_{K,M} : M]$, isto é, $\text{Ins } L/K \leq \text{Ins } M/K$ . □

*Proposição 3.1.1* - Sejam $K \subset L \subset M$ corpos e $M/K$ uma extensão do tipo finito. Então $\text{Ins } M/K \leq \text{Ins } L/K + \text{Ins } M/L$.

*Demonstração:*

Seja $d: M \longrightarrow D(M/K)$ uma derivação universal de $M$ sobre $K$. Pela proposição 2.2.2, temos que $D(M/L) = D(M/K)/MdL$. Como $M/K$ é uma extensão do tipo finito, temos pelo teorema 3.1.1 que $[D(M/K):M] < \infty$ e, portanto $[MdL:M] < \infty$. Logo, $[D(M/L): M] = [D(M/K):M] - [MdL:M]$.

Consideremos a aplicação M-bilinear $\Phi: M \times D(L/K) \longrightarrow MdL$ definida por (se $(m, d_L \ell) \in M \times D(L/K)$ então $\Phi(m, d_L \ell) = md\ell$), onde $d_L$ é uma derivação universal de $L$. Logo, existe um epimorfismo de M-espaços vetoriais $\psi: M \underset{L}{\otimes} D(L/K) \longrightarrow MdL$ definido por ($\psi(m \otimes d_L \ell) = md\ell$ se $(m \otimes \ell) \in (M \underset{L}{\otimes} D(L/K))$). Temos então:

$$[MdL:M] \leq [M \underset{L}{\otimes} D(L/K):M] = [D(L/K):L]$$

Concluimos então que

$$[D(M/K):M] = [D(M/L):M] + [MdL:M] \leq [D(M/L):M] + [D(L/K):L]$$

Como $gr._K tr.M = gr._K tr.L + gr._L tr.M$, a proposição segue imeditamente. □

## *3.2 - O Módulo das Diferenciais em Extensões de Corpos do tipo Finito*

Neste capítulo, de agora em diante, nos ateremos ao estudo de alguns resultados sobre extensões de corpos do tipo finito. É conveniente que se diga, no entanto, que alguns dos resultados formulados nesta parte do trabalho estão provados para extensões não necessariamente do tipo finito, como é o caso do teorema 3.2.1.

*Definição 3.2.1* - Seja L/K uma extensão de corpos. Diz-se que L/K é uma extensão separavelmente gerada quando existe uma base de transcendência separante $\{x_\lambda\}_{\lambda\in\Lambda}$ de L/K, isto é, $L/K(\{x_\lambda\}_{\lambda\in\Lambda})$ é uma extensão algébrica separável e $K(\{x_\lambda\}_{\lambda\in\Lambda})/K$ é uma extensão transcendente pura.

*Teorema 3.2.1* - Sejam $K\subset L$ corpos. Se L/K é uma extensão algébrica separável, então $D(L/K) = (0)$. Reciprocamente, sendo L/K uma extensão do tipo tinito, se $D(L/K) = (0)$ então L/K é uma extensão algébrica separável.

*Demonstração*:

Suponhamos L/K algébrica separável, e seja $d: L \longrightarrow D(L/K)$ uma derivação universal. Consideremos um elemento $x\in L$ e $f\in K[X]$ o polinômio minimal de x sobre K; como x é álgébrico separável, temos $f(x) = 0$ e $f'(x) \neq 0$. Temos então $0 = d0 = d(f(x) = f^d(x)+f'(x)dx = f'(x)dx$ já que d é trivial sobre K; como $f'(x) \neq 0$, vem que $dx = 0$. Logo $(\forall x\in L)(dx=0)$, isto é, $D(L/K) = (0)$.

Reciprocamente, suponhamos L/K do tipo finito e $D(L/K) = (0)$; como $\text{Ins } L/K = [D(L/K):L] - gr._K\, tr.\, L$ e $\text{Ins } L/K \geq 0$, então $gr._K\, tr.L = 0$, isto é, L/K é uma extensão algébrica, e $\text{Ins } L/K = 0$. Suponhamos por absurdo que exista $y\in L$, $y\notin K$ com y algébrico inseparável sobre K; logo, sendo

$g\in K[X]$ o polinômio minimal de $y$ sobre $K$, temos $f(y)=0$ e $f'(y)=0$. Ora, $K[y] = K(y)$ e então, pelo teorema 2.5.1 $D(K(y)/K) = K(y)\Delta y/K(y)\Delta f$ onde $K(y)\Delta y$ indica um $K(y)$-espaço vetorial de dimensão 1, e $\Delta f=f'(y)\Delta y$ ; logo, $[D(K(y)/K):K(y)] = 1$ e, portanto, $\text{Ins } K(y)/K = 1$ já que $\text{gr.}_K \text{ tr. } K(y) = 0$. Como $L/K$ é do tipo finito, o corolário 3.1.2 nos diz que $\text{Ins } L/K \geq \text{Ins } K(y)/K$; logo $\text{Ins } L/K \geq 1$, o que é absurdo pois $\text{Ins } L/K = 0$. □

$$\begin{array}{c} L \\ | \\ K(g) \\ | \\ K \end{array}$$

*Observação 3.2.1* - A segunda afirmação do teorema 3.2.1 é falsa se supormos que $L/K$ não seja uma extensão do tipo finito. Por exemplo, se $K$ for um corpo não perfeito, com característica $p \neq 0$, temos que $K \subsetneq K^{p^{-1}} \subsetneq K^{p^{-2}} \subsetneq \ldots$. Sendo $L = \bigcup_{n=0}^{\infty} K^{p^{-n}}$, então $D(L/K) = (0)$ já que $L=L^p$, e, no entanto, $L/K$ não é uma extensão algébrica separável.

*Corolário 3.2.1* - Uma extensão de corpos $L/K$ do tipo finito é algébrica separável se, e somente se, $\text{Der}_K(L,L) = (0)$.

*Demonstração:*

Sabemos que $\text{Der}_K(L,L) = D(L/K)^*$, através da observação 2.1.2. Como $D(L/K)$ é um $L$-espaço vetorial de dimensão finita, então $D(L/K)^* \simeq D(L/K)$. O resultado segue agora imediatamente do teorema 3.2.1. □

*Corolário 3.2.2* - Sejam $K\subset L$ corpos, $L/K$ uma extensão do tipo finito, $\{x_1,\ldots,x_n\}\subset L$, e $d\colon L \longrightarrow D(L/K)$ uma derivação univer sal. Então $D(L/K) = \sum_{i=1}^{n} Ldx_i$ se, e somente se, $L/K(x_1,\ldots,x_n)$ é uma extensão algébrica separável.

*Demonstração:*

Seja $M = K(x_1,\ldots,x_n)$. O resultado é imediato se observarmos que $LdM = \sum_{i=1}^{n} Ldx_i$ pois d é trivial sobre K, que $D(L/M) = D(L/K)/LdM$ através da proposição 2.2.2, e que $D(L/M) = (0)$ se, e somente se, L/M é uma extensão algébrica separável, segundo o teorema 3.2.1. □

*Teorema 3.2.2* - Seja L/K uma extensão de corpos do tipo finito. Então L/K é uma extensão separavelmente gerada se, e somente se, Ins L/K = 0.

*Demonstração:*

Suponhamos L/K separavelmente gerada e $\{x_1,\ldots,x_n\} \subset L$ uma base de transcedência separante. Como $L/K(x_1,\ldots,x_n)$ é uma extensão algébrica separável, sendo $d: L \longrightarrow D(L/K)$ uma derivação universal, então, pelo corolário 3.2.2, $D(L/K) = \sum_{i=1}^{n} Ldx_i$. Logo $[D(L/K):L] \leq n$ e, portanto Ins L/K = 0 já que $n = gr._K\, tr.\, L$ e $\text{Ins } L/K = [D(L/K):L] - gr._K\, tr.\, L \geq 0$.

Reciprocamente, suponhamos Ins L/K = 0, e, portanto, seja $n = [D(L/K):L)] = gr._K tr.\, L$. Sendo $d: L \longrightarrow D(L/K)$ uma derivação universal, então $D(L/K) = LdL$; logo existe $\{x_1,\ldots, x_n\} \subset L$ tal que $D(L/K) = \bigoplus_{i=1}^{n} Ldx_i$, isto é, $\{dx_i\}_{1\leq i\leq n}$ é uma base de $D(L/K)$ como $L$-espaço vetorial. Temos que $\{x_1,\ldots,x_n\}$ é uma base de transcedência separante de $L/K$. De fato, sendo $M = K(x_1,\ldots,x_n)$, temos então que

$$D(L/M) = D(L/K)/LdM = \left(\bigoplus_{i=1}^{n} Ldx_i\right) / \sum_{i=1}^{n} Ldx_i;$$

logo $D(L/M) = (0)$ e, portanto $L/M$ é uma extensão algébrica separável; mais ainda, $x_1,\ldots,x_n$ são algebricamente independentes sobre $K$ pois $\mathrm{gr.}_K\,\mathrm{tr.}\ L = n$. Logo $\{x_1, \ldots, x_n\}$ é uma base de transcendência separante de $L/K$, e, portanto, $L/K$ é uma extensão separavelmente gerada. □

*Corolário 3.2.3* - Sejam $K \subset L \subset M$ corpos, $M/K$ uma extensão do tipo finito e $L/K$ uma extensão separavelmente gerada. Então $\mathrm{Ins.}\ L/K = \mathrm{Ins}\ M/K$.

*Demonstração:*

Temos que $\mathrm{Ins}\ L/K \leq \mathrm{Ins}\ M/K$ pelo corolário 3.1.2. A proposição 3.1.1 nos diz que $\mathrm{Ins}\ M/K \leq \mathrm{Ins}\ L/K + \mathrm{Ins}\ M/L$. Como pelo teorema anterior $\mathrm{Ins}\ M/L = 0$, então $\mathrm{Ins}\ M/K \leq \mathrm{Ins} L/K$. Logo $\mathrm{Ins}\ L/K = \mathrm{Ins}\ M/K$. □

*Proposição 3.2.4* - Seja $L/K$ uma extensão de corpos separavelmente gerada, do tipo finito, e seja $d\colon L \longrightarrow D(L/K)$ uma derivação universal. $\{x_1, \ldots, x_n\} \subset L$ é uma base de transcedência separante de $L/K$ se, e somente se $\{dx_1,\ldots,dx_n\}$ é uma base de $D(L/K)$ como $L$-espaço vetorial.

*Demonstração:*

Suponhamos $\{x_1,\ldots,x_n\}$ uma base de transcedência separante de L/K, e seja $M = K(x_1,\ldots,x_n)$. Temos então que L/M é uma extensão algébrica separável e, portanto, que $D(L/M) = (0)$ pelo teorema 3.2.1. Como $D(L/M) = D(L/K)/LdM$, então $D(L/K) = LdM = \sum_{i=1}^{n} Ldx_i$ já que d é trivial sobre K. Mas pelo teorema anterior temos que Ins L/K = 0 e que, portanto, $[D(L/K):L] = \text{gr.}_K \text{ tr.} L = n$. Logo $\{dx_1,\ldots,dx_n\}$ é uma base do L-espaço vetorial D(L/K).

Reciprocamente, suponhamos $\{dx_1,\ldots,dx_n\}$ uma L-base de D(L/K). O teorema 3.2.2 nos diz que Ins L/K = 0, isto é, $\text{gr.}_K \text{ tr.}\ L = [D(L/K):L] = n$. O resultado vem agora da demonstração da recíproca do mesmo teorema 3.2.2. □

*Corolário 3.2.4* - Sejam $K \subset L$ corpos com $L = K(x_1,\ldots,x_n)$. Se L/K é uma extensão separavelmente gerada, então pode-se extrair de $\{x_1,\ldots,x_n\}$ uma base de transcedência separante.

*Demonstração:*

Sendo $d: L \longrightarrow D(L/K)$ uma derivação universal, sabemos que $\{dx_1,\ldots,dx_n\}$ gera D(L/K) como L-espaço vetorial; logo existe $\{dx_{m_1},\ldots,dx_{m_k}\} \subset \{dx_1,\ldots,dx_n\}$ tal que $\{dx_{m_1},\ldots,dx_{m_k}\}$ é uma L-base de D(L/K). Logo, $\{x_{m_1},\ldots,x_{m_k}\} \subset \{x_1,\ldots,x_n\}$ é uma base de transcedência separante de L/K, pela proposição 3.2.2. □

*Corolário 3.2.5* - Seja $L/K$ uma extensão de corpos separavelmente gerada, e seja $d:L \longrightarrow D(L/K)$ uma derivação universal. Se $\{x_\lambda\}_{\lambda\in\Lambda}$ é parte de uma base de transcedência separante, então $\{dx_\lambda\}_{\lambda\in\Lambda}$ é uma família de elementos de $D(L/K)$, linearmente independente sobre $L$. Reciprocamente sendo $L/K$ do tipo finito e $\{dx_1,\ldots,dx_n\}\subset D(L/K)$ um conjunto linearmente independente sobre $L$, então $\{x_1,\ldots,x_n\}\subset L$ é um conjunto algebricamente independente sobre $K$, que faz parte de uma base de transcendência separante de $L/K$.

*Demonstração:*

É uma consequência imediata da proposição 3.2.2. □

*Corolário 3.2.6* - Sejam $L/K$ uma extensão de corpos do tipo finito separavelmente gerada, e $d: L \longrightarrow D(L/K)$ uma derivação universal. Se $\{dx_1,\ldots,dx_n\}\subset D(L/K)$ é um conjunto linearmente independente sobre $L$, então $\{x_1,\ldots,x_n\}\subset L$ é um conjunto algebricamente independente sobre $K$.

*Demonstração:*

É imediato o resultado. □

*Observação 3.2.2* - O corolário 3.2.5 é falso se $L/K$ não for uma extensão separavelmente gerada. Por exemplo, seja $K$ um corpo não perfeito, de característica $p \neq 0$. Consideremos $z\in K-K^p$, $f = X^p - z\in K[X]$, $N$ um corpo de raizes de $f$ sobre $K$, $x\in N$ tal que $x^p = z$ e $L = K(x)$. Temos, portanto, que $L/K$ é uma extensão algébrica e que $f$ é o polinômio minimal de $x$ sobre $K$. Também, co mo $K[x]=K(x)=L$ o teorema 2.5.1 nos diz que $D(L/K)$ é um L-espaço vetorial de dimensão 1. Pelo corolário 1.6.2, $dx\neq 0$ já que $x\notin K(L^p) = K(x^p) = K(z) = K$. Logo $dz$ é uma L-base de $D(L/K)$ e, no entanto, $x$ é algébrico sobre K.

*Observação 3.2.3* - A recíproca do corolário 3.2.5 é falsa em geral. Por exemplo, seja $L = K(x)$ onde $x$ é transcendente sobre K, K como característica $p \neq 0$. Então $z = x^p$ também é transcendente sobre K, logo é algebricamente independente sobre K. No entanto $dz = dx^p = 0$ e, portanto, $dz$ não é linearmente independente sobre K.

*Corolário 3.2.7* - Sejam L/K uma extensão de corpos do tipo finito, K com característica zero, $d: L \longrightarrow D(L/K)$ uma derivação universal. Então $\{x_1,\ldots,x_n\} \subset L$ é algebricamente independente sobre K se, e somente se, $\{dx_1,\ldots,dx_n\} \subset D(L/K)$ é um conjunto linearmente independente sobre L.

*Demonstração:*

Observando-se que toda extensão de corpos de característica zero é separavelmente gerada, e que toda base de transcendência de L/K é também uma base de transcedência separante, o resultado vem trivialmente da proposição 3.2.1. □

*Proposição 3.2.2* - Sejam L/K uma extensão de corpos do tipo finito, K com característica zero, $d: L \longrightarrow D(L/K)$ uma derivação universal, $z, x_1,\ldots,x_n \in L$. Então, $dz \in \sum_{i=1}^{n} Ldx_i$, se, e somente se, z é algébrico sobre $K(x_1,\ldots,x_n)$.

*Demonstração:*

Seja $dz \in \sum_{i=1}^{n} Ldx_i$. Se $dz = 0$, então $z$ é algébrico sobre $K$, pelo corolário 1.6.2. Logo podemos supor, sem perda de generalidade, que $dx_1,\ldots,dx_n$ são linearmente independentes sobre $L$. Da hipótese temos que $dx_1,\ldots,dx_n$, $dz$ são linearmente dependentes sobre $L$. Logo, através do corolário 3.2.7, vem que $x_1,\ldots,x_n$ são algebricamente independentes sobre $K$, e que $x_1,\ldots,x_n$, $z$ são algebricamente dependentes sobre $K$, e, portanto, $z$ é algébrico sobre $K(x_1,\ldots,x_n)$.

Reciprocamente, seja $z$ algébrico sobre $K(x_1,\ldots,x_n)$. Se $x_i$ é algébrico sobre $K$ para $i=1,\ldots,n$, então $z$ é algébrico sobre $K$ e, portanto $dz = 0$ pelo corolário 1.6.2. Podemos então supor, sem perda de generalidade, que $x_1,\ldots,x_n$ sejam algebricamente independentes sobre $K$. Da hipótese, $x_1,\ldots,x_n$, $z$ são algebricamente dependentes sobre $K$. Logo temos que $dx_1,\ldots,dx_n$ são linearmente independentes sobre $L$, e $dx_1,\ldots,dx_n$, $dz$ são linearmente dependentes sobre $L$ e, portanto, $dz \in \sum_{i=1}^{n} Ldx_i$. □

Daremos a seguir, um teorema que virá caracterizar um corpo perfeito. Para isto precisamos do

*Lema 3.2.1* - Sejam $K$ um corpo perfeito, $L/K$ uma extensão do tipo finito, $x_1,\ldots,x_n \in L$, $d\colon L \longrightarrow D(L/K)$ uma derivação universal. Se $dx_1,\ldots,dx_n$ são linearmente independentes sobre $L$, então, $x_1,\ldots,x_n$ são algebricamente independentes sobre $K$.

*Demonstração:*

Suponhamos, por absurdo, que $x_1,\ldots,x_n$ sejam algebricamente dependentes sobre $K$; seja, portanto, $f \in K[X_1,\ldots\ldots,X_n]$, $f \neq 0$, f com o menor grau total possível, $f(x_1,\ldots\ldots,x_n) = 0$. Temos então que $0 = d(f(x_1,\ldots,x_n)) = f^d(x_1,\ldots,x_n) + \frac{\partial f}{\partial x_1} dx_1 + \ldots + \frac{\partial f}{\partial x_n} dx_n$; como d é trivial sobre K, então $\sum_{i=1}^{n} \frac{\partial f}{\partial x_i} dx_i = 0$; logo $\frac{\partial f}{\partial x_i} = \frac{\partial f}{\partial X_i}(x_1,\ldots,x_n) = 0$ para $i=1,\ldots,n$, já que $dx_1,\ldots,dx_n$ são linearmente independentes sobre L. Seja $F_i = \frac{\partial f}{\partial X_i}(X_1,\ldots,X_n) \in K[X_1,\ldots,X_n]$ para $i=1,\ldots,n$; como o grau total de $F_i$ é menor que o grau total de f para $i=1,\ldots,n$, segue então que $F_i = 0$ para $i=1,\ldots,n$. Logo $f \in K[X_1^p,\ldots,X_n^p]$. Como K é perfeito, então existe $g \in K[X_1,\ldots,X_n]$ tal que $f = g^p$ com $g(x_1,\ldots,x_n) = 0$, o que é absurdo dada à escolha de f. □

*Teorema 3.2.3* - Seja K um corpo. Então, K é perfeito se, e somente se, toda extensão de corpos L/K do tipo finito é separavelmente gerada.

*Demonstração:*

Suponhamos K perfeito, e seja L/K uma extensão de corpos, arbitrária, do tipo finito. Logo, pelo lema anterior, temos que $[D(L/K):L] \leq gr._K$ tr. L e, portanto Ins L/K = 0. Logo, L/K é uma extensão separavelmente gerada pelo teorema 3.2.2.

Reciprocamente, suponhamos K com característica $p\neq 0$, e por absurdo, seja K não perfeito; tomemos então $y\in K-K^p$ e consideremos N um corpo de raizes de $f = X^p-y\in K[X]$ sobre K , $x\in N$ com $x^p=z$, e $L = K(x)$. Temos que L/K é uma extensão do tipo finito que não é separavelmente gerada já que L/K é algébrica não separável, o que contradiz a hipótese. Logo K é perfeito. □

Seja K um corpo com característica $p\neq 0$. Recordemos que, se L/K é uma extensão de corpos do tipo finito, sendo $M = K(L^p)$, então L/M é uma extensão puramente inseparável e existe $m\in\mathbb{N}$ ($m \geq 0$) tal que $[L:M] = p^m$; m é definido como sendo o p-grau de L/K. Também, lembremos que se L/K é algébrica separável e puramente inseparável, então $L = K$.

*Proposição 3.2.3* - Sejam L/K uma extensão de corpos puramente inseparável, $\{x_\lambda\}_{\lambda\in\Lambda}\subset L$, K com característica $p\neq 0$, $d:L\longrightarrow D(L/K)$ uma derivação universal. Se $L = K(\{x_\lambda\}_{\lambda\in\Lambda})$ então $D(L/K) = \sum_{\lambda\in\Lambda} Ldx_\lambda$. Reciprocamente, além das hipóteses iniciais, sendo L/K do tipo finito e $\Lambda=\{1,\ldots,n\}$, se $D(L/K) = \sum_{i=1}^{n} Ldx_i$, então $L = K(x_1,\ldots,x_n)$.

*Demonstração:*

A primeira afirmação é imediata já que $K(\{x_\lambda\}_{\lambda\in\Lambda}) = K[\{x_\lambda\}_{\lambda\in\Lambda}]$ e d é trivial em K.

Seja, então, $D(L/K) = Ldx_1+\ldots+Ldx_n$ e consideremos

$M = K(x_1,\ldots,x_n)$. Temos que $D(L/M) = D(L/K)/LdM$ da proposição 2.2.2 e, portanto, $D(L/M) = (0)$ já que $LdM = \sum_{i=1}^{n} Ldx_i = D(L/K)$; logo, pelo teorema 3.2.1, $L/M$ é uma extensão algébrica separável já que $L/M$ é do tipo finito; mas $L/M$ é puramente inseparável por hipótese. Logo $L = M = K(x_1,\ldots,x_n)$. □

*Teorema 3.2.4* - Sejam $L/K$ uma extensão do tipo finito, $K$ com característica $p \neq 0$, $d: L \longrightarrow D(L/K)$ uma derivação universal de $L$ sobre $K$, e $\{x_1,\ldots,x_n\} \subset L$. Então $D(L/K) = \bigoplus_{i=1}^{n} Ldx_i$ se, e somente se, $L = \bigoplus_{\nu} K(L^p)M_\nu(x)$ onde $M_\nu(x) = x_1^{\nu_1}\ldots x_n^{\nu_n}$, $0 \leq \nu_i < p$, $i=1,\ldots,n$.

*Demonstração:*

Seja $M=K(L^p)$ e suponhamos $D(L/K) = \bigoplus_{i=1}^{n} Ldx_i$. Claramente $L/M$ é uma extensão puramente inseparável. Mas $D(L/M) = D(L/K)/LdM$ e $LdM = (0)$, e, então, $D(L/M) = D(L/K) = \bigoplus_{i=1}^{n} Ldx_i$. Logo $L = M(x_1,\ldots,x_n)$ pela proposição anterior. Consideremos agora $M=M_0 \subsetneq M_1=M_0(x_1) \subsetneq M_2=M_1(x_2) \subsetneq \ldots \subsetneq M_n=M_{n-1}(x_n) = L$. Temos que $x_i \notin M_{i-1}=M(x_1,\ldots,x_{i-1})$ para todo $i=1,\ldots,n$; de fato, se por absurdo $x_i \in M_{i-1}$, então $dx_i \in \sum_{k=1}^{i-1} Mdx_k$ já que $d$ é trivial sobre $K(L^p) = M$; logo, $dx_i \in \sum_{k=1}^{i-1} Ldx_k$ o que é absurdo já que, por hipótese, $dx_1,\ldots,dx_n$ são linearmente independentes sobre $L$. Temos, também, claramente, que $x_i^p \in M_{i-1}$. Logo o polinômio minimal de $x_i$ sobre $M_{i-1}$ é $f_i = X^p - x_i^p$, $[M_i:M_{i-1}] = p$ e uma $M_{i-1}$-base de $M_i/M_{i-1}$ é dada por $\{1,x_i,\ldots,x_i^{p-1}\}$ para todo $i=1,\ldots,n$. Consequentemente, $[L:M] = p^n$, e uma $M$-base de $L/M$ é da da por $\{x_1^{\nu_1}\ldots x_n^{\nu_n} : 0 \le \nu_i < p, \quad 1 \le i \le n\}$. Logo $L = \bigoplus_{\nu} K(L^p)M_\nu(x)$.

Reciprocamente, suponhamos $L = \bigoplus_{\nu} K(L^p)M_\nu(x)$, portanto $[L: K(L^p)] = p^n$ e $L = K(L^p)(x_1,\ldots,x_n)$. Logo $D(L/K) = \sum_{i=1}^{n} Mdx_i$ já que d é trivial sobre M. Mas $\sum_{i=1}^{n} Kdx_i \subset \sum_{i=1}^{n} K(L^p)dx_i$ e, portanto $D(L/K) = \sum_{i=1}^{n} Kdx_i$. Também, $[D(L:K):L] = n$; de fato, se $[D(L/K):L] = m \neq n$, então $[L:M] = p^m \neq p^n$, o que é absurdo. Logo $D(L/K) = \bigoplus_{i=1}^{n} Kdx_i$. □

*Corolário 3.2.8* - Seja L/K uma extensão de corpos do tipo finito, K com característica $p \neq 0$. Então $[D(L/K):L]$ é igual ao p-grau de L/K e $gr._K\, tr.L \le$ p-grau de L/K.

*Demonstração:*

O primeiro resultado é uma consequência imediata do teorema anterior. O segundo resultado decorre de uma aplicação direta da primeira afirmação deste corolário e do fato que Ins $L/K \ge 0$. □

*Corolário 3.2.9* - Seja L/K uma extensão de corpos do tipo finito, K com característica $p \neq 0$. Então L/K é separavelmente gerada se, e somente se, (p-grau de L/K) = $gr._K\, tr.\, L$.

*Demonstração:*

Decorre imediatamente da primeira afirmação do corolário anterior, e do teorema 3.2.2. □

*Proposição 3.2.4* - Sejam $L/K$ uma extensão de corpos do tipo finito, $K$ com característica $p \neq 0$, $x_1, x_2, \ldots, x_n$, $z \in L$, $d: L \longrightarrow D(L/K)$ uma derivação universal de $L$ sobre $K$. Então, $dz \in \sum_{i=1}^{n} L dx_i$ se, e somente se, $z \in K(L^p)(x_1, \ldots, x_n)$.

*Demonstração:*

Suponhamos que $dz \in \sum_{i=1}^{n} L dx_i$. Se $dz=0$, então $z \in K(L^p)$ pelo corolário 1.6.2. Logo, podemos supor sem perda de generalidade que $dx_1, \ldots, dx_n$ são linearmente independentes sobre $L$; sejam $x_{n+1}, \ldots, x_m \in L$ tais que $\{dx_1, \ldots, dx_n, \ldots, dx_m\}$ seja uma $L$-base de $D(L/K)$. O teorema anterior nos diz, então, que $L = \bigoplus_{\nu} L^p(K) M_\nu(x)$; logo $z = \sum_{\substack{0 \leq \nu_i < p \\ 1 \leq i \leq m}} a_{\nu_1 \ldots \nu_m} x_1^{\nu_1} \ldots x_m^{\nu_m}$ onde $(\forall i=1, \ldots, m)(\forall 0 \leq \nu_i < p)(a_{\nu_1 \ldots \nu_m} \in L^p(K))$, e, portanto,

$$dz = \sum_{j=1}^{m} \nu_j \Big( \sum_{\substack{0 \leq \nu_i < p \\ 1 \leq i \leq m}} a_{\nu_1 \ldots \nu_m} x_1^{\nu_1} \ldots x_j^{\nu_j - 1} \ldots x_m^{\nu_m} \Big) dx_j; \text{ logo}$$

$$\sum_{\substack{0 \leq \nu_i < p \\ 1 \leq i \leq m}} \nu_j \cdot a_{\nu_1 \ldots \nu_m} x_1^{\nu_1} \ldots x_j^{\nu_j - 1} \ldots x_m^{\nu_m} = 0 \text{ para todo } j=n+1, \ldots,$$

$m$, já que $dz \in \sum_{i=1}^{n} L dx_i$ e $\{dx_1, \ldots, dx_m\}$ é uma $L$-base de $D(L/K)$; mas $(\forall i=1, \ldots, m)(\forall\ 0 \leq \nu_i < p)$ $x_1^{\nu_1} \ldots x_m^{\nu_m}$ são linearmente independentes sobre $M$; logo $\nu_j\ a_{\nu_1 \ldots \nu_m} = 0$ para $i=1, \ldots, m$ e $0 \leq \nu_i < p$; portanto, $(\forall j=n+1, \ldots, m)(\forall i=1, \ldots, m)(\forall\ 0 \leq \nu_i < p)$ tem-se $\nu_j = 0$ ou $a_{\nu_1 \ldots \nu_m} = 0$; logo $z \in K(L^p)(x_1, \ldots, x_n)$.

Reciprocamente, seja $z \in K(L^p)(x_1, \ldots, x_n)$; logo existem $f,g \in K(L^p)[X_1,\ldots,X_n]$ tal que $z = \dfrac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$ com $g(x_1,\ldots,x_n) \neq 0$. Como $d$ é trivial sobre $K(L^p)$, segue imediatamente que $dz \in \sum_{i=1}^{n} Ldx_i$. □

Lembremos agora, o Teorema do Elemento primivo: Seja $L/K$ uma extensão de corpos algébrica tal que $L = K(x_1,\ldots,x_n)$ e $x_i$ é algébrico separável para todo $i=2,\ldots,n$. Então, existe $\xi \in L$ tal que $L = K(\xi)$. ([10] pp.167 e 168).

*Teorema 3.2.5* - Sejam $L/K$ uma extensão de corpos do tipo finito, e $n = gr._K\, tr.L$. Então:

a) Se Ins $L/K = 0$, $L$ pode ser obtido de $K$ pela **adjunção** de $(n+1)$ elementos de $L$, e pelo menos $n$ elementos são necessários.

b) Se Ins $L/K = m > 0$, $L$ pode ser obtido de $K$ pela adjunção de $(n+m)$ elementos de $L$ e exatamente $n+m$ elementos são necessários.

*Demonstração:*

a) Pelo teorema 3.2.2 temos que $L/K$ é uma extensão separável; também, $[D(L/K):L] = n = gr._K\, tr.\, L$. Seja, então, $\{x_1,\ldots,x_n\}$ uma base de transcendência separante de $L/K$; logo $L/K(x_1,\ldots,x_n)$ é uma extensão algébrica separável e, portanto, pelo teorema do elemento primitivo, existe $z \in L$ tal que $L=K(x_1,\ldots,x_n)(z)$ já que $L/K$ é do tipo finito. Também, se $L=K(y_1,\ldots,y_t)$ então, evidentemente, $D(L/K) = \sum_{i=1}^{t} Ldy_i$; como

$[D(L/K):L] = n$, então, $t \geq n$. E o resultado está provado.

b) Neste caso temos claramente, que $[D(L/K):L]=m+n$ e que se $L=K(y_1,\ldots,y_t)$, então $t \geq n+m$. Mostremos, pois, que existe um conjunto de $n+m$ geradores de $D(L/K)$ como $L$-espaço vetorial. Para isto, seja $\{dx_1,\ldots,dx_n,\ldots,dx_{n+m}\}$ uma $L$-base de $D(L/K)$. Então, pelo corolário 3.2.2, temos que $L/K(x_1,\ldots,x_{n+m})$ é uma extensão algébrica separável. Logo $gr._K\, tr.K(x_1,\ldots,x_{n+m})=n$ já que $gr._K tr.L=n$. Assim, podemos supor sem perda de generalidade que $x_1,\ldots,x_n$ são algebricamente independentes sobre $K$, e, portanto, que $\{x_1,\ldots,x_n\}$ é uma base de transcendência de $L/K$. Logo, chamando $M=K(x_1,\ldots,x_n)$, temos que $L/M$ é uma extensão algébrica. Seja $T=\{x \in L: x$ é algébrico separável sobre $M\}$; claramente $T$ é um corpo e $K \subset M \subset T \subset L$ onde $T/M$ é uma extensão algébrica separável e $L/T$ é uma extensão puramente inseparável; pelo teorema do elemento primitivo temos então que existe $z \in L$ tal que $T=M(z)$. Também, sabemos que $D(L/T)=D(L/K)/LdT =(\sum_{j=1}^{n+m} Ldx_j)/LdT$, onde $d$ indica uma derivação universal de $L$ sobre $K$; como $x_1,\ldots,x_n \in T$, segue que $D(L/T) =(\sum_{j=n}^{n+m} Ldx_j)/LdT$ e, portanto, $D(L/T)= \sum_{j=n}^{n+m} T\partial x_j$ onde $\partial$ indica uma derivação universal de $L$ sobre $T$. Como $L/T$ é uma extensão puramente inseparável, e do tipo finito, então, pela proposição 3.2.4, $L=T(x_n,\ldots,x_{n+m})$. Logo $L = K(x_1,\ldots,x_n,z)(x_{n+1},\ldots,x_{n+m})=K(x_1,\ldots,x_{n+m},z)$. Finalmente, consideremos a extensão $M(x_{n+1},z)/M$; como $x_{n+1}$ é algébrico sobre $M$, e $z$ é algébrico separável sobre $M$, então, o teorema do elemento primitivo nos garante a existência de $\xi \in M(x_{n+1},z) \subset L$ tal que $M(x_{n+1},z)=M(\xi)$. Logo, $L=K(x_1,\ldots,x_n,x_{n+1},\ldots,x_{n+m},\xi)$ e obtivemos assim, n+m geradores de L/K. □

Terminaremos este capítulo com o teorema que nos dá o resultado fundamental da caracterização de uma extensão separavelmente gerada do tipo finito.

Lembremos, para tanto, de um resultado geral que nos diz que se uma extensão de corpos de característica $p \neq 0$, $L/K$, é separavelmente gerada, então os corpos $K$ e $L^p$ são linearmente disjuntos sobre $K^p$. ([11], pp. 111 e 112).

*Teorema 3.2.6* - Seja $L/K$ uma extensão de corpos do tipo finito, $K$ com característica $p \neq 0$. As seguintes condições são equivalentes:

a) $L/K$ é separavelmente gerada

b) $\operatorname{Ins} L/K = 0$

c) Para todo corpo $M$ tal que $K \subset M \subset L$, $M/K$ é uma extensão separavelmente gerada

d) $K$ e $L^p$ são linearmente disjuntos sobre $K^p$.

*Demonstração:*

O resultado geral acima enunciado nos diz que: (a) $\Longrightarrow$ (d); que (a) $\Longleftrightarrow$ (b), vem do teorema 3.2.2; trivialmente temos que (c) $\Longrightarrow$ (a). Mostremos então que (b) $\Longrightarrow$ (c) e que (d) $\Longrightarrow$ (b), terminando, assim, a prova deste teorema.

Seja $M$ corpo, com $K \subset M \subset L$, e suponhamos $\operatorname{Ins} L/K = 0$. Como $0 \leq \operatorname{Ins} M/K \leq \operatorname{Ins} L/K = 0$, então $\operatorname{Ins} M/K = 0$ e, portanto, M/K é separavelmente gerada, pelo teorema 3.2.2. Logo (b)$\Rightarrow$(c).

Mostremos que (d) $\Longrightarrow$ (b). Para isto, se d é uma derivação universal de L sobre K, seja $\{dx_1,\dots,dx_n\}$ uma L-base de $D(L/K)$, onde $x_1,\dots,x_n \in L$. Verifiquemos que $x_1,\dots,x_n$ são algebricamente independentes sobre K, de onde virá que $gr._K tr.L \geq$ $\geq [D(L/K):L]$ e, portanto, que Ins L/K = 0.

Suponhamos, então, por absurdo, que $x_1,\dots,x_n$ sejam algebricamente dependentes sobre K, seja $f \in K[X_1,\dots,X_n]$, $f \neq 0$, f com menor grau total possível tal que $f(x_1,\dots,x_n) = 0$. Logo $d(f(x_1,\dots,x_n)) = 0$, isto é, $\sum_{i=1}^{n} \frac{\partial f}{\partial x_i} dx_i = 0$, já que d é trivial sobre K. Como $dx_1,\dots,dx_n$ são linearmente independentes sobre L, vem que $(\forall i=1,\dots,n)(\frac{\partial f}{\partial x_i} = \frac{\partial f}{\partial X_i}(x_1,\dots,x_n)=0)$ e, portanto, dada a escolha de f, $\frac{\partial f}{\partial X_i} = 0$ para todo $i=1,\dots,n$. Consequentemente, temos que existe $g \in K[X_1^p,\dots,X_n^p]$, $g \neq 0$ tal que $f=g$. Seja $g = \sum_\alpha a_\alpha M_\alpha(X^p)$. Como para todo $\alpha$, $M_\alpha(x^p) \in L^p$ e $\sum_\alpha a_\alpha M_\alpha(x^p)=0$, segue que $\{M_\alpha(x^p)\}_\alpha$ é um conjunto de elementos de $L^p$ linearmente dependentes sobre K, já que $g \neq 0$; logo, como K e $L^p$ são linearmente disjuntos sobre $K^p$, segue que $\{M_\alpha(x^p)\}_\alpha$ é um conjunto de elementos de $L^p$ linearmente dependentes sobre $K^p$; logo existe uma família $(b_\alpha)$ de elementos não todos nulos de K, tal que $\sum_\alpha b_\alpha^p M_\alpha(x^p)=0$ e, portanto, com $\sum_\alpha b_\alpha M_\alpha(x)=0$, o que é absurdo, dada a escolha de f. □

*Observação 3.2.4* - É essencial a hipótese de que L/K seja do tipo finito para que valha (d) $\Longrightarrow$ (a) no teorema anterior. Por exemplo, seja K um corpo perfeito de característica $p \neq 0$, e

$L = \bigcup_{n=0}^{\infty} K(X^{p^{-n}})$. Claramente $\{X\}$ é uma base de transcendência de $L/K$ e, portanto $gr._K\, tr.L = 1$; se, por absurdo existir $\{y\}$, uma base de transcendência separante de $L/K$, então temos que $L/K(y)$ é uma extensão algébrica separável; logo temos que $L/K(X,y)$ é uma extensão algébrica separável, mas que também é, uma extensão puramente inseparável; portanto, $L=K(X,y)$ e consequentemente, $[L:K(X)] < \infty$, o que é absurdo. Chegamos então que $L/K$ não é uma extensão separavelmente gerada; mas $L^p$ e $K$ são linearmente disjuntos sobre $K^p$, evidentemente, já que $K^p = K$.

CAPÍTULO IV

# O PROBLEMA DO PROLONGAMENTO DE DERIVAÇÕES

## 4.1 - *O Teorema Geral para o Prolongamento de Derivações*

Sejam R,S,T anéis, S uma R-álgebra, T uma S-álgebra.

O teorema que virá a seguir dará uma condição necessária e suficiente para que uma R-derivação de S a valores em um dado T-módulo M possa ser prolongada a uma R-derivação de T a valores em M.

Indicaremos por $d_S^R:S \longrightarrow D(S/R)$ e por $d_T^R:T \longrightarrow D(T/R)$ duas derivações universais.

Considerando a aplicação T-bilinear $\Phi:T\times D(S/R) \longrightarrow D(T/R)$ definida por: (se $(t,d_S^R x)\in T\times D(S/R)$, então $\Phi(t,d_S^R x) = td_T^R x)$, garantimos a existência de um homomorfismo de T-módulos,

$$\begin{tikzcd} T\times D(S/R) \arrow[r, "\Phi"] & D(T/R) \\ T \underset{S}{\otimes} D(S/R) \arrow[ur, "\phi_{R:S,T}"'] & \end{tikzcd}$$

que será denotado por $\phi_{R:S,T}$, definido por: (se $(t\otimes d_S^R x) \in T \underset{S}{\otimes} D(S/R)$, então $\phi_{R:S,T}(t \otimes d_S^R x) = td_T^R x)$.

Indicaremos por $N_{R:S,T}$ o núcleo de $\phi_{R:S,T}$, e por $D_{R:S,T}$ o conúcleo de $\phi_{R:S,T}$.

Temos assim, a seguinte sequência exata:

$$(0) \longrightarrow N_{R:S,T} \xrightarrow{\ i\ } T\underset{S}{\otimes}D(S/R) \xrightarrow{\ \phi_{R:S,T}\ } D(T/R) \xrightarrow{\ q\ } D_{R:S,T} \longrightarrow (0)$$

onde i é a inclusão canônica e q o homomorfismo canônico de mó dulos.

Temos também que $D_{R:S,T} \simeq D(T/S)$, já que $D(T/S) \simeq$ $\simeq D(T/R)/Td_T^R S$ e que $\phi_{R:S,T}(T\underset{R}{\otimes}D(S/R)) = Td_T^R S$.

*Teorema 4.1.1* - Sejam S uma R-álgebra e T uma S-álgebra. Então, para qualquer T-módulo M, toda R-derivação de S a valores em M pode ser estendida a uma R-derivação de T a valores em M se, e somente se:

a) $\phi_{R:S,T}$ é injetora

b) $T \underset{S}{\otimes} D(S/R)$ é isomorfo, como T-módulo, a um somando direto de D(T/R).

*Demonstração:*

Suponhamos que toda R-derivação de S a valores em qualquer T-módulo M possa ser prolongada a uma R-derivação de T a valores em M. Seja $z = \sum_i (t_i \otimes d_S^R x_i)$ um elemento de $T\underset{S}{\otimes}D(S/R)$ tal que $\phi_{R:S,T}(z) = 0$, isto é, $\sum_i t_i d_T^R x_i = 0$. Como a aplicação $\Delta: S \longrightarrow T\underset{S}{\otimes}D(S/R)$ definida por $(\forall x \in S)(\Delta x = 1\otimes d_S^R x)$ é uma R-derivação de S a valores no T-módulo $T\underset{S}{\otimes}D(S/R)$, segue, da hipótese, que existe uma R-derivação $\bar{\Delta}: T \longrightarrow T\underset{S}{\otimes}D(S/R)$ que estende $\Delta$; logo, existe um homomorfismo $\alpha$, de T-módulos, tal que $\alpha \circ d_T^R = \bar{\Delta}$; como $\sum_i t_i d_T^R x_i = 0$, então temos que

$$\begin{tikzcd}[row sep=small]
 & T\otimes_S D(S/R) \\
T \arrow[ur, "\bar{\Delta}"] \arrow[dr, "d_T^R"'] & \\
 & D(T/R) \arrow[uu, "\alpha"'] \\
 & T\otimes_S D(S/R) \arrow[u, "\phi_{R:S,T}"']
\end{tikzcd}$$

$0 = \alpha(\sum_i t_i d_T^R x_i) = \sum_i t_i(\alpha o d_T^R)(x_i) = \sum_i t_i \bar{\Delta} x_i =$

$= \sum_i t_i \Delta x_i = \sum_i t_i (1\otimes d_S^R x_i)$ já que $x_i \in S$ para todo i; portanto $\sum_i t_i \otimes d_S^R x_i = 0$ e $\phi_{R:S,T}$ é injetora. Também, $\alpha o \phi_{R:S,T} = 1_{T\otimes_S D(S/R)}$ pois se $\sum_i t_i \otimes d_S^R x_i \in T\otimes_S D(S/R)$, então $\alpha o \phi_{R:S,T}(\sum_i t_i \otimes d_S^R x_i) =$

$= \alpha(\sum_i t_i d_T^R x_i) = \sum_i t_i (\alpha o d_T^R)(x_i) = \sum_i t_i \bar{\Delta} x_i = \sum_i t_i (1\otimes d_S^R x_i) = \sum_i t_i \otimes d_S^R x_i$

já que $x_i \in S$ para todo i. Logo a sequência exata

$$(0) \longrightarrow T\otimes_S D(S/R) \xrightarrow{\phi_{R:S,T}} D(T/R) \longrightarrow D_{R:S,T} \longrightarrow (0)$$

cinde e, portanto, $D(T/R) = [T\otimes_S D(S/R)] \oplus D_{R:S,T}$, e $T\otimes D(S/R)$ é isomorfo a um somando direto de $D(T/R)$.

Reciprocamente, suponhamos válidas (a) e (b) e suponhamos M um T-módulo e $\Delta: S \longrightarrow M$ uma R-derivação de S. Então

$$\begin{tikzcd}
 & T \arrow[r, "d_T^R"] \arrow[d, dash] & D(T/R) \arrow[dl, "\bar{\alpha}"] \\
D(S/R) \arrow[dr, "\lambda"'] & S \arrow[l, "d_S^R"'] \arrow[d, "\Delta"] & \\
 & M & T\otimes_S D(S/R) \arrow[l, "\alpha"'] \arrow[uu, "\phi_{R:S,T}"']
\end{tikzcd}$$

existe um único homomorfismo $\lambda$ de S-módulos tal que $\lambda o d_S^R = \Delta$. Seja $\alpha$ o homomorfismo de T-módulos induzido naturalmente por $\lambda$, isto é, se $z = \sum_i t_i \otimes d_S^R x_i \in T\otimes_S D(S/R)$, então $\alpha(z) = \sum_i t_i \lambda(d_S^R x_i)$. Como por hipótese, $T\otimes_S D(S/R)$ é isomorfo a um somando direto de $D(T/R)$, e $\phi_{R:S,T}$ é injetora, então existe um T-subespaço vetorial U, de D(T/R) tal que $D(T/R) = (Td_T^R S \oplus U)$. Logo, existe um homomorfismo $\bar{\alpha}$ de T-espaços vetoriais que estende $\alpha$ tal que, se

$\sum_i t_i d_T^R x_i \in Td_T^R S$ e $y \in U$, então $\bar{\alpha}(\sum_i t_i d_T^R x_i + y) = \sum_i \lambda(t_i \otimes d_S^R x_i)$. Consideremos $\bar{\Delta} = \bar{\alpha} o d_T^R$; temos então que $(\forall x \in S)(\bar{\Delta}x = (\bar{\alpha} o d_T^R)x = \bar{\alpha}(d_T^R x) = \alpha(1 \otimes d_S^R x) = (\lambda o d_S^R x) = \Delta x)$, isto é, $\bar{\Delta}$ é uma R-derivação de T que prolonga $\Delta$. □

*Corolário 4.1.1* - Sejam S,R anéis, T um corpo, S uma R-álgebra, T uma S-álgebra. Então, para qualquer T-espaço vetorial M, toda R-derivação de S a valores em M pode ser estendida a uma R-derivação de T se, e somente se, $\phi_{R:S,T}$ é injetora.

*Demonstração:*

É uma consequência imediata do teorema anterior, se lembrarmos que todo subespaço vetorial de um espaço vetorial M, é um somando direto de M. □

*Corolário 4.1.2* - Sejam R,S anéis, T um corpo, S uma R-álgebra, T uma S-álgebra. Então para qualquer T-espaço vetorial M, toda R-derivação de S a valores em M pode ser estendida de uma única maneira a uma R-derivação de T se, e somente, $\phi_{R:S,T}$ é um isomorfismo de T-espaços vetoriais.

*Demonstração:*

Temos, claramente, que $\phi_{R:S,T}$ é sobrejetora, se, e somente se, $D_{R:S,T} \approx D(T/S) = (0)$.

Suponhamos que para qualquer T-espaço vetorial M, toda R-derivação de S possa ser prolongada a uma única R-derivação de T. O teorema anterior nos diz que $\phi_{R:S,T}$ é injetora. Co mo uma derivação universal de T sobre S prolonga a derivação nula de S, e como por hipótese, existe uma única derivação que prolonga a derivação nula, segue que $d_T^S = 0$ e, portanto $D(T/S) = (0)$. Logo $\phi_{R:S,T}$ é um isomorfismo.

Reciprocamente, suponhamos que $\phi_{R:S,T}$ seja um isomorfismo e consideremos $d: S \longrightarrow M$ uma R-derivação de S a valores num T-espaço vetorial M. Como $\phi_{R:S,T}$ é injetora, o corolário anterior nos diz que existe uma R-derivação de T, $\Delta: T \to M$ que prolonga d. Mostremos que $\Delta$ é a única R-derivação de T que prolonga d. Consideremos, para isto, $\bar{\Delta}: T \longrightarrow M$ uma R-derivação de T que prolonga d. Sejam $\lambda, \bar{\lambda}: D(T/R) \longrightarrow M$ os únicos homomorfismos de T-espaços vetoriais tais que $\lambda o d_T^R = \Delta$ e $\bar{\lambda} o d_T^R = \bar{\Delta}$. Se $t \in T$, então $d_T^R t \in T d_T^R S$ já que sendo $\phi_{R:S,T}$ sobrejetora, $(0) = D(T/S) = D(T/R)/T d_T^R S$; logo $d_T^R t = \sum_{i=1}^{n} t_i d_T^R x_i$ onde $t_i \in T$ e $x_i \in S$ para $i=1,\ldots,n$; temos então que $\bar{\Delta} t = (\bar{\lambda} o d_T^R)(t) =$

$$= \bar{\lambda}\left(\sum_{i=1}^{n} t_i d_T^R x_i\right) = \sum_{i=1}^{n} t_i (\bar{\lambda} o d_T^R)(x_i) = \sum_{i=1}^{n} t_i \bar{\Delta} x_i = \sum_{i=1}^{n} t_i d x_i =$$

$$= \sum_{i=1}^{n} t_i \Delta x_i = \sum_{i=1}^{n} t_i (\lambda o d_T^R)(x_i) = \lambda\left(\sum_{i=1}^{n} t_i d_T^R x_i\right) = \lambda o d_T^R (t) = \Delta t,$$ isto é, $\bar{\Delta} = \Delta$. □

*Observação:4.1.1* - No teorema 4.1.1 se T não for um corpo, o fato de $\phi_{R:S,T}$ ser injetora não implica que toda R-derivação de S possa ser prolongada a uma R-derivação de T. Por exemplo, seja R um corpo de característica $p \neq 2$, e sejam $S = R[X^2]$ e $T = R[X]$. A aplicação $\phi_{R:S,T}: T \otimes_S D(S/R) \longrightarrow D(T/R)$ é definida por $\phi_{R:S,T}(t \otimes d_S^R X^2) = 2X t d_S^R X$ e é claramente um isomorfismo. No entanto, a R-derivação, d: $S \longrightarrow T$ definida, por : (se $f \in S$, $df = \frac{\partial f}{\partial X^2}$) não pode ser estendida a uma derivação de T pois $d(X^2) = 2XdX = 1$.

## *4.2 - Extensões Separáveis*

*Definição 4.2.1* - Uma extensão de corpos L/K diz-se *separável* se para qualquer L-espaço vetorial M, toda derivação $D:K \longrightarrow M$ pode ser prolongada a uma derivação $\Delta: L \longrightarrow M$.

*Teorema 4.2.1* - Seja L/K uma extensão de corpos do tipo finito. Então, L/K é separável se, e somente se, L/K é separavelmente gerada.

*Demonstração:*

Decorre imediatamente do teorema 3.2.2 e do corolário 4.1.1. □

*Observação 4.2.1* - Se L/K for uma extensão de corpos não do tipo finito, o teorema anterior é falso. Por exemplo, seja K um corpo perfeito com característica $p \neq 0$, e seja $L = \bigcup_{n=0}^{\infty} K(X^{p^{-n}})$. Já verificamos, através da observação 3.2.4 que L/K não é uma extensão separavelmente gerada. No entanto, como K é perfeito a única derivação de K é a trivial e, consequentemente, pode ser prolongada a uma derivação de L (a derivação nula).

*Proposição 4.2.1* - Sejam $K \subset M \subset L$ corpos. Se L/M e M/K são exten sões separáveis, então L/K é uma extensão separável. Se L/K é separável, então M/K também é separável.

*Demonstração:*

Decorre imediatamente da definição 4.2.1. □

*Proposição 4.2.2* - Se L/K é uma extensão separavelmente gerada, então L/K é uma extensão separável.

*Demonstração:*

Decorre imediatamente dos corolários 1.6.2, 1.6.3 e da proposição anterior. □

*Proposição 4.2.3* - Se K é um corpo perfeito, então toda extensão de corpos L/K é separável.

*Demonstração:*

Se K tem característica zero, o resultado vem imediatamente através do teorema 1.6.2 (a). Se a característica de K for $p \neq 0$, então $K = K^p$; logo $D(K) = (0)$ e, portanto $\phi_{K,L}$ é injetora. O resultado, agora, segue do corolário 4.1.1. □

*Proposição 4.2.4* - Se L/K for uma extensão de corpos algébrica separável, para qualquer L-espaço vetorial M, toda derivação de K a valores em M pode ser prolongada de um único modo, a uma derivação de L. Reciprocamente, se L/K for uma extensão de corpos do tipo finito, então, se para qualquer L-espaço vetorial M, toda derivação de K a valores em M puder ser prolonga da de um único modo a uma derivação de L, então L/K é algébrica separável.

*Demonstração:*

Decorre facilmente, da proposição 4.2.2, do corolário 4.1.2 e do teorema 3.2.1. □

A proposição que segue virá dar um resultado que generaliza uma parte da proposição 3.2.1.

*Proposição 4.2.5* - Se L/K é uma extensão de corpos separavelmente gerada, e se $\{x_\lambda\}_{\lambda\in\Lambda}$ é uma base de transcendência separante de L/K, então $\{d_L^K x_\lambda\}_{\lambda\in\Lambda}$ é uma L-base de D(L/K).

*Demonstração:*

Seja $M = K(\{x_\lambda\}_{\lambda\in\Lambda})$ e consideremos, como no início deste capítulo, a sequência exata

$$(0) \longrightarrow N_{K:M,L} \xrightarrow{i} L\underset{M}{\otimes}D(M/K) \xrightarrow{\phi_{K:M,L}} D(L/K) \xrightarrow{q} D_{K:M,L} \longrightarrow (0)$$

Como L/M é algébrica separável, temos que $N_{K:M,L}=(0)$ pela proposição 4.2.2 e pelo corolário 4.1.2; também $D(L/M) = (0)$ pelo teorema 3.1.1. Logo, $\phi_{K:M,L}$ é um isomorfismo de L-espaços vetoriais, e temos que $L\underset{M}{\otimes}D(M/K) \simeq D(L/K)$. Ora, M/K é uma extensão transcendente pura; logo, D(M/K) é um M-espaço vetorial com uma base dada por $\{d_M^K x_\lambda\}_{\lambda\in\Lambda}$ e, consequentemente $L\underset{M}{\otimes}D(M/K)$ e D(L/K) são L-espaços vetoriais com base de cardinalidade igual à cardinalidade $\Lambda$. Por outro lado, já que

$D(L/M) = (0)$ e que $D(L/M) = D(L/K)/Ld_L^K M$, vem que $D(L/K)=Ld_L^K M=$ $= \sum_{\lambda\in\Lambda} Ld_L^K x_\lambda$ pois $d_L^K$ é trivial sobre K. Portanto $\{d_L^K x_\lambda\}_{\lambda\in\Lambda}$ é uma L-base de $D(L/K)$. □

*Definição 4.2.2* - Seja K um corpo com característica $p\neq 0$. Diz se que *uma extensão de corpos* L/K *preserva a p-independência* se para todo conjunto $X\subset K$ p-independente em K, X também é p-independente em L.

Lembremos, que dado um corpo K com característica $p\neq 0$, um conjunto $X\subset K$ diz-se "p-independente em K", se X é um conjunto p-independente de K sobre $K^p$. Também, diz-se que X é uma "p-base de K" se X é uma p-base de K sobre $K^p$.

O teorema que daremos a seguir virá caracterizar as extensões separáveis.

*Teorema 4.2.2* - Seja K um corpo com característica $p\neq 0$, e seja L/K uma extensão de corpos. São equivalentes as seguintes condições:

a) L/K é separável

b) L/K preserva a p-independência

c) $L^p$ e K são linearmente disjuntos sobre $K^p$.

*Demonstração:*

(a) $\Longrightarrow$ (b). Suponhamos, por absurdo, que L/K não preserva a p-independência; logo, existe $X = \{x_\lambda\}_{\lambda\in\Lambda}\subset K$, X uma p-base de K tal que X não é p-independente em L, e, portanto, existe $x \in X$ tal que $x \in L^p(X-\{x\})$. Sabemos pelo corolário 2.5.2, que $D(K)$ é um K-espaço vetorial com uma base dada por $\{d_K x_\lambda\}_{\lambda \in \Lambda}$; consideremos, então, o homomorfismo de K-espaços vetoriais, $\lambda: D(K) \longrightarrow L$ tal que $\lambda(d_K x) = 1$ e $\lambda(d_K x_\lambda) = 0$, se $x_\lambda \neq x$ com $\lambda \in \Lambda$. A derivação $\Delta$ de K a valores em L definida por $\Delta = \lambda \circ d_K$ admite um prolongamento, por hipótese, a uma derivação $\bar{\Delta}$ de L. Como $x \in L^p(X-\{x\})$, então existem $\{x_1,\ldots,x_n\} \subset X-\{x\}$ e $f \in L^p[X_1,\ldots,X_n]$, $f \neq 0$ tais que $x = f(x_1,\ldots,x_n)$; logo $\bar{\Delta} x = \bar{\Delta} f(x_1,\ldots,x_n) = 0$, o que é absurdo pois $\bar{\Delta} x = \Delta x = 1$. Portanto L/K preserva a p-independência.

(b) $\Longrightarrow$ (a). Seja $X = \{x_\lambda\}_{\lambda \in \Lambda}$ uma p-base de K. Como X é p-independente em K e, por hipótese, L/K preserva a p-independência, existe $Y = \{y_i\}_{i \in I} \subset L$ tal que $X \cup Y$ é uma p-base de L. Temos, pelo corolário 2.5.2, que $D(L)$ é um L-espaço vetorial com uma base dada por $\{d_L x_\lambda\}_{\lambda \in \Lambda} \cup \{d_L y_i\}_{i \in I}$. Sejam M um L-espaço vetorial e $\Delta: K \longrightarrow M$ uma derivação de K, e consideremos o homomorfismo de L-espaços vetoriais $\lambda: D(L) \longrightarrow M$ tal que $\lambda(d_L x_\lambda) = \Delta x_\lambda$ e $\lambda(d_L y_i) = 0$ para $\lambda \in \Lambda$ e $i \in I$. Seja $\bar{\Delta}: L \longrightarrow M$ a derivação de L definida por $\bar{\Delta} = \lambda \circ d_L$; temos que se $k \in K$, então existem $k_1,\ldots,k_n \in K$ e $x_1,\ldots,x_n \in X$ tal que $k = \sum_{i=1}^{n} k_i^p x_i$ já que $K = K^p(X)$; logo $\bar{\Delta} k = \lambda \circ d_L\left(\sum_{i=1}^{n} k_i^p x_i\right) = \lambda\left(\sum_{i=1}^{n} k_i^p d_L x_i\right) =$

$$= \sum_{i=1}^{n} k_i^p \lambda(d_L x_i) = \sum_{i=1}^{n} k_i^p \Delta x_i = \Delta\left(\sum_{i=1}^{n} k_i^p x_i\right) = \Delta k,$$

isto é, $\bar{\Delta}$ é uma derivação de L que estende $\Delta$. Portanto, L/K é separável.

(a) $\Longrightarrow$ (c). Mostremos que K e $L^p$ são linearmente disjuntos sobre $K^p$, isto é, para todo conjunto $Y \subset L$, a independência linear de Y sobre K implica na independência linear de $Y^p$ sobre K. Para tanto, seja $X = \{x_1,\dots,x_n\} \subset L$ um conjunto linearmente independente sobre K. Se, por absurdo, $X^p$ for linearmente dependente sobre K, seja, então, m, o menor natural $(0 < m \leq n)$ tal que $\sum_{i=1}^{m} \alpha_i x_i^p = 0$, com $\alpha_i \in K$ para $i=1,\dots,m$ e $\alpha_m \neq 0$; podemos evidentemente, supor $\alpha_m = 1$. Logo $\sum_{i=1}^{m-1} x_i^p d_L \alpha_i = 0$ já que $d_L \alpha_m = d_L 1 = 0$. Ora, $\phi_{K,L}(\sum_{i=1}^{m-1} x_i^p \otimes d_K \alpha_i) = \sum_{i=1}^{m-1} x_i^p d_L \alpha_i = 0$, e como L/K é separável, pelo corolário 4.1.2, temos que $\phi_{K,L}$ é injetora; portanto, $\sum_{i=1}^{m-1} x_i^p \otimes d_K \alpha_i = 0$. Logo, dada à escolha de m, temos que $\{x_1^p,\dots, x_{m-1}^p\} \subset L$ é linearmente independente sobre K e, portanto, $d_K \alpha_i = 0$ para $i=1,2,\dots,m$ ([8] p.21); consequentemente, pela observação 2.1.3, $\alpha_i \in K^p$ para $i=1,\dots\dots,m$. Sendo $\beta_1,\beta_2,\dots,\beta_m \in K$ tais que $\beta_m = 1$, $\beta_i^p = \alpha_i$ para $i=1,\dots,m$, temos então que $\sum_{i=1}^{m} \beta_i^p x_i^p = 0$, isto é $\sum_{i=1}^{m} \beta_i x_i = 0$ onde $\beta_m = 1$, o que é absurdo pois $\{x_1,\dots,x_m\}$ é linearmente independente sobre K. Logo, K e $L^p$ são linearmente disjuntos sobre $K^p$.

(c) $\Longrightarrow$ (a). Seja $D: K \longrightarrow M$ uma derivação de K a valores num L-espaço vetorial M. Sendo $\{x_\lambda\}_{\lambda \in \Lambda}$ uma base do $K^p$-espaço vetorial $L^p$, X também é uma base do K-espaço vetorial $K[L^p]$ já que, por hipótese, K e $L^p$ são linearmente disjuntos sobre $K^p$; logo, para cada par $\alpha,\beta \in \Lambda$, temos que

$x_\alpha x_\beta = \sum_\lambda a_{\alpha\beta\lambda} x_\lambda$ onde $(a_{\alpha\beta\lambda})_{\lambda\in\Lambda}$ é uma família quase nula de elementos de $K^p$. Consideremos, agora a aplicação $\bar{D}: K[L^p] \longrightarrow M$ tal que, se $z = \sum_{i=1}^{n} b_i x_i \in K[L^p]$ com $b_i \in K$, $x_i \in X$ para $i=1,\ldots,n$, então $\bar{D}z = \sum_{i=1}^{n} x_i Db_i$; é claro que se $z,y \in K[L^p]$, $\bar{D}(z+y) = \bar{D}z + \bar{D}y$ ;

também, sendo $z = \sum_{i=1}^{n} b_i x_i$ e $y = \sum_{j=1}^{n} c_j x_j$ elementos de $K[L^p]$ , $b_i, c_i \in K$, $x_i \in X$ para $i=1,\ldots,n$, temos que $\bar{D}(zy) = \bar{D}(\sum_{i,j} b_i c_j x_i x_j) =$

$= \bar{D} \sum_{i,j,\lambda} b_i c_j a_{ij\lambda} x_\lambda) = \sum_{i,j,\lambda} D(b_i c_j) a_{ij\lambda} x_\lambda)$ já que $a_{ij\lambda} \in K^p$ para

$i,j=1,\ldots,n, \lambda \in \Lambda$; logo,

$$\bar{D}(zy) = \sum_{i,j,\lambda} b_i D(c_j) a_{ij\lambda} x_\lambda + \sum_{i,j,\lambda} c_j D(b_i) a_{ij\lambda} x_\lambda =$$

$$= \sum_{i,j} b_i D(c_j) x_i x_j + \sum_{i,j} c_j D(b_i) x_i x_j = z\bar{D}y + y\bar{D}z.$$

Temos, portanto, que existe $\bar{D}$, derivação de $K[L^p]$ que estende $D$. Pelo exemplo 1.4.3, sabemos existir uma derivação $\Delta$ de $K(L^p)$ que estende $\bar{D}$. Como $L^p \subset K(L^p)$, o teorema 1.6.2, (b) nos diz que existe uma derivação $\bar{\Delta}$ de $L$ que estende $\Delta$. Logo, existe uma derivação $\bar{\Delta}$ de $L$ que estende $D$, e, portanto, $L/K$ é separável. □

# B I B L I O G R A F I A


[1] ATIYAH, M.F e MACDONALD, I.G. - Introduction to Commutative Algebra, Addison Wesley, Reading (1969).

[2] AZEVEDO, A. - Seminários sobre o "Módulo das Diferenciais" ministrados no Curso de Verão de 1974 no Instituto de Matemática e Estatística.

[3] CARTAN, H. e CHEVALLEY, C. - Géométric Algébrique, Seminaire de E.N.S. (1955-1956), Exposé 13 par **P. CARTIER**, Dérivations dans les Corps, pp. 1-13.

[4] CHUNG, I.Y. - Derivation Modules of Free Joins and m-adic Completions of Algebras, Proc. of the A.M.S. , vol.34, nº 1 (1972), pp.49-56.

[5] DIEUDONNÉ, J.A. - Sur les extensions transcendentes séparables, Summa Brasiliensis Mathematicae, vol. II, fasc. 1 (1947), pp. 1-20.

[6] MAC LANE, S. - Modular Fields I, Separating Transcendence Bases, Duke Math. J. vol. 5 (1939), pp.372-393.

[7] NAKAI, Y. - On the Theory of Differencial in Commutative Rings, J.Math.Soc.Japan, vol.13 nº 1 (1961) pp. 63-84.

[8] NORTHCOTT, D.G. - An Introduction to Homological Algebra, Cambridge at the University Press (1960).

[9] SUZUKI, S. - Differencial of Commutative Rings, Queen's Papers in Pure and Applied Mathematics, nº29 (1971)

[10] VAN DER WAERDEN, B.L. - Algebra Moderna, vol.I, Publicações da Sociedade **Portuguesa** de Matemática, Lisboa, (1956).

[11] ZARISKI, O. e SAMUEL, P. - Commutative Algebra, vol.I, D. Van Nostrand Company, Inc., Princeton, New Jersey, (1958).