SEPARABILIDADE, RAMIFICAÇÃO E DIFERENTE

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida pelo Sr. ANTONIO APARECIDO DE ANDRADE e aprovada pela Comissão Julgadora.

Campinas, 15 de abril de 1988.

Prof. Dr. Antonio Paques
Orientador

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Matemática.

An24s
9463/BC

UNICAMP
BIBLIOTECA CENTRAL

AGRADECIMENTOS

Expresso minha gratidão ao Prof. Dr. Antonio Paques pela exigente e paciente orientação do presente trabalho.

À FAPESP, que, com seu apoio financeiro possibilitou a realização do mesmo.

Aos Professores Paulo R. Brumatti e Francisco Thaine Prada pelo auxílio na compreensão de alguns resultados.

Ao Prof. Hygino Hugueros Domingues pelo constante estímulo em continuar no estudo da Matemática.

À Maria Gorete

Ao Emersom

ÍNDICE

INTRODUÇÃO

O principal objetivo deste trabalho é o de procurar dar uma descrição clara de como as noções de separabilidade, ramificação e diferente se interrelacionam. Este trabalho é apresentado em três capítulos, **a saber:**

1) SEMISIMPLICIDADE E SEPARABILIDADE

Aqui, fazemos, inicialmente, uma rápida revisão da teoria clássica das álgebras semisimples e das álgebras separáveis sobre um corpo, procurando evidenciar como a noção de separabilidade é uma extensão natural da noção de semisimplicidade. Apresentamos os teoremas de Wedderburn para álgebras semisimples e álgebras separáveis, além de alguns teoremas que fornecem propriedades - definição das álgebras separáveis sobre corpos, buscando mostrar que algumas delas são naturalmente extensíveis ao caso de um anel comutativo. Concluímos o capítulo com um estudo da caracterização de separabilidade via derivação.

2) ÁLGEBRAS SEPARÁVEIS

O nosso intuito neste capítulo é os resultados básicos de uma teoria geral de álgebras sobre anéis comutativos.

No primeiro parágrafo damos a definição de separabilidade sobre um anel comutativo e apresentamos uma razoável lista de

exemplos. No segundo parágrafo tratamos das propriedades básicas de álgebras separáveis. Os resultados aí apresentados mostram que uma considerável porção da teoria clássica é preservada nesta extensão da noção de separabilidade para anéis. Por exemplo, é provado que separabilidade é mantida via produto tensorial, soma direta e extensão de escalares, que separabilidade é transitiva e que uma álgebra A é separável sobre um anel R se, e somente se, A é separável sobre seu centro Z(A) e Z(A) é separável sobre R.

3) SEPARABILIDADE, RAMIFICAÇÃO E DIFERENTE

Neste capítulo introduzimos a noção de ramificação e diferente, apresentamos alguns casos onde separabilidade e não-ramificação são equivalentes e concluímos com a demonstração de que, nestes casos, não-ramificação é decidível à partir de condições sobre o diferente.

Incluímos no texto um Apêndice, onde listamos (sem demonstração) resultados básicos de àlgebra comutativa utilizados ao longo dos Capítulo II e III, com o único intuito de facilitar ao leitor o seu acesso aos mesmos.

CAPÍTULO I

SEMISIMPLICIDADE E SEPARALIDADE

Neste capítulo trataremos do estudo e caracterização das álgebras semisimples (§1) e separáveis sobre corpos (§§2 e 3). Em todo o capítulo nos restringimos somente às álgebras de dimensão finita sobre um corpo, embora os resultados aqui listados para álgebras semisimples sejam válidas dentro do contexto, obviamente mais geral, de anéis artinianos.

Em todo este capítulo, salvo menção contrária, a letra K denotará um corpo. Por álgebra de dimensão finita sobre um corpo K entendemos uma K-álgebra que como K-espaço vetorial é de dimensão finita. Toda álgebra considerada neste e nos demais capítulos é associativa, com elemento identidade e não necessariamente comutativa. Todo módulo é unitário e todo homomorfismo de álgebras leva elemento identidade em elemento identidade.

§1. SEMISIMPLICIDADE

(1.1) DEFINIÇÃO: Seja A uma K-álgebra. Um elemento $a \in A$ é dito *nilpotente* se existe um inteiro $m \geq 1$ tal que $a^m = 0$. Um ideal I de A é dito *nilpotente* se existe um inteiro $m \geq 1$ tal que $I^m = 0$. Neste caso, o menor inteiro $m \geq 1$ tal que $I^m = 0$ é chamado *índice de nilpotência de* I.

Evidentemente, dizer que $I^m = 0$ equivale a dizer que o

produto de quaisquer m elementos de I é zero. Portanto, se I é nilpotente segue-se que todos os elementos de I são nilpotentes. Reciprocamente, temos o seguinte:

(1.2) PROPOSIÇÃO: Sejam A uma K-álgebra de dimensão finita n e I um ideal lateral de A. Se todo elemento de I é nilpotente, então I é nilpotente e seu índice de nilpotência é no máximo n.

DEMONSTRAÇÃO: Suponhamos que I seja um ideal à esquerda de A cujos elementos são nilpotentes. Sejam $a_1,\ldots,a_{n+1} \in I$ e consideremos a seguinte cadeia de subespaços de A

$$I \supseteq Ia_{n+1} \supseteq Ia_n a_{n+1} \supseteq \cdots \supseteq Ia_1 \cdots a_{n+1} .$$

Como $\dim_K A = n$ temos que $I = Ia_{n+1}$ ou existe $2 \leq i \leq n+1$ tal que $Ia_i \cdots a_{n+1} = Ia_{i-1} \cdots a_{n+1}$. Em ambos os casos, podemos afirmar que para algum s, $1 \leq s \leq n+1$, existe $b \in I$ tal que $a_s \cdots a_{n+1} = ba_s \cdots a_{n+1}$. Multiplicando à esquerda por potências de b, obtemos $a_s \cdots a_{n+1} = b^t a_s \cdots a_{n+1}$ para todo $t \geq 1$. Daí resulta que $a_s \cdots a_{n+1} = 0$, pois por hipótese b é nilpotente e consequentemente $a_1 a_2 \cdots\cdots a_{n+1} = 0$. Como estes são n+1 elementos arbitrários de I, concluímos que $I^{n+1} = 0$. ∎

(1.3) PROPOSIÇÃO: Sejam A uma K-álgebra e N(A) a soma de todos os ideais (bilaterais) nilpotentes de A. Então:

1) $N(A)$ é um ideal (bilateral) de A que contém todos os ideais laterais (à esquerda e à direita) nilpotentes de A.

2) Se A for de dimensão finita sobre K então $N(A)$ é o maior ideal nilpotente de A.

3) Se A for comutativa então $N(A) = \{a \in A : a \text{ é nilpotente}\}$.

DEMONSTRAÇÃO:

1) Claramente $N(A)$ é um ideal bilateral de A. Sejam I um ideal lateral à esquerda nilpotente de A e m um inteiro ≥ 1 tal que $I^m = 0$. Então o ideal bilateral IA satisfaz:

$$(IA)^m = (IA)(IA) \ldots (IA) = I(AI)(AI)\ldots(AI)A = I^m A = 0.$$

Portanto $I \subset IA \subset N(A)$. O mesmo raciocínio se aplica ao caso de um ideal lateral à direita.

2) Mostremos inicialmente que a soma $I+J$ de dois ideais bilaterais I e J nilpotentes é nilpotente. De fato, se $I^n = 0$ e $J^m = 0$ então $(I+J)^m \subset I$ e, consequentemente $(I+J)^{mn} \subset I^n = 0$. Usando indução, podemos afirmar que a soma finita de ideais (bilaterais) nilpotentes é nilpotente. Agora, como todo elemento de $N(A)$ está contido em alguma soma finita de ideais (bilaterais) nilpotentes, concluímos que todo elemento de $N(A)$ é nilpotente. Decorre, então, da Proposição 1.2 que $N(A)$ é nilpotente. Por 1) concluímos que $N(A)$ é o maior ideal nilpotente de A.

3) Já vimos em 2) que $N(A) \subset \{a \in A : a \text{ é nilpotente}\}$. Se

A é comutativa então todo elemento nilpotente a de A gera um ideal nilpotente Aa e portanto $a \in Aa \subset N(A)$. ∎

(1.4) DEFINIÇÃO: Seja A uma K-álgebra. O ideal N(A) de A é chamado *radical* de A.

Vimos na proposição acima que $N(A) \subset \{a \in A : a$ é nilpotente$\}$. **Além disso, se A não é** comutativa essa inclusão é própria. Para ver isto basta considerar $A = M_2(K)$ = álgebra das matrizes 2×2, a coeficientes em K. Neste caso N(A) = 0 (cf. proposição 1.9) e a matriz $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ é nilpotente.

Damos, a seguir, uma melhor descrição dos elementos de N(A).

(1.5) DEFINIÇÃO: Sejam A uma K-álgebra e $a \in A$. Dizemos que a é *propriamente nilpotente* se ax (consequentemente xa) é nilpotente para todo $x \in A$.

Evidentemente todo elemento propriamente nilpotente é nilpotente pois a = a.1 é nilpotente. A recíproca, contudo, não é verdadeira. Basta tomar $A = M_2(K)$ e $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Claramente a é nilpotente e se tomarmos $b = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ obtemos $ab = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ que não é nilpotente.

(1.6) PROPOSIÇÃO: Se A é uma K-álgebra de dimensão finita, então $N(A) = \{a \in A : a$ é propriamente nilpotente$\}$.

DEMONSTRAÇÃO: Se $a \in A$ é propriamente nilpotente então Aa é nilpotente (cf. Proposição 1.2) e daí $a \in Aa \subset N(A)$. Por outro lado, se $a \in N(A)$ então $xa \in N(A)$ para todo $x \in A$. Logo xa é nilpotente para todo $x \in A$, ou seja, a é propriamente nilpotente. ∎

(1.7) DEFINIÇÃO: Seja A uma K-álgebra de dimensão finita. Dizemos que A é *semisimples* se $N(A) = 0$, ou seja, A não possui ideais laterais nilpotentes.

Notemos que toda K-álgebra de dimensão finita sem elementos nilpotentes não nulos é semisimples. A recíproca também vale se a álgebra for comutativa.

(1.8) EXEMPLOS:

1) Todo corpo extensão finita de K ou, mais geralmente, toda K-álgebra com divisão e de dimensão finita é semisimples.

2) Toda soma direta $A_1 \oplus \ldots \oplus A_n$ de K-álgebras com divisão e de dimensão finita sobre K é semisimples.

3) Seja $f \in K[x]$, onde $f = p_1^{e_1} \ldots p_n^{e_n}$ com p_i polinômios irredutíveis em $K[x]$. Então $A = K[x]/_{\langle f \rangle}$ é semisimples se,e somente se, $e_i = 1$ $(i = 1,\ldots,n)$. Ou seja, A é semisimples se, e somente se, f é separável.

DEMONSTRAÇÃO: Seja a aplicação $\varphi: A \longrightarrow K[x]/_{\langle p_1^{e_1}\rangle} \oplus \ldots \oplus K[x]/_{\langle p_n^{e_n}\rangle}$ definida por $\varphi(\bar{g}) = g + \langle p_1^{e_1}\rangle + \ldots + g + \langle p_n^{e_n}\rangle$ onde $\bar{g} = g + \langle f \rangle$ com $g \in K[x]$. Temos que φ é um isomorfismo pois é claramente um homomorfismo de K-álgebras injetor e as álgebras A e $K[x]/_{\langle p_1^{e_1}\rangle} \oplus \ldots \oplus K[x]/_{\langle p_n^{e_n}\rangle}$ têm mesma dimensão como K-espaços vetoriais. Também temos que $N(A) = \langle p_1\rangle/_{\langle p_1^{e_1}\rangle} \oplus \ldots \oplus \langle p_n\rangle/_{\langle p_n^{e_n}\rangle}$.

Daí $N(A) = 0$ se, e somente se, $\langle p_i\rangle/_{\langle p_i^{e_i}\rangle} = 0$ $(i = 1,\ldots,n)$ e, neste caso, $\langle p_i\rangle = \langle p_i^{e_i}\rangle$ ou $e_i = 1$ (pois p_i é irredutível) $\forall i = 1,\ldots,n$. ∎

4) Sejam K um corpo, G um grupo finito. Se a característica de K (car(K)) não divide a ordem de G (o(G)), então K[G] é uma K-álgebra semisimples.

DEMONSTRAÇÃO: Sejam $g_1 = 1, g_2, \ldots, g_n$ os elementos de G. Se $a = \sum_{i=1}^{n} \alpha_i g_i \in K[G]$ podemos escrever $L_a = \sum_{i=1}^{n} \alpha_i L_{g_i}$ onde para cada $x \in K[G]$, L_x é a multiplicação a direita por x. Sejam $M_a, M_{g_1}, \ldots, M_{g_n}$ as matrizes de $L_a, L_{g_1}, \ldots, L_{g_n}$, respectivamente, com relação a base G. Então $M_a = \sum_{i=1}^{n} \alpha_i M_{g_i}$. Agora, suponhamos que exista $0 \neq a = \sum_{i=1}^{n} \alpha_i g_i \in N(K[G])$. Logo existe i, $1 \leq i \leq n$ tal que $\alpha_i \neq 0$. Podemos supor que $\alpha_1 \neq 0$ pois caso contrário, multiplicando a pelo g_i^{-1} apropriado obtemos o

elemento desejado. Desde que $a \in N(K[G])$, a é nilpotente e consequentemente, M_a é nilpotente. Claramente os autovalores de uma matriz nilpotente são todos nulos e o polinômio característico de M_a é

$$X^n - Tr(M_a)X^{n-1} + \ldots + (-1)^n \det(M_a) ,$$

onde $Tr(M_a)$ indica a soma dos elementos da diagonal principal de M_a. Desde que as raízes do polinômio característico de M_a são os autovalores de M_a, então o coeficiente de X^{n-1} é igual a soma desses autovalores e portanto nulo, ou seja, $Tr(M_a) = 0$. Como $Tr : M_n(K) \longrightarrow K$ é uma aplicação K-linear, temos $0 = Tr(M_a) = Tr(\sum_{i=1}^{n} \alpha_i M_{g_i}) = \sum_{i=1}^{n} \alpha_i Tr(M_{g_i})$. Observemos que $L_{g_i}(g_j) \neq g_j$ $(i \neq 1)$ e $L_1(g_j) = g_j$. Daí $Tr(M_{g_i}) = 0$ $(i \neq 1)$ e $Tr(M_{g_1}) = n$. Portanto $0 = \sum_{i=1}^{n} \alpha_i Tr(M_{g_i}) = \alpha_1 n$. Desde que $\alpha_1 \neq 0$, $n.1 = 0$, ou seja, car(K) divide n o que é um absurdo. Portanto K[G] é semisimples. ∎

5) Toda álgebra de matrizes com coeficientes num corpo extensão finita de K ou numa K-álgebra com divisão e de dimensão finita é semisimples. Mais geralmente, se A é uma K-álgebra semisimples, então $M_n(A)$ é semisimples. Isto segue trivialmente da seguinte proposição:

(1.9) PROPOSIÇÃO: Seja A uma K-álgebra de dimensão finita. Então $M_n(N(A)) = N(M_n(A))$.

DEMONSTRAÇÃO: Desde que $N(A)$ é um ideal de A, é imediato que $M_n(N(A))$ é um ideal de $M_n(A)$, Como $N(A)$ é um ideal nilpotente de A (digamos seja m seu índice de nilpotência) segue que o produto de m elementos de $N(A)$ é nulo. Seja $M \in M_n(N(A))$. Observando que as componentes da matriz M^m são somas finitas de produtos de m elementos de $N(A)$, concluímos que $M^m = 0$. Logo todo elemento de $M_n(N(A))$ é nilpotente e consequentemente o ideal $M_n(N(A))$ é também nilpotente (cf. proposição 1.2). Portanto $M_n(N(A)) \subset N(M_n(A))$.

Reciprocamente, denotando por e_{ij} $(i,j = 1,\ldots,n)$ as matrizes elementares, podemos reescrever todo elemento de $M_n(A)$ na forma $\sum_{i,j=1}^{n} a_{ij}e_{ij}$, com $a_{ij} \in A$. Tomemos um elemento $\sum_{i,j=1}^{n} a_{ij}e_{ij} \in N(M_n(A))$ e vamos mostrar que $a_{ij} \in N(A)$ $(i,j = 1,\ldots,n)$. Recordemos que $e_{ij}e_{k\ell} = \delta_{jk}e_{i\ell}$. Para $k,\ell = 1,\ldots,n$ temos

$$(a_{k\ell}e_{1k})\left(\sum_{i,j=1}^{n} a_{ij}e_{ij}\right)(a_{k\ell}e_{\ell 1}) = \sum_{i,j=1}^{n} a_{k\ell}a_{ij}e_{k\ell}(e_{1k}e_{ij})e_{\ell 1} =$$

$$= \sum_{i,j=1}^{n} a_{k\ell}a_{ij}a_{k\ell}\delta_{ki}e_{ij}e_{\ell 1} = \sum_{i,j=1}^{n} a_{k\ell}a_{ij}a_{k\ell}\delta_{ki}\delta_{j\ell}e_{11} =$$

$$= a_{k\ell}^3 e_{11} \in N(M_n(A)). \text{ Então } a_{k\ell}^3 e_{11} \text{ é nilpotente e portanto } a_{k\ell} \text{ é nilpotente. Agora, como para todo } x \in A \text{ e para todo } \sum_{i,j=1}^{n} a_{ij}e_{ij} \in N(M_n(A)) \text{ temos } \sum_{i,j=1}^{n} (xa_{ij})e_{ij} = x\sum_{i,j=1}^{n} a_{ij}e_{ij} =$$

$= (\sum_{i,j=1}^{n} xe_{ij})(\sum_{i,j=1}^{n} a_{ij}e_{ij})$, segue que xa_{ij} é nilpotente para todo $i,j = 1,\ldots,n$, e portanto a_{ij} são propriamente nilpotentes $(i,j = 1,\ldots,n)$. Daí $a_{ij} \in N(A)$, $i,j=1,\ldots,n$. Isto mostra que $N(M_n(A)) \subset M_n(N(A))$. ∎

No que se segue apresentamos uma série de resultados em que descreveremos propriedades das álgebras semisimples e que são resultados auxiliares à demonstração do Teorema de Wedderburn (Teorema 1.24).

(1.10) LEMA: Seja A uma K-álgebra de dimensão finita e I um ideal à esquerda (ou à direita) não nulo de A. Se I não é nilpotente, então existe $0 \neq e \in I$ tal que $e^2 = e$.

DEMONSTRAÇÃO: Como I é não nilpotente, existe $a \in I$ não nilpotente. Seja então a seguinte sequência $Ia \supseteq Ia^2 \supseteq \ldots$. Como A é de dimensão finita, existe um inteiro $m \geq 1$ tal que $Ia^m = Ia^{m+1} = \ldots$. Sejam $B = Ia^m$ e $b = a^{m+1}$. Então temos que $Bb = Ia^m a^{m+1} = Ia^{2m+1} = Ia^m = B$. Logo existe $e \in B$ tal que $eb = b$ e consequentemente, $(e^2 - e)b = 0$. Seja $\varphi : B \to B$ tal que $\varphi(x) = xb$. É claro que φ é K-linear. Como $Bb = B$, φ é sobre. Como A é de dimensão finita, B é de dimensão finita e daí φ é injetora. Assim, de $0 = (e^2 - e)b = \varphi(e^2 - e)$ obtemos que $e^2 = e$. Notemos que $e \neq 0$ pois caso contrário teríamos $0 = eb = b$ e consequentemente $a^{m+1} = b = 0$ o que contradiz o fato de a não ser nilpotente. Portanto $e \neq 0$ e $e^2 = e$. ∎

(1.11) TEOREMA: Sejam A uma K-álgebra semisimples e I um

ideal à esquerda (resp. à direita) não nulo de A. Então $I = Ae$ (resp. $I = eA$) para algum idempotente não nulo $e \in I$.

DEMONSTRAÇÃO: Seja I um ideal à esquerda não nulo de A. Como A é semisimples, I não é nilpotente e portanto existe $0 \neq e_o \in I$, um elemento idempotente (cf. 1.10). Consideremos o seguinte conjunto

$$an(e_o) = \{b \in I : be_o = 0\}$$

chamado anulador de e_o em I. Claramente $an(e_o)$ é um ideal à esquerda de A. Suponhamos $an(e_o) \neq 0$. Desde que A é semisimples, $an(e_o)$ não é nilpotente e portanto existe um idempotente $0 \neq e_1 \in an(e_o)$. Seja $f_o = e_o + e_1 - e_oe_1 \in I$. Temos que $f_o \neq 0$ pois caso contrário $0 = f_oe_o = e_o^2 + e_1e_o - e_oe_1e_o = e_o^2 = e_o$ o que é um absurdo. Também $f_o^2 = f_o$. Para cada $b \in I$ tal que $bf_o = 0$ temos que $0 = (bf_oe_o)e_o = b(f_oe_o) = be_o$ o que significa que $b \in an(e_o)$ e portanto $an(f_o) \subset an(e_o)$. Além disso, desde que $e_1f_o = e_1$ então $e_1 \notin an(f_o)$ e portanto $an(f_o) \underset{+}{\subset} an(e_o)$. Daí, se $an(f_o) \neq 0$ repetimos o mesmo raciocínio e obtemos a seguinte sequência

$$an(e_o) \underset{+}{\supset} an(f_o) \underset{+}{\supset} an(g_o) \underset{+}{\supset} \ldots$$

onde $e_o, f_o, g_o, \ldots$ são idempotentes não nulos de I. Desde que A é de dimensão finita, este processo pára em um número finito de etapas. Portanto podemos afirmar que existe $0 \neq e \in I$ tal

que $e^2 = e$ e $an(e) = 0$. Para todo $b \in I$, temos $(b - be)e = 0$ o que acarreta que $b = be$. Daí $Ae \subset I \subset Ae$ e portanto $I = Ae$.

Por um raciocínio análogo mostra-se que $I = eA$ no caso em que I é um ideal lateral à direita. ∎

(1.12) COROLÁRIO: Sejam A uma K-álgebra semisimples e I um ideal não nulo de A. Então $I = Ae = eA$ para algum idempotente não nulo $e \in I$ e central em A. Em particular, I é uma K-álgebra com elemento idempotente e.

DEMONSTRAÇÃO: A demonstração do teorema nos assegura que existem idempotentes $e_1, e_2 \in I$ não nulos tais que $e_1 b = b = be_2$ para todo $b \in I$. Em particular, $e_1 = e_1 e_2 = e_2$. Logo $e_1 = e_2 = e$ é o elemento identidade da multiplicação de I. Mais ainda $I = Ae = eA$. Resta mostrar que e é central em A, ou seja, $ae = ea$ para todo $a \in A$. Notemos que $ea, ae \in I$ para todo $a \in A$. Logo $ae = e(ae) = (ea)e = ea$ para todo $a \in A$. ∎

Vimos nesse corolário, que se I é um ideal não nulo de uma K-álgebra semisimples, então I também é uma K-álgebra com elemento identidade central em A. A proposição seguinte nos assegura que I é, além disso, uma K-álgebra semisimples.

(1.13) PROPOSIÇÃO: Sejam A uma K-álgebra e I um ideal não nulo de A. Se A é semisimples, então I é uma K-álgebra semisimples.

DEMONSTRAÇÃO: É suficiente mostrar que $N(I) = 0$. Para isso

mostremos que $N(I) = N(A) \cap I$. Notemos que $N(A) \cap I$ é um ideal de I. Como N(A) é nilpotente, todo elemento de N(A) é nilpotente. Logo todo elemento de $N(A) \cap I$ é nilpotente. Então $N(A) \cap I$ é nilpotente e, consequentemente $N(A) \cap I \subset N(I)$. Também N(I) é nilpotente (cf. proposição 1.2), então existe um inteiro $m \geq 1$ tal que $N(I)^m = 0$. Então para todo $a \in N(I)$ temos $(Aa)^{2m} = ((AaA)a)^m \subseteq (N(I)a)^m \subseteq N(I)^m = 0$. Portanto para todo $a \in N(I)$ temos $(xa)^{2m} = 0$ para todo $x \in A$, o que significa que todo elemento de N(I) é propriamente nilpotente. Isto implica que $N(I) \subset N(A) \cap I$ (cf. Prop. 1.6). Portanto $N(I) = N(A) \cap I$ e consequentemente, considerando que A seja semisimples, N(I) = 0, ou seja, I é uma K-álgebra semisimples. ∎

(1.14) DEFINIÇÃO: Seja A uma K-álgebra. Dizemos que A é *simples* se os únicos ideais de A são os triviais, isto é, {0} e A.

Notemos que toda K-álgebra de dimensão finita simples é semisimples. Com efeito, seja A uma K-álgebra simples e consideremos N(A). Logo N(A) = 0 ou N(A) = A. Se N(A) = A então $1 \in N(A)$ que é um absurdo. Logo N(A) = 0, ou seja, A é semisimples.

(1.15) EXEMPLO: A álgebra $M_n(D)$ das matrizes $n \times n$ ($n \geq 1$) a coeficientes em D onde, D é uma K-álgebra com divisão é simples.

DEMONSTRAÇÃO: Sejam I um ideal não nulo de $M_n(D)$ e $0 \neq x \in I$. Denotando por e_{ij} $(i,j = 1,\ldots,n)$ as matrizes elementares,

podemos escrever $x = \sum_{i,j=1}^{n} a_{ij}e_{ij}$ com $a_{ij} \in D$ e $a_{k\ell} \neq 0$ para algum k e algum ℓ. Como I é ideal, $y = \sum_{r=1}^{n} e_{rk}x e_{\ell r}$

$$= \sum_{r=1}^{n} e_{rk}\Big(\sum_{i,j=1}^{n} a_{ij}e_{ij}\Big)e_{\ell r} = \sum_{k=1}^{n}\sum_{i,j=1}^{n} a_{ij}(e_{rk}e_{ij})e_{\ell r} =$$

$$= \sum_{r=1}^{n}\sum_{i,j=1}^{n} a_{ij}\delta_{ki}e_{rj}e_{\ell r} = \sum_{r=1}^{n}\sum_{i,j=1}^{n} a_{ij}\delta_{ki}\delta_{j\ell}e_{rr} = \sum_{r=1}^{n} a_{k\ell}e_{rr} =$$

$= a_{k\ell}I_n \in I$. Desde que $a_{k\ell} \neq 0$, y é inversível e $y^{-1} = a_{k\ell}^{-1}I_n$. Portanto $I_n = yy^{-1} \in I$ e consequentemente $I = M_n(D)$. ∎

Nosso objetivo a seguir é mostrar o seguinte teorema:

(1.16) TEOREMA: Toda K-álgebra semisimples é uma soma direta finita de K-álgebras simples.

A demonstração deste teorema é uma consequência imediata dos seguintes lemas:

(1.17) LEMA: Sejam A uma K-álgebra semisimples e I um ideal não nulo de A. Se I é minimal então I é uma K-álgebra simples.

DEMONSTRAÇÃO: Desde que I é uma K-álgebra, resta mostrar que os únicos ideais de I são os triviais. Seja J um ideal não nulo de I e consideremos o ideal IJI de A que está contido em I. Se $IJI = 0$ então $J^3 \subset IJI = 0$, ou seja, $J^3 = 0$ que é um absurdo pois I é semisimples (cf. 1.13). Logo $IJI \neq 0$ e da minimalidade de I segue-se que $I = IJI \subset J \subset I$, ou seja,

$J = I$. Portanto I é uma K-álgebra simples. ∎

(1.18) LEMA: Sejam A uma K-álgebra semisimples e $I_1,\ldots,I_n$ ideais minimais de A distintos. Então a soma $I_1 + \ldots + I_n$ é direta. Em particular, A contém apenas um número finito de ideais minimais.

DEMONSTRAÇÃO: Já vimos que existem idempotentes não nulos e centrais $e_1,\ldots,e_n$ de A tais que $I_i = e_iA = Ae_i$ $(i = 1,\ldots,n)$. Mostremos que esses idempotentes são ortogonais dois a dois, isto é, $e_ie_j = 0$ $(i \neq j)$. Com efeito, se $e_ie_j \neq 0$ para algum i e algum $j \neq i$, teríamos $0 \neq e_ie_j \in I_i \cap I_j$, ou seja $I_i \cap I_j \neq 0$. Da minimalidade de I_i e I_j temos que $I_i = I_i \cap I_j = I_j$ contradizendo nossa hipótese.

Suponhamos, agora, que $a_1e_1 + \ldots + a_ne_n = 0$ $(a_i \in A)$. Multiplicando por e_i à direita obtemos $a_ie_i = a_ie_i^2 = 0$ $(i=1,\ldots,n)$. Logo a soma $I_1 + \ldots + I_n$ é direta. Finalmente, desde que A é de dimensão finita e $\dim(I_1 + \ldots + I_n) = \dim I_1 + \ldots + \dim I_n$ é fácil ver que A só pode ter um número finito de ideais minimais. ∎

(1.19) LEMA: Seja A uma K-álgebra semisimples. Se $I_1,\ldots,I_n$ são todos os ideais minimais de A, então $A = I_1 \oplus \ldots \oplus I_n$.

DEMONSTRAÇÃO: Resta apenas mostrar que $A \subset I_1 + \ldots + I_n$. Como antes, existem idempotentes não nulos centrais e ortogonais dois a dois $e_1,\ldots,e_n$ tais que $I_i = Ae_i = e_iA$ $(i = 1,\ldots,n)$.

Seja $e = e_1 + \ldots + e_n$. Claramente e é idempotente central em A, e além disso $e_i e = e_i$ $(i = 1,\ldots,n)$. Afirmamos que $e = 1$, a identidade de A. Com efeito, se $e \neq 1$ então $J = (1 - e)A = A(1 - e)$ é um ideal não nulo de A. Esse ideal J contém um dos ideais minimais de A, digamos, I_k para algum $1 \leq k \leq n$. Assim, podemos escrever $e_k = (1 - e)a$ para algum $a \in A$, e consequentemente temos $e_k = e_k^2 = e_k(1 - e)a = 0$ (pois $e_k e = e_k$) o que é uma contradição. Portanto $e = 1$ e $a = a.1 = a.e = ae_1 + \ldots + ae_n \in I_1 + \ldots + I_n$ para todo $a \in A$, ou seja, $A \subset I_1 + \ldots + I_n$. ∎

(1.20) TEOREMA (de Wedderburn para álgebras simples): Se A é uma K-álgebra simples então A é isomorfa à álgebra $D_n = M_n(D)$ das matrizes $n \times n$, para algum inteiro $n \geq 1$, a coeficientes em uma K-álgebra com divisão D. O inteiro n e a álgebra D são unicamente determinados por A.

Antes de demonstrarmos este teorema recordaremos a seguinte definição:

(1.21) DEFINIÇÃO: Sejam A um anel não necessariamente comutativo (em particular uma K-álgebra) e M um A-módulo à esquerda (ou à direita) não nulo. Dizemos que M é um A-módulo à *esquerda* (ou à *direita*) *simples* se os únicos submódulos de M são $\{0\}$ e M.

DEMONSTRAÇÃO DO TEOREMA: Seja M um ideal à esquerda minimal de A. Tal M existe pois A é um K-espaço vetorial de dimensão

finita. Obviamente M é um A-módulo à esquerda simples e claramente $D = End_A(M)$ é uma K-álgebra com divisão. Consideremos M como um D-módulo à esquerda via a ação $d.m = d(m)$ para todo $m \in M$ e para todo $d \in D$. Consideremos também para todo $a \in A$, a aplicação $\ell_a : M \longrightarrow M$, $x \longrightarrow ax$. Pode-se ver facilmente que $\ell_a \in End_D(M)$, para todo $a \in A$, assim como a aplicação $i : A \longrightarrow End_D(M)$, $a \longrightarrow \ell_a$, é um homomorfismo de K-álgebras, obviamente injetor pois A é simples. Verifiquemos que i é também sobrejetor. Para todo $y \in M$, a aplicação $r_y : M \longrightarrow M$, $x \longrightarrow xy$, é claramente um elemento de D. Logo $f(xy) = f(x)y$, para todo $x,y \in M$ e para todo $f \in End_D(M)$.

Afirmamos que $i(M)$ é um ideal à esquerda em $End_D(M)$. De fato, pois temos $f.i(x)(y) = f(xy) = f(x)y = i(f(x))(y)$, para todo $x,y \in M$ e para todo $f \in End_D(M)$ e, consequentemente, $f.i(x) = i(f(x)) \in i(M)$ para todo $f \in End_D(M)$.

Agora, como A é simples, temos $A = MA$ e, por conseguinte, $i(A) = i(MA) = i(M)i(A)$ é um ideal à esquerda de $End_D(M)$. Como $id_M = i(1_A) \in i(A)$ segue-se que $i(A) = End_D(M)$, ou seja, i é sobrejetor. Finalmente, como A é de dimensão finita sobre K então a dimensão de M como D-espaço vetorial à esquerda é também finita (digamos n) e, naturalmente $End_D(M) \simeq M_n(D)$.

A segunda parte deste teorema decorre do Lema 1.23 abaixo:

(1.22) LEMA: Seja D uma K-álgebra com divisão e $D_n = M_n(D)$. Então:

1) Os ideais $L_i = \{\sum_j a_j e_{ij} : a_j \in D\}$, $1 \leq i \leq n$, de matrizes coluna são ideais à esquerda minimais de D_n e $D_n = L_1 \oplus \ldots \oplus L_n$.

2) Todos os D_n-módulos à esquerda simples, em particular todos os ideais à esquerda minimais de A, são isomorfos.

DEMONSTRAÇÃO:

1) Claramente $D_n = L_1 \oplus \ldots \oplus L_n$. Se $x = \sum_j a_j e_{ij} \in L_i$, com $a_k \neq 0$ para algum $1 \leq k \leq n$, então $(a_k^{-1} e_{ki})x = e_{ki} \in L_i$. Disto segue-se que o ideal à esquerda gerado por qualquer elemento não nulo de L_i é L_i. Portanto L_i é minimal.

2) Obviamente os L_i são isomorfos como D_n-módulos à esquerda. Seja N um D_n-módulo à esquerda simples. Desde que $A = L_1 \oplus \ldots \oplus L_n$ e $AN = N$, existe $1 \leq i \leq n$ tal que $\{0\} \subset L_i N \subset N$ e, consequentemente, $L_i N = N$. A aplicação $L_i \longrightarrow N$, $y \longrightarrow yx$, não é nula para algum $x \in N$ e é, claramente, um homomorfismo de D_n-módulos. Desde que L_i e N são simples, esta aplicação é um isomorfismo. ∎

(1.23) LEMA: Se D e D' são K-álgebras com divisão tais que as correspondentes álgebras de matrizes D_n e D'_n, são isomorfas, então D e D' são isomorfas e $n = n'$.

DEMONSTRAÇÃO: Para mostrar que $D \simeq D'$ é suficiente mostrar que para todo D_n-módulo à esquerda simples N, existe um isomorfismo de K-álgebras $D \simeq \mathrm{End}_{D_n}(N)$. Desde que quaisquer dois D_n-módulos

à esquerda simples são isomorfos (cf. lema 1.22), podemos tomar $N = D^n = \{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in D\}$. Além disso $N = D^n$ é também um D-módulo à direita, o que nos permite considerar a aplicação $\varphi : D \longrightarrow End_{D_n}(D^n)$ dada por $\varphi(d) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 d \\ \vdots \\ x_n d \end{pmatrix}$ para todo $d, x_1, \ldots, x_n \in D$. Obviamente, φ é um homomorfismo de K-álgebras. Além disso φ é injetor pois D é um anel com divisão. Para mostrar que φ é sobrejetor tomamos $f \in End_{D_n}(D^n)$ e escrevemos $f(e_1) = e_1\lambda_1 + \ldots + e_n\lambda_n$, com $\lambda_i \in D$, onde $\{e_1, \ldots, e_n\}$ é a base canônica de D^n sobre D. Das equações $f(e_1) = f(e_{11}e_1) = e_{11}f(e_1) = e_1\lambda_1$ e $f(e_j) = f(e_{j1}e_1) = e_{j1}\lambda_1$, $2 \leq j \leq n$, segue-se que $\varphi(\lambda_1) = f$ e portanto φ é sobrejetor. Desde que $D \simeq D'$ então $n^2 = \dim_D D^n = \dim_{D'} D'^n = n'^2$ e, consequentemente $n = n'$. ∎

(1.24) TEOREMA (de Wedderburn para álgebras semisimples): Se A é uma K-álgebra semisimples então A é isomorfa a uma soma direta finita $D_{n_1}^{(1)} \oplus \ldots \oplus D_{n_r}^{(r)}$ onde $D_{n_i}^{(i)} = M_{n_i}(D^{(i)})$ (i=1,...,n) é álgebra de matrizes $n_i \times n_i$ a coeficientes em $D^{(i)}$ e cada $D^{(i)}$ é uma K-álgebra com divisão e de dimensão finita sobre K.

DEMONSTRAÇÃO: Decorre trivialmente dos teoremas 1.16 e 1.20. ∎

(1.25) COROLÁRIO: Seja A uma K-álgebra comutativa. Então A é

semisimples se, e somente se, $A \simeq F_1 \oplus \ldots \oplus F_r$, onde cada F_i é um corpo extensão finita de K.

Encerramos este parágrafo com um teorema-definição para álgebras semisimples e que nos será bastante útil no parágrafo seguinte.

(1.26) TEOREMA: Seja A uma K-álgebra de dimensão finita. Então são equivalentes as seguintes afirmações:

1) A é semisimples

2) A é soma direta finita de ideais à esquerda minimais

3) Todo A-módulo à esquerda é uma soma de submódulos simples

4) Todo A-módulo à esquerda é uma soma direta de submódulos simples.

5) Todo submódulo de um A-módulo à esquerda M é somando direto de M.

6) Toda sequência exata de A-módulos à esquerda
$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ cinde .

7) Todo ideal à esquerda de A é um somando direto de A como A-módulo à esquerda.

8) A não contém ideais laterais nilpotentes.

DEMONSTRAÇÃO:

(1) $\Longrightarrow$ (2) Decorre dos teoremas 1.16 e 1.20 e do lema 1.22.

(2) $\Longrightarrow$ (3) Seja M um A-módulo à esquerda. Desde que $A = Ae_1 \oplus \ldots \oplus Ae_n$ onde Ae_i são ideais à esquerda minimais, $e_i \neq 0$ e $e_i^2 = e_i$ $(i = 1,\ldots,n)$, temos que $M = \sum_{x\in M} \sum_{i=1}^{n} Ae_i x$. Para cada $i=1,\ldots,n$ e para cada $x \in M$, seja $f: Ae_i \longrightarrow Ae_i x$ a aplicação A-linear dada por $f_i(ae_i) = ae_i x$. Claramente f_i $(i = 1,\ldots,n)$ é sobrejetora. Como $Ker(f_i)$ $(i = 1,\ldots,n)$ é um ideal à esquerda de A contido em Ae_i e Ae_i $(i = 1,\ldots,n)$ é minimal obtemos $Ker(f_i) = 0$ ou $Ker(f_i) = Ae_i$ $(i = 1,\ldots,n)$. Daí $Ae_i x \simeq Ae_i$ e portanto é simples ou $Ae_i x = 0$. Isto mostra (3).

(3) $\Longrightarrow$ (4) Seja M um A-módulo à esquerda. Por hipótese M é uma soma de submódulos simples $(N_i)_{i\in I}$. Seja N um submódulo de M e $F = \{L \subset I : N + \sum_{i\in L} N_i$ é direta$\}$. Desde que $\phi \in F$ segue-se que $F \neq \phi$. Notemos que F é ordenado por inclusão e se $L_1 \subset L_2 \subset \ldots$ é uma cadeia de elementos de F então $UL_i \in F$. Portanto o Lema de Zorn nos assegura que F possui um elemento maximal J. Seja $V = N + \sum_{i\in J} N_i$. Como $J \in F$ a soma V é direta. Mostremos que $V = M$. Para todo $i \in J$ temos $N_i \subset V$ e para todo $i \notin J$ a soma $V + N_i$ não é direta pois J é maximal para essa propriedade e consequentemente $V \cap N_i \neq \neq \{0\}$ para todo $i \notin J$. Como N_i é simples obtemos que $V \cap V_i = N_i$, ou seja, $N_i \subset V$. Portanto $M = V$ e isto prova (4), pois basta considerar $N = 0$.

(4) $\Longrightarrow$ (5) Segue-se pelo mesmo raciocínio usado em (3) $\Longrightarrow$ (4).

(5) ==> (6) Seja a sequência exata de A-módulos à esquerda $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$. Logo $f(M')$ é um submódulo de M e, consequentemente, $f(M')$ é um somando direto de M, ou seja, existe H tal que $M = f(M') \oplus H$. Para cada $x'' \in M''$ existe $x \in M$ tal que $g(x) = x''$. Por outro lado existem $y \in f(M') = Ker(g)$ e $z \in H$ únicos tais que $x = y + z$, e portanto $x'' = g(x) = g(y + z) = g(y) + g(z)$, ou seja, para cada $x'' \in M''$ existe um $z \in H$ tal que $g(z) = x''$. É fácil ver que tal $z \in H$ é, de fato, único. Definimos $h: M'' \longrightarrow M$ tal que $h(x'') = z$. Mostremos que h é A-linear. De fato: sejam $x'', y'' \in M''$. Logo existem $z_1, z_2 \in H$ únicos tais que $g(z_1) = x''$, $g(z_2) = y''$ e portanto $g(z_1 + z_2) = x'' + y''$. Se $h(x'' + y'') = z \in H$ então $g(z) = g(z_1 + z_2)$, ou seja, $z - (z_1 + z_2) \in Ker(g) = f(M')$. Então $z - (z_1 + z_2) \in f(M') \cap H = \{0\}$, ou seja, $z = z_1 + z_2$ o que significa que $h(x'' + y'') = h(x'') + h(y'')$. Agora sejam $x'' \in M''$ e $a \in A$. Logo existe $z \in H$ único tal que $g(z) = x''$ e portanto $g(az) = ax''$. Se $h(ax'') = z' \in H$ então $g(z') = g(az)$, ou seja, $z' - az \in Ker(g) = f(M')$ e, consequentemente, $z' - az \in H \cap f(M') = \{0\}$ o que significa que $z' = az$, ou seja, $h(ax'') = ah(x'')$.

Claramente $g \circ h = i f_{M''}$ e portanto a sequência cinde.

(6) ==> (7) Seja I um ideal à esquerda de A e consideremos a sequência exata $0 \longrightarrow I \longrightarrow A \xrightarrow{\pi} A/_I \longrightarrow 0$ de

A-módulos à esquerda. Por (6) esta sequência cinde, ou seja, existe $h : A/_I \longrightarrow A$ tal que $\pi \circ h = id$. Consequentemente $A = I \oplus h(A/_I)$ o que mostra que I é somando direto de A.

(7) $\Rightarrow$ (8) Consideremos $N(A)$ que é um ideal à esquerda de A. Logo existe um ideal à esquerda N' de A tal que $A = N(A) \oplus N'$ como A-módulos à esquerda. Então $1 = x + x'$ com $x \in N(A)$ e $x' \in N'$, e então $x = x^2 + xx'$, donde obtemos $x - x^2 = xx' \in N(A) \cap N' = 0$. Assim $x^2 = x$. Por outro lado, $x \in N(A)$ e portanto x é nilpotente, ou seja, existe um inteiro $n \geq 1$ tal que $x^n = 0$. Então $x = x^2 = x^3 = \ldots = x^n = 0$ e, consequentemente, $x' = 1$ e $N' = A$. Disto segue-se que $N(A) = 0$.

(8) $\Rightarrow$ (1) Por definição. ∎

(1.27) OBSERVAÇÃO: Todo A-módulo à esquerda M" para o qual vale a afirmação (6) do teorema 1.26 é chamado um A-módulo à esquerda projetivo (ver Apêndice **A-1**). Consequentemente, do teorema podemos concluir que uma K-álgebra A de dimensão finita é semisimples se, e somente se, todo A-módulo à esquerda é projetivo.

§2. SEMISIMPLICIDADE E SEPARABILIDADE

Sejam K um corpo de $car(K) = p$, p primo, e L um corpo extensão finita e inseparável de K. Logo existe $\alpha \in L$ tal que α não é separável sobre K. Se $f \in K[x]$ é o polinômio minimal de α sobre K e f' denota a derivada formal de f, então $f'(\alpha) = 0$ e, **por conseguinte, f divide f'** em $K[x]$, o que implica que f' é identicamente nulo. Disto decorre que $f = \sum_{i=0}^{n} a_i X^{ip}$, para algum inteiro $n \geq 1$, onde $a_0, a_1, \ldots, a_n \in K$ e $a_n = 1$. Seja $E = K(a_0^{1/p}, \ldots, a_{n-1}^{1/p})$ e consideremos $\beta = \alpha^n \otimes 1 + \alpha^{n-1} \otimes a_{n-1}^{1/p} + \ldots + 1 \otimes a_0^{1/p} \in L \otimes_K E$. Observemos que $1, \alpha, \ldots, \alpha^n$ são linearmente independentes sobre K, pois caso contrário teríamos $\lambda_0 + \lambda_1 \alpha + \ldots + \lambda_n \alpha^n = 0$ com $\lambda_i \in K$ não todos nulos, o que implicaria que o polinômio f divide o polinômio não nulo $g = \lambda_0 + \lambda_1 X + \ldots + \lambda_n X \in K[x]$ o que é um absurdo. Consequentemente $1 \otimes 1, \ldots, \alpha^n \otimes 1$ são linearmente independentes sobre E e portanto $\beta \neq 0$. Além disso, $\beta^p = (\alpha^n \otimes 1)^p + (\alpha^{n-1} \otimes a_{n-1}^{1/p})^p + \ldots + (1 \otimes a_0^{1/p})^p = \alpha^{np} \otimes 1 + \alpha^{p(n-1)} \otimes a_{n-1} + \ldots + 1 \otimes a_0 = (\alpha^{pn} + a_{n-1}\alpha^{p(n-1)} + \ldots + a_0) \otimes 1 = 0$. Portanto β é um elemento nilpotente não nulo em $L \otimes_K E$, o que implica que $L \otimes_K E$ não é semisimples.

Este exemplo, que acabamos de analisar, mostra que existem

álgebras semisimples cuja semisimplicidade não é preservada por extensão de escalares. Surge aí, naturalmente, a seguinte questão: quais são as álgebras semisimples sobre um corpo K que permanecem semisimples sobre um corpo $L \supset K$, via extensão de escalares? O principal resultado deste parágrafo (o Teorema de Wedderburn para álgebras separáveis) dá uma resposta à essa questão.

(2.1) DEFINIÇÃO: Seja A uma K-álgebra de dimensão finita. Dizemos que A é *separável* sobre K se $A \otimes_K E$ é uma E-álgebra semisimples, para todo corpo E contendo K. Em particular, $A = A \otimes_K K$ deve ser semisimples se A for separável.

(2.2) EXEMPLOS:

1) Seja K um corpo. Então $M_n(K)$ é uma álgebra separável pois para todo corpo E contendo K temos $M_n(K) \otimes_K E \simeq M_n(K \otimes_K E) \simeq M_n(E)$ que é uma E-álgebra semisimples.

2) Sejam K um corpo e G um grupo finito tais que $car(K)$ não divide $o(G)$. Então $K[G]$ é uma álgebra separável pois para todo corpo E contendo K temos $K[G] \otimes_K E \simeq (K \otimes_K E)[G] \simeq E[G]$ que é uma E-álgebra semisimples.

3) Seja $f \in K[x]$, onde K é um corpo e $f = p_1^{e_1}, \ldots, p_n^{e_n}$, com p_i polinômios irredutíveis em $K[x]$. Seja E um corpo extensão de K. Sabemos que $K[x]/_{\langle f \rangle} \otimes_K E \simeq E[x]/_{\langle f \rangle}$ é uma E-álgebra semisimples se, se somente se, $e_i = 1$ $(i = 1, \ldots, n)$. Assim, $K[x]/_{\langle f \rangle}$ é separável se, e somente se, $e_i = 1$ $(i = 1, \ldots, n)$.

Para a demonstração do Teorema de Wedderburn para álgebras separáveis necessitamos dos seguintes dois resultados auxilia - res.

(2.3) PROPOSIÇÃO: Seja A uma K-álgebra simples com centro $Z(A) = K$ e seja E um corpo extensão de K. Então $A \otimes_K E$ é simples.

DEMONSTRAÇÃO: Seja I um ideal não nulo de $A \otimes_K E$. Basta mostrarmos que I contém um elemento não nulo da forma $a \otimes e$ com $a \in A$ e $e \in E$. Com efeito, se I contém um elemento $a \otimes e$ não nulo com $a \in A$ e $e \in E$, então I contém $(a \otimes e)(1 \otimes E) = a \otimes eE = a \otimes E$. Consequentemente I contém $(A \otimes e)(a \otimes E)(A \otimes 1) = AaA \otimes E$. Como AaA é um ideal não nulo de A e A é simples então $AaA = A$ e portanto $I \supset A \otimes_K E$, ou seja, $I = A \otimes_K E$.

Suponhamos, por absurdo, que I não contém elementos não nulos da forma $a \otimes e$, com $a \in A$ e $e \in E$. Seja, então, $x = \sum_{i=1}^{s} a_i \otimes e_i$ um elemento não nulo de I, com s minimal.

Claramente $s > 1$ e $a_s \neq 0$. Desde que A é simples $Aa_sA = A$ e, por conseguinte, existem elementos $c_i, c_i' \in A$, $1 \leq i \leq t$ tais que $1 = \sum_{i=1}^{t} c_i a_s c_i'$. Portanto temos $\sum_{i=1}^{t} (c_i \otimes 1)x(c_i' \otimes 1) = \sum_{i=1}^{s} a_i' \otimes e_i \in I$, com $a_i' = \sum_{j=1}^{t} c_j a c_j'$, $1 \leq i \leq s-1$ e $a_s' = 1$, o que garante que, podemos assumir, sem perda de generalidade, que $a_s = 1$. Da minimalidade de s, decorre que a_{s-1} e a_s são

linearmente independentes sobre K e, consequentemente, $a_{s-1} \notin$ $\notin Z(A) = K$. Seja $a \in K$ tal que $aa_{s-1} - a_{s-1}a \neq 0$ e consideremos $y = (a \otimes 1)x - x(a \otimes 1) = (aa_1 - a_1a) \otimes e_1 + \ldots +$ $(aa_{s-1} - a_{s-1}a) \otimes e_{s-1}$. Os e_i são linearmente independentes sobre K (também como consequência da minimalidade de s) e a última parcela de y é não nula. Logo, $y \in I$ é não nulo e tem comprimento menor que s, o que contradiz a minimalidade assumida para s. Portanto I deve conter um elemento não nulo da forma $a \otimes e$, o que conclui a demonstração. ∎

(2.4) PROPOSIÇÃO: Seja D uma K-álgebra com divisão de dimensão finita. Seja L o centro de D. **Então L é separável sobre K se, e somente** se, D é separável sobre K.

DEMONSTRAÇÃO: Suponhamos L separável sobre K. Como a dimensão de L sobre K é finita existe $\alpha \in L$ e $f \in K[x]$ (polinômio irredutível de α sobre K) tal que $L = K[\alpha] \simeq K[x]/_{\langle f \rangle}$. Seja E um corpo extensão de K. Então $D \otimes_K E \simeq D \otimes_L (L \otimes_K E)$ e $L \otimes_K E \simeq K[x]/_{\langle f \rangle} \otimes_K E \simeq E[x]/_{\langle f \rangle}$. Seja $f = \prod_{i=1}^{r} f_i$ em $E[x]$, com f_i fatores irredutíveis de f em $E[x]$. **Logo** $L \otimes_K E \simeq$ $\simeq E[x]/_{\langle f \rangle} \simeq E[x]/_{\langle f_1 \rangle} \oplus \ldots \oplus E[x]/_{\langle f_r \rangle}$. Notemos que $L \simeq L \otimes_K K \subset$ $\subset L \otimes_K E \simeq E[x]/_{\langle f \rangle}$. Mostremos que $L \subset E[x]/_{\langle f_i \rangle}$. Sejam $p_i : E[x] \longrightarrow E[x]/_{\langle f_i \rangle}$ $(i=1,\ldots,r)$ as projeções canônicas. Como f_i divide f em $E[x]$ então $\langle f \rangle \subset \mathrm{Ker}(p_i)$ $(i = 1,\ldots,r)$ e portanto existem homomorfismos $\bar{p}_i : E[x]/_{\langle f \rangle} \longrightarrow E[x]/_{\langle f_i \rangle}$ dados por $\bar{p}_i(\bar{g}) = p_i(g)$ para todo $g \in E[x]$. Sejam

$\varphi_i : K[x]/_{\langle f \rangle} \longrightarrow E[x]/_{\langle f_i \rangle}$ $(i=1,\ldots,r)$ as restrições dos $\overline{p}_i$ a $K[x]/_{\langle f \rangle}$. Mostremos que cada φ_i é injetora. Com efeito, se $\overline{g} \in \mathrm{Ker}(\varphi_i)$ então $\varphi_i(\overline{g}) = \overline{0} = p_i(g)$. Então $g \in \langle f_i \rangle$, ou seja, f_i divide g. Se f divide g então $\overline{g} \equiv 0$ em $K[x]/_{\langle f \rangle}$. Se f não divide g então $MDC(f,g) = 1$ em $K[x]$ pois f é irredutível sobre K. Como f_i divide g e f_i divide f em $E[x]$ então f_i divide 1 em $E[x]$ o que é um absurdo pois f_i não é constante. Portanto $\mathrm{Ker}(\varphi_i) = 0$ e φ_i é injetora, ou seja, $L \simeq K[x]/_{\langle f \rangle} \subset E[x]/_{\langle f_i \rangle}$. Como os f_i são irredutíveis sobre E, cada $F_i \simeq E[x]/_{\langle f_i \rangle}$ é um corpo extensão de L. Desde que D é simples com centro L, a proposição anterior nos assegura que $D \otimes_L F_i$ é simples $(r = 1,\ldots,r)$. Logo $D \otimes_K E \simeq D \otimes_L (L \otimes_K E) \simeq D \otimes_L (F_1 \oplus \ldots \oplus F_v) = D \otimes_L F_1 \oplus \ldots \oplus D \otimes_L F_v$ e portanto $D \otimes_K E$ é semisimples.

Reciprocamente, suponhamos que D é separável sobre K e suponhamos por absurdo que L não é separável sobre K. Neste caso, decorre do exemplo dado no início deste parágrafo que é possível encontrar um corpo E extensão de K e um elemento nilpotente e central $\beta \in D \otimes_K E$. Consequentemente o ideal gerado por β em $D \otimes_K E$ é nilpotente; ou seja, $D \otimes_K E$ não é semisimples, o que contradiz a hipótese sobre D. Portanto L é separável sobre K. ∎

(2.5) TEOREMA (de Wedderburn para álgebras separáveis): Se A é uma K-álgebra de dimensão finita. Então A é separável sobre K se, e somente se, $A \simeq M_{n_1}(D_1) \oplus \ldots \oplus M_{n_r}(D_r)$ com D_i K-álgebras com divisão, $\dim_K D_i < \infty$ e $Z(D_i)$ separável sobre K $(i=1,\ldots,r)$.

DEMONSTRAÇÃO: Suponhamos A separável sobre K. Logo A é semisimples. Portanto $A = M_{n_1}(D_1) \oplus \ldots \oplus M_{n_r}(D_r)$ com D_i K-álgebras com divisão e $\dim_K D_i < \infty$. Como A é separável, para todo corpo E contendo K, $A \otimes_K E \simeq M_{n_1}(D_1) \otimes_K E \oplus \ldots \oplus M_{n_r}(D_r) \otimes_K E$ é semisimples, donde segue-se que $M_{n_i}(D_i) \otimes_K E = M_{n_i}(D_i \otimes_K E)$ é semisimples e consequentemente $D_i \otimes_K E$ é semisimples (cf. proposição 1.9). A proposição 2.4 acima nos garante, então, que o centro $Z(D_i)$ de D_i é separável sobre K.

Reciprocamente, suponhamos que $A = M_{n_1}(D_1) \oplus \ldots \oplus M_{n_r}(D_r)$ com D_i K-álgebras com divisão, $\dim_K D_i < \infty$ e $Z(D_i)$ separável sobre K ($i=1,\ldots,r$). Então D_i é separável sobre K (cf. proposição 2.4); ou seja, para todo corpo E contendo K, $D_i \otimes_K E$ é semisimples ($i=1,\ldots,r$), e consequentemente $A \otimes_K E \simeq M_{n_1}(D_1) \otimes_K E \oplus \ldots \oplus M_{n_r}(D_r) \otimes_K E$ é semisimples. Portanto A é separável sobre K. ∎

(2.6) COROLÁRIO: Seja A uma K-álgebra comutativa de dimensão finita. Então A é separável sobre K se, e somente se $A = L_1 \oplus \ldots \oplus L_n$ onde os L_i são corpos extensões finitas e separáveis de K.

Terminaremos este parágrafo apresentando uma caracterização de álgebra separável sobre um corpo que permite a extensão natural dessa noção ao caso de anéis comutativos.

Dada uma K-álgebra A, denotamos por A^o a K-álgebra oposta de A, isto é, $A^o = \{x^o : x \in A\}$ munido das operações:

$x^o + y^o = (x + y)^o$ e $x^o y^o = (yx)^o$. Indiquemos por $A^e = A \otimes_K A^o$ a assim chamada *álgebra envolvente* de A. Podemos ver A como um A^e-módulo à esquerda via a ação: $(x \otimes y^o)a = xay$ para todo $a,x,y \in A$.

A aplicação multiplicação $\phi : A \times A^o \longrightarrow A$ definida por $\phi(x,y^o) = xy$ é obviamente K-bilinear e portanto induz uma aplicação K-linear, também indicada por ϕ, de $A \otimes_K A^o$ em A, dada por $\phi(\sum_{i=1}^{n} x_i \otimes y_i^o) = \sum_{i=1}^{n} x_i y_i$. Esta aplicação ϕ é obviamente sobrejetora, pois para todo $x \in A$, $\phi(x \otimes 1^o) = x$. Além disso para qualquer $a,b,x,y \in A$ temos $\phi((a \otimes b^o)(x \otimes y^o)) =$
$= \phi(ax \otimes (yb)^o) = (ax)(yb) = a(x\,y)b = (a \otimes b^o)(xy) =$
$= (a \otimes b^o)\phi(x \otimes y^o)$ o que mostra que ϕ é também A^e-linear . Portanto temos a seguinte sequência exata de A^e-módulos à esquerda $0 \longrightarrow J(A) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0$ **onde** $J(A) = \mathrm{Ker}(\phi)$.

(2.7) TEOREMA: Seja A uma K-álgebra de dimensão finita. Então A é separável sobre K se, e somente se, a sequência exata de A^e-módulos à esquerda $0 \longrightarrow J(A) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0$ cinde.

Para a demonstração deste teorema necessitamos do seguinte lema.

(2.8) LEMA: Seja A uma K-álgebra de dimensão finita. Então A é separável sobre K se, e somente se, existe um corpo E extensão de K tal que $A \otimes_K E = E_{n_1} \oplus \ldots \oplus E_{n_r}$ onde $E_{n_i} = M_{n_i}(E)$.

DEMONSTRAÇÃO: Suponhamos A separável sobre K. Seja E um corpo algebricamente fechado contendo K. Daí $A \otimes_K E$ é semisimples e portanto $A \otimes_K E \simeq D_{n_1}^{(1)} \oplus \ldots \oplus D_{n_r}^{(r)}$ onde $D^{(i)}$ são álgebras com divisão e de dimensão finita sobre E. Sejam $\dim_K D^{(i)} = m_i < \infty$, i=1,...,r. Assim, para todo $x \in D^{(i)}$, $1, x, \ldots, x^{m_i}$ são linearmente dependentes sobre E, ou seja, existem $a_o, \ldots, a_{m_i} \in E$, não todos nulos, tais que $a_o + a_1 x + \ldots + a_{m_i} x^{m_i} = 0$, o que significa que x é algébrico sobre E, acarretando $x \in E$. Isto mostra que $D^{(i)} \subset E \subset D^{(i)}$, ou seja, $D^i = E$, (i=1,...,r) e portanto $A \otimes_K E \simeq E_{n_1} \oplus \ldots \oplus E_{n_r}$.

Reciprocamente, seja E um corpo extensão de K tal que $A \otimes_K E \simeq E_{n_1} \oplus \ldots \oplus E_{n_r}$. Seja F um corpo arbitrário extensão de K e mostremos que $A \otimes_K F$ é semisimples. Consideremos o corpo $EF = (E \otimes_K F)_M$ para algum ideal maximal M de $E \otimes_K F$. Como $E \simeq E \otimes_K K \subset E \otimes_K F$ e a restrição da aplicação canônica $E \otimes_K F \longrightarrow EF$ à E é injetiva (pois se $0 \neq x \in E$ é tal que $x \otimes 1 \in M$ então $1 \otimes 1 = (x^{-1} \otimes 1)(x \otimes 1) \in M$ o que é um absurdo), consequentemente, EF contém E. Analogamente EF contém F. Agora $A \otimes_K EF \simeq (A \otimes_K E) \otimes_E EF \simeq (E_{n_1} \oplus \ldots \oplus E_{n_r}) \otimes_E EF \simeq E_{n_1} \otimes_E EF \oplus \ldots \oplus E_{n_r} \otimes_E EF \simeq (EF)_{n_1} \oplus \ldots \oplus (EF)_{n_r}$, ou seja, $A \otimes_K EF$ é semisimples. Por outro lado, $A \otimes_K EF \simeq (A \otimes_K F) \otimes_F EF$ e se $A \otimes_K F$ tem um ideal nilpotente não nulo I então $I \otimes_F EF$ é um ideal nilpotente não nulo de $A \otimes_K EF$ o que contradiz a conclusão acima. Portanto $A \otimes_K F$ é semisimples. ∎

DEMONSTRAÇÃO DO TEOREMA: Suponhamos A separável sobre K. Consequentemente A^o é também separável sobre K. Então o lema 2.8 nos garante que existem corpos E e E' contendo K tais que $A \otimes_K E \simeq E_{n_1} \oplus \ldots \oplus E_{n_r}$ e $A^o \otimes_K E' \simeq E'_{m_1} \oplus \ldots \oplus E'_{m_s}$. Consideremos agora o corpo $EE' \simeq (E \otimes_K E')_M$ para algum ideal maximal M de $E \otimes_K E'$. Desde que EE' contém E e E' temos $A \otimes_K EE' \simeq$ $\simeq (A \otimes_K E) \otimes_E EE' \simeq (EE')_{n_1} \oplus \ldots \oplus (EE')_{n_r}$ e $A^o \otimes_K EE' \simeq (A \otimes_K E') \otimes_{E'} EE'$ $\simeq (EE')_{m_1} \oplus \ldots \oplus (EE')_{m_s}$ e, consequentemente $A \otimes_K A^o \otimes_K EE'$ $\simeq (A \otimes_K EE') \otimes_{EE'} (A^o \otimes_K EE') \simeq ((EE')_{n_1} \oplus \ldots \oplus (EE')_{n_r}) \otimes_{EE'} ((EE')_{m_1} \oplus$ $\oplus \ldots\ldots\ldots \ldots \oplus (EE')_{m_s}) \simeq (EE')_{n_1 m_1} \oplus \ldots \oplus (EE')_{n_1 m_s} \oplus \ldots \oplus$ $(EE')_{n_r m_1} \oplus \ldots \oplus (EE')_{n_r m_s}$ e portanto $A^e = A \otimes_K A^o$ é uma K-álgebra separável. Em particular A^e é semisimples e consequentemente toda sequência exata de A^e-módulos à esquerda $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ cinde (cf. Teorema 1.26). Em particular, a sequência exata $0 \longrightarrow J(A) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0$ cinde.

Reciprocamente, suponhamos que a sequência exata de A^e-módulos à esquerda $0 \longrightarrow J(A) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0$ cinde. Mostremos que A é separável sobre K, verificando que $B = A \otimes_K F$ é semisimples para todo corpo F extensão de K. Observemos que $B^e = B \otimes_F B^o \simeq (A \otimes_K F) \otimes_F (A^o \otimes_K F) \simeq (A \otimes_K A^o) \otimes_K F \simeq A^e \otimes_K F$. Denotemos por $\phi' = \phi \otimes 1 : B^e \longrightarrow B$. Como a sequência exata $0 \longrightarrow J(A) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0$ cinde, existe uma aplicação A^e-linear $\varphi : A \longrightarrow A^e$ tal que $\phi \circ \varphi = id_A$. Seja

$\varphi' = \varphi \otimes 1 : B \longrightarrow B^e$. Claramente φ' é B^e-linear tal que $\phi' \circ \varphi' = id_B$. Seja $\varphi'(1) = \sum_{i=1}^{t} x_i \otimes y_i^o$ com $x_i, y_i \in B$. Logo $\sum_{i=1}^{t} x_i y_i = 1$. Para mostrar que B é semisimples, basta verificar que se $N \subset M$ são B-módulos à esquerda então N é somando direto de M (cf. teorema 1.26). Para toda aplicação K-linear $f : M \longrightarrow M$ e para todo $x,y \in B$, definimos $(x \otimes y^o)f$ como sendo a aplicação K-linear de M em M dada por $(x \otimes y^o)(f)(m) = xf(ym)$ para todo $m \in M$. Como M,N são B-módulos e B é uma K-álgebra então M,N são K-espaços vetoriais e consequentemente N é somando direto de M como K-espaços vetoriais. Seja $\pi : M \longrightarrow N$ a projeção canônica e denotamos por $\pi' = \varphi'(1)\pi$. Como $\pi = id_N$ sobre N então para todo $n \in N$ temos que $\pi'(n) = (\sum_{i=1}^{t} x_i \otimes y_i^o)\pi(n) = \sum_{i=1}^{t} x_i \pi(y_i n) = \sum_{i=1}^{t} x_i y_i n = n$. Portanto $\pi'^2 = \pi'$. Finalmente, para cada $b \in B$ e para todo $m \in M$ temos $\pi'(bm) = (1 \otimes b^o)\pi'(m) = (1 \otimes b^o)\varphi'(1)\pi(m) = \varphi'((1 \otimes b^o).1)\pi(m) = \varphi((b \otimes 1^o).1)\pi(m) = (b \otimes 1^o)\varphi'(1)\pi(m) = (b \otimes 1^o)\pi'(m) = b\pi'(m)$, ou seja π' é B-linear. Consequentemente π' é uma projeção B-linear de M em N e portanto N é somando direto de M como B-módulo à esquerda. Isto mostra que B é semisimples. ∎

(2.9) OBSERVAÇÃO: As afirmações:

(i) A sequência exata de A^e-módulos à esquerda $0 \longrightarrow J(A) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0$ cinde.

(ii) A é um A^e-módulo projetivo

são equivalentes (como veremos no próximo capítulo). Assim, considerando o Teorema 2.7, podemos afirmar que uma K-álgebra A é separável se, e somente se, A é um A^e-módulo projetivo.

§3. SEPARABILIDADE E DERIVAÇÃO

Sejam K um corpo e F uma extensão finita de K. Sabemos que F é uma extensão separável de K se, e somente se, cada elemento α de F é raiz simples de seu polinômio minimal (mônico irredutível) $m_\alpha \in K[x]$, se, e somente se, α não é raiz de m'_α, onde m'_α denota a derivada formal de m_α.

O resultado acima nos dá um critério para se decidir sobre a separabilidade de extensões finitas de um dado corpo, via a noção de derivada. O que veremos a seguir, neste parágrafo, é uma generalização do conceito da derivada e consequentemente uma nova formulação do resultado acima. Esta nova formulação nos permitirá a extensão desse resultado as álgebras de dimensão finita sobre corpos.

(3.1) DEFINIÇÃO: Sejam $F \subset L$ extensões do corpo K. Uma K-*derivação* de F em L é uma aplicação K-linear $D : F \longrightarrow L$ tal que $D(xy) = D(x)y + xD(y)$ para todo $x,y \in F$.

(3.2) EXEMPLOS:

1) A aplicação K-linear nula de K em K.

2) Sejam $car(K) = p$, p primo, $a \in K$ tal que $a \notin K^p$ e $F = K[x]/_{(x^p-a)}$. Desde que a derivada usual $d : K[x] \longrightarrow K[x]$

se anula em $(x^p - a)$, ou seja $Ker(d) \supset (x^p - a)$, então ela induz uma K-derivação $D : F \longrightarrow F$ dada por $D\overline{f} = \overline{d}f$. Claramente D é não nula.

(3.3) PROPOSIÇÃO: Sejam $F \subset E \subset L$ extensões de K tal que E é uma extensão finita e separável de F. Então cada K-derivação D de F em L se extende de maneira única a uma K-derivação $\tilde{D}$ de E em L.

DEMONSTRAÇÃO: Desde que $E = F(\alpha)$ para algum $\alpha \in E$ (pois E é extensão finita e separável de F), seja $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ o polinômio minimal de α sobre F. Seja D uma K-derivação de F em L e suponhamos inicialmente que $\tilde{D}$ é a sua extensão a E. Então temos $0 = \tilde{D}(f(\alpha)) = \sum_{i=0}^{n} \tilde{D}(a_i\alpha^i) =$

$= \sum_{i=0}^{n} \tilde{D}(a_i)\alpha^i + \sum_{i=0}^{n} a_i\, i\alpha^{i-1}\, \tilde{D}(\alpha) = \sum_{i=0}^{n} D(a_i)\alpha^i + \sum_{i=0}^{n} a_i\, i\alpha^{i-1}\tilde{D}(\alpha) =$

$= f^D(\alpha) + f'(\alpha)\tilde{D}(\alpha)$, onde $f^D(x) = \sum_{i=1}^{n} D(a_i)x^i$ e $f'(x) =$

$= \sum_{i=1}^{n} a_i\, i x^{i-1}$. Logo, desde que $f'(\alpha) \neq 0$, $\tilde{D}(\alpha) = -f^D(\alpha)/f'(\alpha)$ está completamente determinado por D e de maneira única. Reciprocamente, seja D uma K-derivação de F em L e mostremos que D se extende à uma K-derivação $\tilde{D}$ de E em L. Para tanto é suficiente considerar $\tilde{D}(\alpha) = -f^D(\alpha)/f'(\alpha)$ e definir

$\tilde{D}(\sum_{i=0}^{n-1} b_i\alpha^i) = \sum_{i=0}^{n-1} D(b_i)\alpha^i + \sum_{i=1}^{n-1} b_i\, i\alpha^{i-1}\tilde{D}(\alpha)$, quaisquer que

sejam $b_o,\ldots,b_{n-1} \in F$. Evidentemente $\tilde{D}$ é K-linear de F em L, $\tilde{D}_{|F} = D$ e $\tilde{D}(xy) = \tilde{D}(x)y + x\tilde{D}(y)$ para todo $x,y \in E$. ∎

(3.4) TEOREMA: Seja F uma extensão finita de K. Então F é separável sobre K se, e somente se, toda K-derivação de F em F é nula.

DEMONSTRAÇÃO: Suponhamos inicialmente, que F é separável sobre K e seja D uma K-derivação de F em F. Como $D(1) = D(1.1) = D(1) + D(1) = 2D(1)$ então $D(1) = 0$ e consequentemente, $D(\lambda) = \lambda D(1) = 0$ para todo $\lambda \in K$. Logo D e a aplicação K-linear nula de F em F extendem a derivação nula de K em K, donde segue-se que $D = 0$ (cf. Proposição 3.3). Reciprocamente, se F não é separável sobre K, decorre da teoria de corpos que $car(K) = p$, para algum primo p, e que é sempre possível encontrar um subcorpo E de F, que contém o fecho separável de K em F, satisfazendo $E^p \subsetneq E$ e $[F:E] = p$. Além disso, $F \simeq E[x]/_{(x^p - a)}$ para algum $a \in E \setminus E^p$. De acordo com o exemplo 2) dado em (3.2) concluímos que existe uma E-derivação (e, consequentemente, também K-derivação) não nula $D : F \longrightarrow F$, o que é uma contradição. Portanto F é separável sobre K. ∎

Consideremos, agora, A uma K-álgebra e M um A-bimódulo, isto é, M é um A-módulo à esquerda e à direita e, $(ax)b = a(xb)$ para todo $a,b \in A$. Admitiremos sempre que $\lambda m = m\lambda$ para todo $\lambda \in K$. Uma K-derivação de A em M é uma aplicação K-linear $D : A \longrightarrow M$ tal que $D(ab) = aD(b) + D(a)b$ para todo $a,b \in A$.

(3.5) EXEMPLOS:

1) Toda K-derivação de F em L, onde $F \subset L$ são extensões do corpo K.

2) Para cada $m \in M$, a aplicação $\partial_m : A \longrightarrow M$ dada por $\partial_m(a) = am - ma$ para todo $a \in A$ é uma K-derivação chamada *Derivação interior*. Naturalmente, se A é comutativa e M é um A-módulo (isto é, $ax = xa$ para todo $x \in M$ e para todo $a \in A$) então $\partial_m = 0$ para todo $m \in M$.

3) Seja $\phi : A^e \longrightarrow A$ o homomorfismo de A^e-módulos à esquerda $\phi(\sum_i a_i \otimes b_i^o) = \sum a_i b_i$. Como $J(A) = Ker(\phi)$ é um A^e-módulo à esquerda então J(A) é um A-bimódulo via as ações $ax = (a \otimes 1^o)x$ e $xa = (1 \otimes a^o)x$ para todo $x \in J(A)$. A aplicação $\delta : A \longrightarrow J(A)$ dada por $\delta(a) = a \otimes 1^o - 1 \otimes a^o$, para todo $a \in A$, é uma K-derivação de A. Logo uma K-derivação D de A em algum A-bimódulo M é interior se, e somente, se existe $m \in M$ tal que $D(a) = \delta(a)m$ para todo $a \in A$. Para tanto basta notar que todo A-bimódulo M é um $A \otimes_K A^o$-módulo à esquerda via a ação $(a \otimes b^o)x = axb$ para todo $a,b \in A$ e para todo $x \in M$.

(3.6) OBSERVAÇÕES:

1) O conjunto das K-derivações ($Der_K(A,M)$) de A em M é claramente um K-módulo.

2) Com as mesmas notações dos exemplos anteriores temos que $A\delta(A) = J(A)$. Com efeito, seja $x \in A\delta(A)$. Então $x = \sum_{i=1}^{n} a_i \delta(b_i)$

com $a_i, b_i \in A$. Mas $a_i\delta(b_i) = a_i(b_i \otimes 1^o - 1 \otimes b_i^o) = a_ib_i \otimes 1^o - a_i \otimes b_i^o \in J(A)$, ou seja, $x \in J(A)$. Reciprocamente, seja $x = \sum_{i=0}^{n} a_i \otimes b_i^o \in J(A)$. Então $x = \sum_{i=1}^{n} a_i(1 \otimes b_i^o - b_i \otimes 1^o) = -\sum_{i=1}^{n} a_i\delta(b_i) \in A\delta(A)$.

(3.7) TEOREMA: Seja A uma K-álgebra de dimensão finita. Então A é separável sobre K se, e somente se, toda K-derivação de A (em qualquer A-bimódulo M) é interior.

DEMONSTRAÇÃO: Suponhamos, inicialmente, que A é separável sobre K. Ertão a sequência exata de A^e-módulos à esquerda $0 \longrightarrow J(A) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0$ cinde (cf. teorema 2.7). Logo existe uma aplicação A^e-linear $h : A \longrightarrow A^e$ tal que $\phi \circ h = id_A$. Seja $e = h(1) = \sum_{i=1}^{n} x_i \otimes y_i^o \in A^e$. Claramente $\phi(e) = 1$. Da observação 2) de (3.6) decorre que $J(A)$ é um ideal de A^e gerado por elementos da forma $a \otimes 1^o - a \otimes 1^o$ para todo $a \in A$. Além disso, para todo $a \in A$, $(a \otimes 1^o)e = (a \otimes 1^o)h(1) = h((1 \otimes a^o).1) = (1 \otimes a^o)h(1) = (1 \otimes a^o)e$.

Sejam M um A-bimódulo, $D : A \longrightarrow M$ uma K-derivação e consideremos $m = \sum_{i=1}^{n} x_iD(y_i) \in M$. Então, para todo $a \in A$, temos $am - ma = \sum_{i=1}^{n} ax_iD(y_i) - \sum_{i=1}^{n} x_iD(y_i)a = \sum_{i=1}^{n} ax_iD(y_i) -$

$-\sum_{i=1}^{n} x_i D(y_i a) + D(a)$. Por outro lado, notemos que a aplicação $\varphi : A \times A^o \longrightarrow M$, dada por $\varphi((a,b^o)) = aD(b)$ é K-bilinear e, consequentemente, induz uma aplicação K-linear $\tilde{\varphi} : A \otimes_K A^o \longrightarrow M$ tal que $\tilde{\varphi}(\sum_{i=1}^{n} a_i \otimes b_i^o) = \sum_{i=1}^{n} a_i D(b_i)$. Assim, desde que $(a \otimes 1^o)e = (1 \otimes a^o)e$ ou $\sum_{i=1}^{n} ax_i \otimes y_i^o = \sum_{i=1}^{n} x_i \otimes (y_i a)^o$, obtemos $\tilde{\varphi}(\sum_{i=1}^{n} ax_i \otimes y_i^o) = \tilde{\varphi}(\sum_{i=1}^{n} x_i \otimes (y_i a)^o)$ ou $\sum_{i=1}^{n} ax_i D(y_i) = \sum_{i=1}^{n} x_i D(y_i a)$ e consequentemente $am - ma = \sum_{i=1}^{n} ax_i D(y_i) - \sum_{i=1}^{n} x_i D(y_i a) + D(a) = D(a)$, para todo $a \in A$, o que mostra que D é uma derivação interior.

Reciprocamente, suponhamos que toda derivação de A (em qualquer A-bimódulo M) é interior. Seja $A^e = A \otimes_K A^o$ visto como A-bimódulo via as ações $(a \otimes b^o)c = a \otimes (bc)^o - ab \otimes c^o$ e $c(a \otimes b^o) = ca \otimes b^o$ para todo $a,b,c \in A$ e consideremos a aplicação K-linear $\partial : A \longrightarrow A^e$ dada por $\partial(a) = 1 \otimes a^o$. Desde que $\partial(bc) = 1 \otimes (bc)^o = (1 \otimes b^o)c + b(1 \otimes c^o) = \partial(b)c + b\partial(c)$, vemos que ∂ é uma K-derivação e, portanto, existe $e = \sum_{i=1}^{n} x_i \otimes y_i^o \in A^e$ tal que $\partial(a) = ae - ea$ para todo $a \in A$. Logo temos $1 \otimes a^o = \sum_{i=1}^{n} ax_i \otimes y_i^o - \sum_{i=1}^{n} x_i \otimes (y_i a)^o + \sum_{i=1}^{n} x_i y_i \otimes a^o$ para todo $a \in A$. Em particular, para $a = 1$ temos $1 \otimes 1^o =$

$$= \sum_{i=1}^{n} x_i \otimes y_i^o - \sum_{i=1}^{n} x_i \otimes y_i^o + \sum_{i=1}^{n} x_i y_i \otimes 1^o = \sum_{i=1}^{n} x_i y_i \otimes 1^o \quad ,$$

donde segue-se que $\sum_{i=1}^{n} x_i y_i = \phi(\sum_{i=1}^{n} x_i \otimes y_i^o) = \phi(1 \otimes 1^o) = 1.$

Portanto, voltando a igualdade $1 \otimes a^o = \sum_{i=1}^{n} ax_i \otimes y_i^o -$

$- \sum_{i=1}^{n} x_i \otimes (y_i a)^o + \sum_{i=1}^{n} x_i y_i \otimes a^o$, obtemos $\sum_{i=1}^{n} ax_i \otimes y_i^o =$

$= \sum_{i=1}^{n} x_i \otimes (y_i a)^o$ ou, equivalentemente, $(a \otimes 1^o)e = (1 \otimes a^o)e$

para todo $a \in A$. Agora seja $h : A \longrightarrow A^e$ uma aplicação dada por $h(a) = (a \otimes 1^o)e$. Claramente $h(a + b) = h(a) + h(b)$ para todo $a,b \in A$, $\phi \circ h = id_A$. Também para todo $a,b,c \in A$ temos $h((a \otimes b^o)c) = h(acb) = (acb \otimes 1^o)e = (ac \otimes 1^o)(b \otimes 1^o)e =$ $= (ac \otimes 1^o)(1 \otimes b^o)e = (ac \otimes b^o)e = (a \otimes b^o)(c \otimes 1^o)e =$ $= (a \otimes b^o)h(c)$, ou seja, h é A^e-linear e portanto a sequência exata $0 \longrightarrow J(A) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0$ cinde. Consequentemente A é separável sobre K (cf. Teorema 2.7). ∎

(3.8) COROLÁRIO: Seja A uma K-álgebra de dimensão finita e comutativa. Então A é separável sobre K se, e somente se, toda K-derivação de A (em qualquer A-módulo M) é nula.

CAPÍTULO II

ÁLGEBRAS SEPARÁVEIS

Este capítulo é todo dedicado ao estudo da noção e propriedades da separabilidade sobre anéis comutativos.

Em todo o capítulo, a letra R denotará sempre um anel comutativo com elemento identidade.

Com intuito de evitarmos sermos repetitivos , assumiremos aqui a mesma notação e terminologia utilizadas no capítulo I.

§1. DEFINIÇÃO E EXEMPLOS

(1.1) TEOREMA: Seja A uma R-álgebra. Então às seguintes condições são equivalentes:

i) A é um A^e-módulo à esquerda projetivo

ii) A sequência exata de A^e-módulos à esquerda

$$0 \longrightarrow J(A) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0 \qquad \text{cinde}$$

iii) existe $e \in A^e$ tal que $\phi(e) = 1$ e $J(A)e = 0$.

DEMONSTRAÇÃO:

i) $\Longleftrightarrow$ ii) Decorre imediatamente da definição de módulo projetivo (ver apêndice, Prop. A-1)

ii) $\Rightarrow$ iii) Por hipótese existe um A^e-homomorfismo $h: A \to A^e$

tal que ϕ o h = id. Seja $e = h(1) \in A^e$. Logo $\phi(e) = 1$. Para mostrar que $J(A)e = 0$, vejamos inicialmente que $J(A)$ é um ideal de A^e gerado por elementos da forma $a \otimes 1^o - 1 \otimes a^o$ $(a \in A)$. Claramente $a \otimes 1^o - 1 \otimes a^o \in J(A)$ $(a \in A)$. Por outro lado, se $\sum_{i=1}^{n} a_i \otimes b_i^o \in J(A)$ então $\sum_{i=1}^{n} a_i b_i = 0$ e consequentemente $\sum_{i=1}^{n} a_i \otimes b_i^o = \sum_{i=1}^{n} (a_i \otimes 1^o)(1 \otimes b_i^o - b_i \otimes 1^o)$, ou seja, $J(A)$ é gerado por elementos da forma $a \otimes 1^o - 1 \otimes a^o$ $(a \in A)$ (cf. observação (3.6) 2) do cap. I). Agora para todo $a \in A$, $(a \otimes 1^o)e = (a \otimes 1^o)h(1) = h((a \otimes 1^o).1) = h(a) = h((1 \otimes a^o).1) = (1 \otimes a^o)h(1) = (1 \otimes a^o).e$, ou seja, $(a \otimes 1^o - 1 \otimes a^o)e = 0$ e consequentemente $J(A)e = 0$.

iii) $\Rightarrow$ ii) Por hipótese existe $e \in A^e$ tal que $\phi(e) = 1$ e $J(A)e = 0$. Definimos $h: A \longrightarrow A^e$ por $h(a) = (a \otimes 1^o)e = (1 \otimes a^o)e$. Claramente $h(a+b) = h(a)+h(b)$ para todo $a,b \in A$ e ϕ o h = id. Agora para todo $a,b,c \in A$ temos $h((a \otimes b^o).c) = h(acb) = (acb \otimes 1^o)e = (ac \otimes 1^o)(b \otimes 1^o)e = (ac \otimes 1^o)(1 \otimes b^o)e = (ac \otimes b^o)e = (a \otimes b^o)(c \otimes 1^o)e = (a \otimes b^o)h(c)$, ou seja, h é A^e-linear e portanto a sequência $0 \longrightarrow J(A) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0$ cinde ∎

(1.2) DEFINIÇÃO: Seja A uma R-álgebra. Dizemos que A é *separável* sobre R se satisfaz uma das condições equivalentes do teorema (1.1) acima.

De acordo com o teorema (2.7) do capítulo I vemos que a noção de separabilidade sobre anéis comutativos é uma extensão natural da correspondente noção sobre corpos.

O elemento $e \in A^e$ verificando a condição (iii) do teorema (1.1) acima é claramente um elemento idempotente ($e^2-e=(e-1)e \in J(A)e = 0$) chamado *idempotente de separabilidade* de A. Portanto A é separável sobre R se e somente se possui um idempotente de separabilidade. Esse idempotente em geral não é único (cf. exemplo 1.3 f) abaixo). Contudo, se A for comutativa o idempotente de separabilidade é único, pois se $e_1, e_2 \in A^e$, $e_1 \neq e_2$ são tais que $\phi(e_1) = \phi(e_2) = 1$ e $J(A)e_1 = J(A)e_2 = 0$, então $\phi(e_1) - \phi(e_2) = \phi(e_1 - e_2) = 0$, ou seja, $e_1 - e_2 \in \text{Ker } \phi$. Portanto, $(e_1 - e_2)e_1 = e_1^2 - e_2e_1 = e_1 - e_2e_1 \in J(A)e_1 = 0$ e $(e_2 - e_1)e_2 = e_2 - e_1e_2 \in J(A)e_2 = 0$, e consequentemente $e_1 = e_2$.

(1.3) EXEMPLOS:

a) R é claramente separável sobre R. Mais geralmente, um produto de cópias de R, $R^n = R \times \ldots \times R$ é separável sobre R.

b) Seja $U \subset R$ um sistema multiplicativo de R. Então R_U é separável sobre R, pois neste caso a multiplicação ϕ é um isomorfismo. Em particular, Q é uma $\mathbb{Z}$-álgebra separável.

c) $A = \mathbb{Z}/p\mathbb{Z}$, com p primo, é uma $\mathbb{Z}$-álgebra separável. Novamente, aqui, a multiplicação $\phi: \mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ é um isomorfismo.

d) Sejam $R = \mathbb{Z}[\sqrt{-3}]$ e $A = \mathbb{Z}[w]$, onde w é uma raíz terceira primitiva da unidade. A é uma R-álgebra separável cujo

idempotente de separabilidade é dado por $1 \otimes 1 + 1 \otimes w - w \otimes 1$.

e) $A = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, a $\mathbb{R}$-álgebra de quatérnios, é uma $\mathbb{R}$-álgebra separável. Um idempotente de separabilidade é dado por $e = \frac{1}{4}(1 \otimes 1^{o} - i \otimes i^{o} - j \otimes j^{o} - k \otimes k^{o})$.

f) A álgebra das matrizes $n \times n$, $M_n(R)$, à coeficientes em R é separável. De fato: sejam e_{ij} as matrizes elementares. Seja $e = \sum_{i=1}^{n} e_{ij} \otimes e_{ji}$ para j fixo entre 1 e n. Então $\phi(e) = \sum_{i=1}^{n} e_{ij}e_{ji} = \sum_{i=j}^{n} e_{ii} = 1$, e para todo k e ℓ, $(e_{k\ell} \otimes 1 - 1 \otimes e_{k\ell})e = \sum_{i=1}^{n} (e_{k\ell}e_{ij} \otimes e_{ji} - e_{ij} \otimes e_{ji}e_{k\ell}) = e_{kj} \otimes e_{j\ell} - e_{kj} \otimes e_{j\ell} = 0$. Desde que os $e_{k\ell}$ geram $M_n(R)$ como R-módulo, isto mostra que $J(M_n(R))e = 0$. Portanto $M_n(R)$ é uma R-álgebra separável e e é o idempotente de separabilidade.

g) Seja G um grupo finito cuja ordem n é uma unidade em R. Então a álgebra de grupo $R[G]$ é uma R-álgebra separável. Com efeito, tomando $e = \frac{1}{n} \sum_{x \in G} x \otimes x^{-1}$ em $R[G]^{e}$ temos $\phi(e) = 1$, e para todo $y \in G$, $(y \otimes 1)e = \frac{1}{n} \sum_{x \in G} yx \otimes x^{-1} = \frac{1}{n} \sum_{x \in G} z \otimes z^{-1}y = (1 \otimes y)e$. Portanto $R[G]$ é R-separável e e é um idempotente de separabilidade.

h) Sejam $f \in R[X]$ um polinômio mônico e $A = \frac{R[X]}{\langle f \rangle} = R[x]$, com $x = X + \langle f \rangle$. Se f' denota a derivada formal de f e $f'(x)$ é inversível em A, então A é separável sobre R. Em particular se K é um corpo e $f \in K[X]$ é um polinômio separável sobre K então $K[X]/_{\langle f \rangle}$ é separável sobre K. De fato, sejam $f(x) = a_0x^{n} + \ldots + a_n$ com $a_i \in R$, $a_0 = 1$ e

$e = \frac{f_{n-1}(x)}{f'(x)} \otimes 1 + \ldots + \frac{f_o(x)}{f'(x)} \otimes x^{n-1}$ onde $f_k(x) = a_o x^k + a_1 x^{k-1} + \ldots + a_k$, $0 \leq k \leq n$. Notemos que $f_n - x f_{n-1} = a_n$, $f_{n-1} - x f_{n-2} = a_{n-1}$, ... , $f_1 - x f_o = a_1$. Daí $e(x \otimes 1) = \frac{x f_{n-1}(x)}{f'(x)} \otimes 1 + \ldots + \frac{x f_o(x)}{f'(x)} \otimes x^{n-1}$, onde $\frac{f_o(x)}{f'(x)} \otimes x^n = \frac{a_o}{f'(x)} \otimes x^n = \frac{1}{f'(x)} \otimes a_o x^n = \frac{-1}{f'(x)} \otimes (a_1 x^{n-1} + \ldots + a_n)$. Por outro lado , como $e(x \otimes 1) = \frac{f_n(x) - a_n}{f'(x)} \otimes 1 + \frac{f_{n-1}(x) - a_{n-1}}{f'(x)} \otimes x + \ldots + \frac{f_2(x) - a_2}{f'(x)} \otimes x^{n-2} + \frac{f_1(x) - a_1}{f'(x)} \otimes x^{n-1}$, temos que $e(1 \otimes x) - e(x \otimes 1) = \frac{-1}{f'(x)} \otimes (a_1 x^{n-1} + \ldots + a_n) + \frac{a_n}{f'(x)} \otimes 1 + \frac{a_{n-1}}{f'(x)} \otimes x + \ldots + \frac{a_1}{f'(x)} \otimes x^{n-1} = 0$. Agora tenos que $\phi(e) = \frac{1}{f'(x)} (f_{n-1}(x) + f_{n-2}(x)\, x + \ldots + f_o(x)\, x^{n-1})$ e notando que

$$f_{n-1}(x) = a_o x^{n-1} + a_1 x^{n-2} + \ldots + a_{n-1}$$

$$f_{n-2}(x)\, x = a_o x^{n-1} + a_1 x^{n-2} + \ldots + a_{n-2} x$$

$$\vdots$$

$$f_2(x)\, x^{n-3} = a_o x^{n-1} + a_1 x^{n-2} + a_2 x^{n-3}$$

$$f_1(x)\, x^{n-2} = a_o x^{n-1} + a_1 x^{n-2}$$

$$f_o(x)\, x^{n-1} = a_o x^{n-1}$$

temos que $f'(x) = f_{n-1}(x) + f_{n-2}(x)x + \ldots + f_o(x)x^{n-1}$ e portanto $\phi(e) = 1$. Portanto $R[x]/_{(f)}$ é separável e e é um idempotente de separabilidade.

§ 2. PROPRIEDADES:

Uma das primeiras propriedades que gostaríamos de observar é a seguinte:

No exemplo 1.3 b) acima vemos que uma álgebra separável sobre um anel R não é necessariamente livre como R-módulo e muito menos finitamente gerada. Contudo, no caso de R ser corpo, uma R-álgebra separável é necessariamnte de dimensão finita como R-espaço vetorial, conforme Proposição abaixo.

(2.1) PROPOSIÇÃO: Seja A uma R-álgebra separável. Se R for um corpo então $\dim_R A < \infty$.

DEMONSTRAÇÃO: Se R é corpo, então A e A^o são espaços vetoriais sobre R. Sejam $\{x_i\}_{i \in I}$ uma base de A^o e $\{f_i\}_{i \in I}$ uma base de $\mathrm{Hom}_R(A^o,R)$ definida por $f_i(x_j) = \delta_{ij}$. Todo elemento de A^o é claramente da forma $a = \sum_{i \in I} f_i(a)x_i$ onde $f_i(a) = 0$ exceto para um número finito de i's. Identificando $A \otimes_R R$ com A, podemos considerar $\{1 \otimes f_i\}_{i \in I}$ como base de $\mathrm{Hom}_A(A^e,A)$ e $\{1 \otimes x_i\}_{i \in I}$ como base de A^e sobre A. Logo para todo $x \in A^e$ temos que $x = \sum_{i \in I} (1 \otimes f_i)(x)(1 \otimes x_i)$.

Sejam $\phi: A^e \longrightarrow A$ a aplicação A^e-linear dada pelo produto e $e \in A^e$ tal que $\phi(e) = 1$ e $J(A)e = 0$. Então temos, para todo $a \in A$, $a = \phi((1 \otimes a^o)e) = \phi(\sum_{i\in I} (1 \otimes f_i)((1 \otimes a^o)e)(1 \otimes x_i)) = \sum_{i\in I} (1 \otimes f_i)((1 \otimes a^o)e)x_i$ pois ϕ é A^e-linear e $(1 \otimes f_i)((1 \otimes a^o)e) \in A \otimes_R R \subset A^e$. Por outro lado, $(1 \otimes f_i)((1 \otimes a^o)e) = (1 \otimes f_i)((a \otimes 1^o)e) = (a \otimes 1^o)(1 \otimes f_i)(e)$ pois $J(A)e = 0$. Consequentemente, $\{i \in I : (1 \otimes f_i)((1 \otimes a)e) \neq 0\} \subset J = \{i \in I : (1 \otimes f_i)(e) \neq 0\}$ e este último é finito e independente de a. Então $a = \sum_{j\in J} (1 \otimes f_j)((1 \otimes a^o)e)x_j$ e considerando $e = \sum_{i=1}^{n} a_i \otimes b_i^o$, temos

$$a = \sum_{j\in J} (1 \otimes f_j)((1 \otimes a^o) \sum_{i=1}^{n} a_i \otimes b_i^o)x_j =$$

$$= \sum_{j\in J} (1 \otimes f_j)(\sum_{i=1}^{n} a_i \otimes (b_i a)^o)x_j = \sum_{\substack{i=1 \\ j\in J}}^{n} (a_i \otimes f_j(b_i a))x_j =$$

$$= \sum_{\substack{i=1 \\ j\in J}}^{n} (a_i f_j(b_i a) \otimes 1^o)x_j = \sum_{\substack{i=1 \\ j\in J}}^{n} a_i f_j(b_i a)x_j = \sum_{\substack{i=1 \\ j\in J}}^{n} f_j(b_i a)a_i x_j.$$

Isto mostra que o conjunto finito $\{a_i x_j : i = 1,\ldots,n , j \in J\}$ gera A^o sobre R e consequentemente gera A sobre R. Isto significa que $\dim_R A < \infty$ ∎

Damos a seguir o análogo para anéis do teorema 3.7 do capítulo I.

Recordamos, antes, as noções de derivação e derivação interior vistas no §3 do capítulo I.

UNICAMP
BIBLIOTECA CENTRAL

Sejam A uma R-álgebra e M um A^e-módulo ou, equivalentemente, um A-bimódulo. Uma R-derivação de A em M é uma aplicação R-linear $d: A \to M$ tal que $d(ab) = d(a)b + ad(b)$, para todo $a,b \in A$. Dizemos que d é interior se existe $m \in M$ tal que $d(a) = am - ma = \delta(a)m$, onde $\delta: A \to J(A)$ é a R-derivação dada por $\delta(a) = a \otimes 1^o - 1 \otimes a^o$. Denotamos por $Der_R(A,M)$ o R-módulo das R-derivações de A em M.

(2.2) TEOREMA: Seja A uma R-álgebra. São equivalentes:

i) A é separável sobre R

ii) Toda R-derivação de A (em um A^e-módulo) é interior.

Para a demonstração deste teorema necessitamos da seguinte proposição.

(2.3) PROPOSIÇÃO: Sejam A uma R-álgebra e M um A-bimódulo. Então o homomorfismo $\varphi: Hom_{A^e}(J(A),M) \to Der_R(A,M)$ definido por $f \to f \circ \delta$ é um isomorfismo tal que as derivações interiores correspondam as aplicações A^e-lineares de J(A) em M que se extendem à A^e. Se, além disso, A é comutativa e se M é A-módulo, a mesma aplicação induz um isomorfismo de $Hom_A(J(A)/J(A)^2, M)$ em $Der_R(A,M)$.

DEMONSTRAÇÃO: Mostremos, inicialmente, que φ é bijeção. Ela é injetora, pois $f \circ \delta = 0$ se, e somente se, $f \circ \delta(A) = 0$ se, e somente se, $Af(\delta(A)) = f(A\delta(A)) = f(J(A)) = 0$ se, e somente se, $f = 0$. Agora, para mostrar que φ é sobre seja

$D: A \to M$ uma R-derivação. Definimos a aplicação $f: A^e \to M$ por $f(a \otimes b) = -a\,D(b)$. Claramente f é R-linear e $f(\delta(A)) = f(a \otimes 1^o - 1 \otimes a^o) = -aD(1) + 1D(a) = D(a)$ pois $D(a) = D(a) + aD(1)$ $(a \in A)$. Agora mostremos que f restrita a $J(A)$ é A^e-linear; para isso seja $x \otimes y^o \in A^e$ e $\sum_{i=1}^{n} a_i \otimes b_i^o \in J(A)$. Então $f((x \otimes y^o)(\sum_{i=1}^{n} a_i \otimes b_i^o)) = f(\sum_{i=1}^{n} xa_i \otimes (b_i y)^o) = -\sum_{i=1}^{n} xa_i\,D(b_i y) =$

$$= -\sum_{i=1}^{n} xa_i(D(b_i)y + b_i D(y)) = -\sum_{i=1}^{n} xa_i D(b_i)y - \sum_{i=1}^{n} xa_i b_i D(y) =$$

$$= -\sum_{i=1}^{n} xa_i D(b_i)y \; ; \text{ por outro lado, } (x \otimes y^o) f(\sum_{i=1}^{n} a_i \otimes b_i^o) =$$

$$= (x \otimes y^o)(-\sum_{i=1}^{n} a_i D(b_i)) = -(x \otimes y^o)\sum_{i=1}^{n} a_i D(b_i) = -\sum_{i=1}^{n} x a_i D(b_i)y.$$

Agora, se D é inteira então $D(a) = \delta(a)m$ para algum $m \in M$, e definindo $f: A^e \to M$ por $f(1 \otimes 1^o) = m$ temos que $f(D(a)) = f(a \otimes 1^o - 1 \otimes a^o) = am - ma$. Reciprocamente, se f é definida sobre A^e, $D(a) = f(D(a)) = D(a) f(1 \otimes 1^o) = D(a)m$.

Finalmente, se A é comutativa e M um A-módulo, definimos $\psi: \mathrm{Hom}_A(J(A)/J(A)^2, M) \to \mathrm{Hom}_{A^e}(J(A), M)$ por $\psi(f) = f \circ \pi$ onde $\pi: J(A) \to J(A)/J(A)^2$. Segue imediatamente de $a \otimes b = ab \otimes 1 - a(1 \otimes b - b \otimes 1)$ que $f \circ \pi$ é um A^e-homomorfismo. A aplicação ψ é injetiva pois π é sobre. Para mostrar que ψ é sobre, é suficiente notar que um A^e-homomorfismo $f: J(A) \to M$ é nulo sobre $J(A)^2$. De fato,

$f((a \otimes 1 - 1 \otimes a)(b \otimes 1 - 1 \otimes b)) = af(b \otimes 1 - 1 \otimes b) -$

$- f(b \otimes 1 - 1 \otimes b)a = 0$. Logo ψ é um isomorfismo e conse-

quentemente $\mathrm{Hom}_A(J(A)/J(A)^2, M)$ é isomorfo a $\mathrm{Der}_R(A,M)$.■

DEMONSTRAÇÃO DO TEOREMA 2.2 (compare com a demonstração do Teorema 3.7 do capítulo I)

i) $\Rightarrow$ ii) Por hipótese, a sequência exata de A^e-módulos $0 \to J(A) \to A^e \to A \to 0$ é cindida. Logo, considerando que $\mathrm{Hom}_{A^e}(-,M)$ comuta com soma direta finita, obtemos que a sequência $0 \to \mathrm{Hom}_{A^e}(A,M) \to \mathrm{Hom}_{A^e}(A^e,M) \to \mathrm{Hom}_{A^e}(J(A),M) \to 0$ também é exata (e cinde), para todo A^e-módulo M.

Notemos que $\mathrm{Hom}_{A^e}(J(A),M) \simeq \mathrm{Der}_R(A,M)$ como R-módulos, via a aplicação $f \to f \circ \delta$ (cf. Proposição 2.3 acima). Por outro lado, é fácil ver que $\mathrm{Hom}_{A^e}(A^e,M) \simeq M$ como R-módulos, via as aplicações $f \to f(1 \otimes 1^o)$ e $m \to (f_m : a \otimes b^o \to amb)$. Assim, reunindo essas afirmações, vemos que existe uma aplicação sobrejetiva $M \to \mathrm{Der}_R(A,M)$ dada por $m \to f_m \circ \delta$ e, desde que, $(f_m \circ \delta)(a) = f_m(a \otimes 1^o - 1 \otimes a^o) = am - ma = \delta(a)m$, para todo $a \in A$, concluimos que toda R-derivação de A em M é interior.

ii) $\Rightarrow$ i) Se toda R-derivação de A é interior, em particular, $\delta : A \to J(A)$ é interior e portanto existe $x_o \in J(A)$ tal que $\delta(a) = \delta(a)x_o$, para todo $a \in A$. Definimos $\varphi : A^e \to J(A)$ como sendo o homomorfismo de A^e-módulos dado por $\varphi(1 \otimes 1^o) = x_o$. Considerando que $J(A)$ é gerado por $\{\delta(a) : a \in A\}$ e que $\varphi(\delta(a)) = \varphi(\delta(a)(1 \otimes 1^o)) = \delta(a)\,\varphi(1 \otimes 1^o) = \delta(a)x_o = \delta(a)$, para todo $a \in A$, a sequência exata $0 \to J(A) \to A^e \to A \to 0$ cinde e portanto A é separável ■

(2.4) COROLÁRIO: Seja A uma R-álgebra comutativa. São equivalentes:

i) A é separável sobre R

ii) Toda R-derivação de A é nula

iii) $J(A) = J(A)^2$

A separabilidade mantém-se via soma direta e produto direto.

(2.5) PROPOSIÇÃO: Sejam A e B R-álgebras separáveis. Então $A \otimes_R B$ e $A \oplus B$ são R-álgebras separáveis. Além disso, centro $(A \otimes_R B)$ = centro $(A) \otimes_R$ centro(B).

DEMONSTRAÇÃO: Sejam $\phi_A: A^e \to A$ e $\phi_B: B^e \to B$ as aplicações A^e-lineares e B^e-lineares dadas pelo produto. Claramente $(A \otimes_R B)^e = A^e \otimes_R B^e$. Seja o seguinte diagrama comutativo

$$\begin{array}{ccc} \mathrm{Hom}_{A^e}(A,A^e) \otimes_R \mathrm{Hom}_{B^e}(B,B^e) & \xrightarrow{\phi'_A \otimes \phi'_B} & \mathrm{Hom}_{A^e}(A,A) \otimes_R \mathrm{Hom}_{B^e}(B,B) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{(A \otimes_R B)^e}(A \otimes_R B, (A \otimes_R B)^e) & \xrightarrow{\phi_1} & \mathrm{Hom}_{(A \otimes_R B)^e}(A \otimes_R B, A \otimes_R B) \end{array}$$

onde ϕ'_A e ϕ'_B são as induzidas de ϕ_A e ϕ_B, respectivamente, e as aplicações verticais são isomorfismos (ver Apêndice, Prop. A-9). Como ϕ'_A e ϕ'_B são sobrejetivas (ver Apêndice, Prop. A-1) então $\phi'_A \otimes \phi'_B$ é sobrejetiva e consequentemente

ϕ_1 é sobrejetiva, ou seja, $A \otimes_R B$ é separável sobre R.

Observando que $\mathrm{Hom}_{A^e}(A,A) \simeq \mathrm{centro}(A)$, via as aplicações $f \to f(1)$ e $a \to f_a: x \to ax$, a afirmação sobre o centro de $(A \otimes B)$ decorre do segundo isomorfismo vertical do diagrama acima.

Finalmente, provemos que $A \times B$ é R-separável. Para isso, é suficiente mostrar que a sequência exata $0 \to J(A \times B) \to (A \times B)^e \xrightarrow{\phi} A \times B \to 0$ cinde, onde a aplicação ϕ é dada pelo produto. Notemos que $(A \times B)^e = A \otimes A^o \times A \otimes B^o \times B \otimes A^o \times B \otimes B^o$. Por hipótese existem aplicações $h_A: A \to A^e$ e $h_B: B \to B^e$ tais que $\phi_A \circ h_A = id$ e $\phi_B \circ h_B = id$. Observemos que ϕ restrita a A^e é ϕ_A e que ϕ restrita a B^e é ϕ_B. Definimos $h_A \times h_B: A \times B \to (A \times B)^e$ de modo natural. Seja a inclusão $i: A^e \times B^e \to (A \times B)^e$. Seja a aplicação $h = i \circ (h_A \times h_B)$. Claramente h é $(A \times B)^e$-linear. Mostremos que $\phi \circ h = id$. Com efeito, $(\phi \circ h)(a,b) = \phi \circ i \circ (h_A,h_B)(a,b) = (\phi \circ i)(h_A(a),h_B(b)) = \phi(h_A(a),h_B(b)) = (a,b)$. Portanto $A \times B$ é R-separável ∎

A separabilidade é preservada por extensão de escalares.

(2.6) PROPOSIÇÃO: Se A é uma R-álgebra separável e S uma R-álgebra comutativa então $A \otimes_R S$ é uma S-álgebra separável.

DEMONSTRAÇÃO: Mostremos, inicialmente, que $J(A \otimes_R S) = J(A) \otimes_R S$. De fato, a sequência exata $0 \to J(A) \to A^e \xrightarrow{\Phi} A \to 0$, vista como sequência de A-módulos, é cindida. Como secção podemos

considerar a aplicação $f: A \to A^e$ tal que $f(a) = a \otimes 1^o$. Em particular a sequência acima é também cindida como sequência de R-módulos. Considerando, agora, que $(A \otimes_R A^o) \otimes_R S \cong (A \otimes_R S) \otimes_S (A^o \otimes_R S) \cong (A \otimes_R S) \otimes_S (A \otimes_R S)^o$, o resultado segue-se. Logo $J(A \otimes_R S) = J(A) \otimes_R S$ e se $e \in A^e$ é um idempotente de separabilidade para A, é imediato que $e \otimes 1$ é um idempotente de separabilidade para $A \otimes_R S$ ■

A recíproca da proposição 2.6 acima é válida com alguma hipótese sobre S. A título de ilustração damos a seguir a seguinte proposição.

(2.7) PROPOSIÇÃO: Sejam A uma R-álgebra e S uma R-álgebra comutativa. Se S é um R-módulo fielmente projetivo e se $A \otimes_R S$ é uma S-álgebra separável então A é separável sobre R.

Observemos que um R-módulo S é *fielmente projetivo* se S é finitamente gerado, projetivo e fiel (isto é, o anulador de S em R é nulo).

Para a demonstração da Proposição 2.7 necessitamos do seguinte lema.

(2.8) LEMA: Seja S uma R-álgebra a qual é fielmente projetivo como R-módulo. Então R é um somando direto de S como R-módulo.

DEMONSTRAÇÃO: Desde que S é um R-módulo projetivo, existem

$x_i \in S$ e $f_i \in \mathrm{Hom}_R(S,R)$, $i \in I$, tais que $x = \sum_{i \in I} f_i(x)x_i$, para todo $x \in S$, com $f_i(x) = 0$ exceto para um número finito de $i \in I$ (ver Apêndice, Prop. A-1). Então, se $I \subset R$ é o ideal de R gerado por $\{f(x): f \in \mathrm{Hon}_R(S,R) , x \in S\}$, temos $IS = S$. Disto decorre que existe $a \in I$ tal que $(1 - a)S = 0$ (ver Apêndice, Prop. A-2). Como S é fiel, $a = 1$ e portanto $I = R$. Sejam $g_i \in \mathrm{Hom}_R(S,R)$ e $y_i \in S$, $1 \leq i \leq n$, tais que $\sum_{i=1}^{n} g_i(y_i) = 1$. A aplicação R-linear $t: S \to R$ dada por $t(x) = \sum_{i=1}^{n} g_i(xy_i)$ é uma secção para a inclusão $i: R \to S$. Agora é imediato ver que R é um somando direto de S ∎

DEMONSTRAÇÃO DA PROPOSIÇÃO 2.7: Desde que S é um R-módulo fielmente projetivo, R é somando direto de S como R-módulo e consequentemente A é somando direto de $A \otimes_R S$ como A^e-módulo. Como $A \otimes_R S$ é separável sobre S, então $A \otimes_R S$ é somando direto de $A^e \otimes_R S$ como $A^e \otimes_R S$-módulo. Portanto A é somando direto de $A^e \otimes_R S$ como A^e-módulo. Desde que S é R-projetivo e A^e é um A^e-módulo segue que $A^e \otimes_R S$ é A^e-projetivo. Logo A é A^e-projetivo, pois A é somando direto de $A^e \otimes_R S$. Portanto A é separável sobre R ∎

A separabilidade é transitiva.

(2.9) TEOREMA: Seja S uma R-álgebra comutativa e A uma S-álgebra. Então temos:

(i) se A é R-separável então A é S-separável

(ii) se A é S-separável e S é R-separável, então A é R-separável.

(iii) se A é R-separável e se A é um S-módulo fielmente projetivo, então S é R-separável.

DEMONSTRAÇÃO:

(i) Seja o seguinte diagrama comutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker\phi & \longrightarrow & A \otimes_R A^o & \xrightarrow{\phi} & A & \longrightarrow & 0 \\ & & & & \downarrow i & & & & \\ 0 & \longrightarrow & \ker\varphi & \longrightarrow & A \otimes_S A^o & \xrightarrow{\varphi} & A & \longrightarrow & 0 \end{array}$$

onde as aplicações ϕ e φ são os produtos. Como A é R-separável existe uma aplicação $A \otimes_R A^o$-linear $h: A \to A \otimes_R A^o$ tal que $\phi \circ h = id$. Seja $f = i \circ h$. Claramente f é $A \otimes_S A^o$-linear e $\varphi \circ f = id$. Portanto a sequência exata $0 \to \ker\varphi \to A \otimes_S A^o \overset{\varphi}{\leftrightarrows} A \to 0$ cinde, ou seja, A é S-separável.

(ii) Desde que S é R-separável, então a sequência exata $0 \to J(S) \to S \otimes_R S \overset{\phi}{\to} S \to 0$ cinde, ou seja, S é somando direto de $S \otimes_R S = S^e$. Daí $S \otimes_{S^e}(A \otimes_R A^o) = A \otimes_S A^o$ (a identificação aqui é feita via as aplicações $s \otimes a \otimes a^o \to sa \otimes a^o$ e $a \otimes a^o \to 1 \otimes a \otimes a^o$) é somando direto de $S^e \otimes_{S^e}(A \otimes_R A^o) = A \otimes_R A^o$. Finalmente, A é somando direto de $A \otimes_R A^o$, pois por hipótese A é somando direto de $A \otimes_S A^o$. Portanto A é $A \otimes_R A^o$-projetivo, ou seja, A é R-separável.

(iii) Desde que A é R-separável, segue que A é somando

direto de $A \otimes_R A^O$. Mas $A \otimes_R A^O$ é $S \otimes_R S$-projetivo pois A é S-projetivo. Como A é um S-módulo fielmente projetivo então S é um somando direto de A como um S-módulo (cf. Lema 2.8). Portanto S é $S \otimes_R S$-projetivo , ou seja , S é R-separável ■

(2.10) COROLÁRIO: Sejam S uma R-álgebra e A uma S-álgebra. Se R e S são corpos, então A é separável sobre R se, e somente se, A é separável sobre S e S é separável sobre R.

(2.11) TEOREMA: Seja A uma R-álgebra finitamente gerada como R-módulo ou comutativa e finitamente gerada como R-álgebra. São equivalentes:

i) A é uma R-álgebra separável

ii) A_p é uma R_p-álgebra separável, para todo ideal primo P de R.

iii) A_M é uma R_M-álgebra separável, para todo ideal maximal M de R.

DEMONSTRAÇÃO:

i) ⇒ ii) por extensão de escalares, desde que $A_p = R_p \otimes_R A$ (cf. Prop. 2.6)

ii) ⇒ iii) é obvia

Para a demonstração de iii) $\Rightarrow$ i) necessitamos do lema seguinte.

(2.12) LEMA: Seja A uma R-álgebra. Se A é finitamente gerado como R-módulo ou A é comutativa e finitamente gerada como R-álgebra, então $J(A) = \ker(A \otimes_R A^o \xrightarrow{\phi} A)$ é finitamente gerado como A^e-módulo e A é de apresentação finita como A^e-módulo.

(Observemos, aqui, que um R-módulo T é de *apresentação finita* se existe uma sequência exata de R-módulos: $F_1 \rightarrow F_o \rightarrow T \rightarrow 0$ onde F_o e F_1 são finitamente gerados e F_o é livre - ver Apêndice)

DEMONSTRAÇÃO DO LEMA: Se J(A) é finitamente gerado sobre A^e, A é de apresentação finita sobre A^e, pois pela definição de J(A) a sequência $0 \rightarrow J(A) \rightarrow A^e \xrightarrow{\phi} A \rightarrow 0$ é exata . Esta sequência é cinde como A-módulos á esquerda, uma secção $j: A \rightarrow A^e$ é definido por $j(a) = a \otimes 1$. Em particular a sequência acima também é cindida como sequência de R-módulos. Provemos, portanto, no primeiro caso que J(A) é um R-módulo finitamente gerado, portanto a fortiori um A^e-módulo finitamente gerado. No segundo caso, mostremos que se os elementos $(x_i)_{i \in I}$ geram A como R-álgebra, os elementos $(x_i \otimes 1 - 1 \otimes x_i)_{i \in I}$ geram J(A) como $A \otimes_R A$-módulo. Sabemos que os elementos $(x_i \otimes 1 - 1 \otimes a)_{a \in A}$ geram J(A) como $A \otimes_R A$-módulo (cf. demonstração do Teorema 1.1 do Capítulo II). É suficiente portanto provar que $a \otimes 1 - 1 \otimes a$ é combinação linear dos elementos $(x_i \otimes 1 - 1 \otimes x_i)_{i \in I}$ com coeficientes em $A \otimes_R A$. Por indução, é suficiente provar para

$a = st$ com $s,t \in (x_i)_{i\in I}$. Mas neste caso $st \otimes 1 - 1 \otimes st = (1 \otimes s)(t \otimes 1 - 1 \otimes t) + (s \otimes 1)(t \otimes 1 - 1 \otimes t)$ ■

Continuação da demonstração do Teorema 2.11.

iii) ⇒ i) Para todo ideal maximal M de R, temos $A^e \otimes_R R_M = (A \otimes_R A^o) \otimes_R R_M = (A \otimes_R R_M) \otimes_{R_M} (A \otimes_R R_M)^o = A_M \otimes A_M^o = A_M^e$. Seja $\phi_M : A_M^e \to A_M$ a aplicação induzida por $\phi: A^e \to A$. Sejam $\phi' : \mathrm{Hom}_{A^e}(A,A^e) \to \mathrm{Hom}_{A^e}(A,A)$ e $\phi'_M : \mathrm{Hom}_{A_M^e}(A_M, A_M^e) \to \mathrm{Hom}_{A_M^e}(A_M,A_M)$ as aplicações induzidas por ϕ e ϕ_M, respectivamente. Pelo Lema 2.12 acima A é um A^e-módulo de apresentação finita. Logo considerando que $\mathrm{Hom}_{R/M}(R/M, R/M) \simeq R_M$ via a aplicação $f \to f(1)$, as aplicações verticais no diagrama

$$\begin{array}{ccc} \mathrm{Hom}_{A^e}(A,A^e) \otimes_R R_M & \xrightarrow{\phi' \otimes 1} & \mathrm{Hom}_{A^e}(A,A) \otimes_R R_M \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{A_M^e}(A_M, A_M^e) & \xrightarrow{\phi'_M} & \mathrm{Hom}_{A_M^e}(A_M,A_M) \end{array}$$

são isomorfismos (ver apêndice, Prop A-9). Como, por hipótese, A_M é um A_M^e-módulo projetivo então ϕ'_M é sobrejetivo (ver Apêndice, Prop A-1) e, consequentemente, $\phi' \otimes 1$ é sobrejetivo, para todo ideal maximal M de R. Logo ϕ' é sobrejetivo (ver Apêndice, Prop. A-8) e, portanto, a sequência exata $0 \to J(A) \to A^e \xrightarrow{\phi} A \to 0$ cinde, ou seja, A é uma R-álgebra separável ■

O teorema 2.11 reduz o estudo de álgebras separáveis ao caso local. Os dois teoremas seguintes nos permitem reduzir o estudo da separabilidade ao caso de corpos.

(2.13) TEOREMA: Seja A uma R-álgebra finitamente gerada como R-módulo. Então A é R-separável se , e somente se , A/MA é R/M-separável para todo ideal maximal M de R.

DEMONSTRAÇÃO: Seja M um ideal maximal de R . Desde que $A/MA \cong A_M/MA_M$ e $R_M/MR_M \cong R/M$ (ver Apêndice, Prop. A-7), podemos supor R um anel local com ideal maximal M. Suponhamos A separável sobre R. Desde que $A \otimes_R R/M = A/MA$ e $R \otimes_R R/M \cong R/M$. o resultado segue. Reciprocamente, suponhamos que A/MA é R/M-separável. Indicamos $\overline{X} = X/MX = X \otimes_R R/M$ para todo R-módulo X. Então $\overline{A^e} = \overline{A}^e$ e $J(\overline{A}) = \overline{J(A)}$ (cf . demonstração da Proposição 2.6). Seja $\delta: A \to J(A)$ a derivação dada por $\delta(a) = a \otimes 1^o - 1 \otimes a^o$, para todo $a \in A$, e seja $\overline{\delta}$ a derivação induzida por δ em $\overline{A}$. Por hipótese $\overline{\delta}$ é interior, então $\overline{\delta}(\overline{a}) = \overline{\delta}(\overline{a})\overline{x}_o$ para algum $\overline{x}_o \in J(\overline{A})$. Também $J(\overline{A}) = \overline{A}\delta(\overline{A}) = \overline{A}\,\overline{\delta}(\overline{A})x_o$. Desde que $\overline{J(A)} = J(A)/MJ(A) = J(\overline{A})$, temos que $J(\overline{A}) = J(A)x_o + MJ(A)$ onde $x_o \in J(A)$ é tal que $\overline{x}_o = x_o + MJ(A)$. Como A é finitamente gerado sobre R, segue que $J(A) = A\delta(A)$ é finitamente gerado sobre R. Portanto pelo Lema de Nakayama (ver Apêndice, Cor. A-3) temos que $J(A) = J(A)x_o$. Seja $f: A^e \to J(A)$ o homomorfismo de A^e-módulos definido por $f(y) = yx_o$ $(y \in A^e)$

e seja $i: J(A) \to A^e$ a inclusão. A aplicação $f \circ i$ é sobrejetiva pois $J(A) = J(A)x_o$, e como $J(A)$ é finitamente gerado sobre R segue que $f \circ i$ é também injetora (ver Apêndice, Cor. A-4). Portanto $f \circ i$ é um isomorfismo. Logo existe $g: J(A) \to J(A)$ tal que $g \circ f \circ i = id$. Seja então $h = g \circ f$. Portanto a sequência exata $0 \to J(A) \to A^e \xrightarrow{\phi} A \to 0$ cinde, ou seja, A é separável sobre R ∎

(2.14) TEOREMA: Seja S uma R-álgebra comutativa e finitamente gerada como R-álgebra. São equivalentes:

i) S é separável sobre R

ii) $S \otimes_R K(P)$ é separável sobre $K(P)$, para todo ideal primo P de R ($K(P) = R_P/PR_P$).

DEMONSTRAÇÃO:

i) ⇒ ii) decorre da Proposição 2.6 acima.

ii) ⇒ i) De acordo com o Corolário 2.4 acima basta mostrar que $\Omega(S) = J(S)/J(S)^2 = 0$. Para termos isto é suficiente provar que $\Omega(S)_Q = 0$, para todo ideal primo Q de S (ver Apêndice, Prop. A-8). Sejam então Q um ideal primo de S e $P = Q \cap R$. Passando de R para R_P e de S para S_P, vemos que podemos supor sem perda de generalidade que R é um anel local de ideal maximal P e $K(P) = R/P$. Desde que $J(S) \otimes_R K(P) = J(S \otimes_R K(P))$ (cf. demonstração da Prop. 2.6), temos $\Omega(S) \otimes_R K(P) =$

$= \Omega(S \otimes_R K(P))$ e, consequentemente $\Omega(S)_Q / (P\Omega(S))_Q = \left(\Omega(S)/P\Omega(S)\right)_Q =$

$= (\Omega(S) \otimes_R K(P))_Q = (\Omega(S \otimes_R K(P)))_Q = 0$, por hipótese (cf. Corolário 2.4). Logo, $\Omega(S)_Q = (P\,\Omega(S))_Q$. O resultado decorrerá, agora, do Lema de Nakayama (ver Apêndice, Cor. A-3) se mostrarmos que $\Omega(S)_Q$ é um S_Q-módulo finitamente gerado. De fato, como S é uma R-álgebra finitamente gerada sejam $\{x_i : 1 \leq i \leq n\}$ seus geradores. Já sabemos que os elementos $(x_i \otimes 1 - 1 \otimes x_i)$, $1 \leq i \leq n$, geram J(S) como S⊗S-módulo (cf. demonstração do Lema 2.12). Se denotamos por $\overline{(x_i \otimes 1 - 1 \otimes x_i)}$, $1 \leq i \leq n$, as correspondentes classes módulo $J(S)^2$, temos: $a \otimes b\,\overline{(x_i \otimes 1 - 1 \otimes x_i)} =$

$= [ab \otimes 1 - a(b \otimes 1 - 1 \otimes b)]\,\overline{(x_i \otimes 1 - 1 \otimes x_i)} = (ab \otimes 1)\overline{(x_i \otimes 1 - 1 \otimes x_i)} -$

$- a\overline{(b \otimes 1 - 1 \otimes b)(x_i \otimes 1 - 1 \otimes x_i)} = ab \otimes 1\,\overline{(x_i \otimes 1 - 1 \otimes x_i)}$, o que mostra que $\Omega(S)$ é finitamente gerado como S-módulo e, consequentemente, também $\Omega(S)_Q$ como S_Q-módulo ∎

Concluimos este parágrafo com um resultado (Teorema 2.17) que permite dividir o estudo de separabilidade em duas partes: álgebras comutativas e álgebras centrais.

(2.15) DEFINIÇÃO: Uma R-álgebra A é dita *central* se é fiel como R-módulo e se Z(A) = centro(A) = R. Se, além disso, A é R-separável dizemos que A é uma R-*álgebra central separável*.

Se R é um corpo e A uma R-álgebra central separável, então A é semisimples, isto é, um produto finito de anéis simples A_i (cf. Teorema 1.16 do Capítulo I). Desde que o centro de A é R temos que existe somente um A_i, ou seja, A

é simples e tem centro R. Para um anel comutativo R, uma R-álgebra central separável não é necessariamente simples, mas seus ideais maximais são da forma IA com I um ideal maximal de R. Com efeito, consideremos um ideal maximal M de A e seja $I = M \cap R$. Logo A/M é simples e o centro de A/M é R/I, e consequentemente R/I é corpo (pois tomando $0 \neq a \in Z(A/M)$ temos que $A/M\, a\, A/M = A/M\, a$ é um ideal não nulo de A/M. Então $A/M = A/M\, a$ e portanto existe $b \in A/M$ tal que $ba = 1$, e claramente $b \in Z(A/M)$). Temos também que A/IA é uma R/I-álgebra central separável. Portanto A/IA é semisimples e consequentemente A/IA é simples. Assim IA é um ideal maximal de A e M = IA.

(2.16) LEMA: Seja A uma R-álgebra central separável. Então A é um R-módulo finitamente gerado e projetivo.

DEMONSTRAÇÃO: Notemos, inicialmente, que A^e é também uma R-álgebra central separável (cf. Prop. 2.5). Seja e um idempotente de separabilidade de A. Então A^e e A^e é um ideal da R-álgebra central separável A^e. Se este ideal for próprio, existirá um ideal próprio I de R tal que A^e e $A^e \subset I A^e$ e IA^e é próprio. Aplicando $\phi: A^e \to A$ (a aplicação A^e-linear dada pelo produto) a esta inclusão, obtemos que A = IA e portanto $A^e = IA^e$ que é uma contradição. Portanto A^e e $A^e = A^e$. Seja, então, $a_i, b_i \in A^e$ $(i = 1,\ldots,n)$ com $1 \otimes 1^o = \sum_{i=1}^{n} a_i$ e b_i. Desde que $(1 \otimes a^o)e = (a \otimes 1^o)e$, para todo $a \in A$, podemos assumir que

$a_i = x_i \otimes 1^o$ com $x_i \in A$. Observemos, agora, que $Z(A) = eA$. De fato: $eA \subset A$ (pois A é um A^e-módulo) e $(ea)b = (1 \otimes b^o)ea = (b \otimes 1^o)ea = b(ea)$, para todo $a,b \in A$, o que mostra que $eA \subset Z(A)$. Reciprocamente, escrevendo $e = \sum_i \alpha_i \otimes \beta_i^o$, temos $ex = (\sum_i \alpha_i \otimes \beta_i^o)x = \sum_i \alpha_i x \beta_i = (\sum_i \alpha_i \beta_i)x = \phi(e)x = x$, para todo $x \in Z(A)$, o que mostra que $Z(A) \subset eA$.

Logo, para cada eb_i considerado acima, temos $(eb_i)a = e(b_i a) \in eA = Z(A) = R$, para todo $a \in A$. Sejam $f_i : A \to R$ as aplicações lineares dadas por $f_i(a) = (eb_i)a$, para todo $a \in A$, $1 \leq i \leq n$. Claramente, todo $a \in A$ pode ser escrito na forma $a = (1 \otimes 1^o)a = (\sum_{i=1}^{n} a_i e b_i)a = \sum_{i=1}^{n} f_i(a)x_i$, o que mostra que o conjunto $\{x_i, f_i : 1 \leq i \leq n\}$ é uma base projetiva para A sobre R (ver Apêndice, Teorema A-1). Portanto A é um R-módulo projetivo finitamente gerado ∎

Decorre deste Lema 2.16 e do Teorema 2.9 o seguinte Teorema.

(2.17) TEOREMA: Uma R-álgebra A é separável se, e somente se, A é separável sobre $Z(A)$ e $Z(A)$ é separável sobre R.

CAPÍTULO III

SEPARABILIDADE, RAMIFICAÇÃO E DIFERENTE

Neste capítulo apresentamos um estudo da noção de ramificação (segundo Auslander e Buchsbaum [AB]) e suas propriedades, assim como um estudo da relação existente entre esta noção e a noção de separabilidade. Abordamos também, neste capítulo, a noção de diferente e exibimos situações onde não ramificação é decidível a partir de condições sobre o diferente.

Neste capítulo a letra R denotará sempre um anel comutativo com elemento identidade. Assumimos também que em todo este capítulo os anéis (e, por conseguinte, todas as álgebras) considerados são comutativos com elemento identidade.

Com o intuito de uma maior clareza possível, julgamos necessário algumas considerações iniciais sobre a notação e terminologia que utilizamos ao longo deste capítulo.

Começamos por observar que dado um anel R, uma R-álgebra é um anel junto com um homomorfismo de anéis $f : R \longrightarrow S$. Se Q é um ideal primo de S, o ideal $f^{-1}(Q)$ de R é chamado *contração* de Q e é denotado por $Q \cap R$. Também consideremos o quociente $R/_{Q\cap R}$ como sendo um subanel de $S/_{Q}$, sendo que a identificação, neste caso, é dada pelo monomorfismo induzido por f. Se $x \in R$, denotamos $f(x)$ em S por x, desde que isto não cause nenhuma confusão. Da mesma forma, se I é um ideal de R,

denotamos o ideal $f(I)S$ simplesmente por IS. É claro que $IS \cap R \supset I$. Os únicos sistemas multiplicativos de R que consideramos são aqueles que não interceptam o núcleo de f. Também neste caso denotamos $f(U)$ em S por U. Se U é um sistema multiplicativo de R e U' é um sistema multiplicativo de S contendo U (isto é, $U' \supset f(U)$) então $f : R \longrightarrow S$ induz um homomorfismo $f' : R_U \longrightarrow S_{U'}$ o que dá à $S_{U'}$ uma estrutura de R_U-álgebra. Em particular se Q é um ideal primo de S e $P = Q \cap R$ então S_Q é uma R_p-álgebra e R_P/PR_P é um subcorpo de S_Q/QS_Q.

§1. RAMIFICAÇÃO E SEPARABILIDADE

(1.1) DEFINIÇÃO: Seja S uma R-álgebra. Um ideal primo Q de S é dito *não ramificado* se $P = Q \cap R$ satisfaz as seguintes propriedades:

a) $PS_Q = QS_Q$

b) S_Q/PS_Q é um corpo extensão separável e finita de R_P/PR_P.

A R-álgebra S é dita *não ramificada*, se:

a) todo ideal primo de S é não ramificado.

b) para todo ideal primo P de R existe somente um número finito de ideais primos Q de S tais que $P = Q \cap R$.

(1.2) EXEMPLOS:

a) Seja Q o conjunto dos números racionais considerado como uma $\mathbf{Z}$-álgebra. Então Q é não ramificada. Com efeito, seja $q \in Q$ um ideal primo. Então $q = (0)$ e consequentemente $p = (0) = q \cap \mathbf{Z}$. Claramente $pQ_q = qQ_q$ e $\frac{Q_q}{qQ_q} = Q$ é um corpo extensão separável de $\frac{\mathbf{Z}_p}{p\mathbf{Z}_p} = Q$. Agora, desde que $(0) \subset Q$ é o único ideal primo acima de $(0) \subset \mathbf{Z}$, segue-se que Q é uma $\mathbf{Z}$-álgebra não ramificada.

b) Seja q um número primo. Então a $\mathbf{Z}$-álgebra $S = \mathbf{Z}/q\mathbf{Z}$ é não ramificada. Com efeito, seja $Q = (0) = (\bar{q})$ o único ideal primo de S (S é corpo). Seja $P = (q) = Q \cap \mathbf{Z}$. Obviamente $PS_Q = QS_Q$, e desde que $\mathbf{Z}_P/P\mathbf{Z}_P$ é isomorfo a S (ver Apêndice, Prop. A-7) seque-se que $\frac{S_Q}{QS_Q} = S$ é um corpo extensão separável de $\frac{\mathbf{Z}_p}{P\mathbf{Z}_P}$. Finalmente, desde que $(0) \subset S$ é o único ideal **primo** acima de $(q) \subset \mathbf{Z}$ segue-se que S é uma $\mathbf{Z}$-álgebra não ramificada.

c) Sejam p e q primos distintos, ξ_p uma raiz p-ésima primitiva da unidade, $\mathbf{Z}_{(q)} = R$ e $S = \mathbf{Z}_{(q)}[\xi_p] = (\mathbf{Z}[\xi_p])_{(q)}$. Afirmamos que S é uma R-álgebra não ramificada. De fato, observemos que os únicos ideais primos de $\mathbf{Z}_{(q)}$ são (0) e $q\mathbf{Z}_{(q)}$. Se $P = (0)$ e $U = R - P$, é imediato que $R_U/PR_U = Q$ e $\frac{S_U}{PS_U} = Q(\xi_p)$, ou seja, S_U/PS_U é, obviamente, uma R_U/PR_U-álgebra separável. Sejam, agora, $P = q\mathbf{Z}_{(q)}$ e $U = R - P$. Desde que P é um ideal

maximal de R e (q) é um ideal maximal de $\mathbb{Z}$, decorre da Prop. (A-7) do Apêndice que: $R_{\mathcal{U}}/_{PR_{\mathcal{U}}} = R_P/_{PR_P} \simeq R/_{PR} = \mathbb{Z}_{(q)}/_{q\mathbb{Z}_{(q)}}$

$\simeq \frac{\mathbb{Z}}{q\mathbb{Z}} = \mathbb{F}_q$ e $S_{\mathcal{U}}/_{PS_{\mathcal{U}}} \simeq S_P/_{PS_P} \simeq S/_{PS} = \mathbb{Z}[\xi_p]_{(q)}/_{q(\mathbb{Z}[\xi_p])_{(q)}}$

$\simeq \mathbb{Z}[\xi_p]/_{q\mathbb{Z}[\xi_p]}$. Por outro lado, decorre da proposição (A-12) do Apêndice que existem ideais maximais $Q_1,\ldots,Q_s$ de $\mathbb{Z}[\xi_p]$ tais que $q\mathbb{Z}[\xi_p] = Q_1 \ldots Q_s = Q_1 \,..\, Q_s$. Logo $S_{\mathcal{U}}/_{PS_{\mathcal{U}}} \simeq \mathbb{Z}[\xi_p]/_{q\mathbb{Z}[\xi_p]} \simeq \mathbb{Z}[\xi_p]/_{Q_1} \oplus$

$\oplus \ldots \oplus \mathbb{Z}[\xi_p]/_{Q_s}$ (cf. A-10 do Apêndice) e cada $\mathbb{Z}[\xi_p]/_{Q_i}$ é um corpo extensão finita (pois $\mathbb{Z}[\xi_p]$ é finitamente gerado sobre $\mathbb{Z}$) e separável sobre $\mathbb{F}_p$ (pois $\mathbb{F}_p$ é um corpo perfeito). Consequentemente, $S_{\mathcal{U}}/_{PS_{\mathcal{U}}}$ é também neste caso, uma $R_{\mathcal{U}}/_{PR_{\mathcal{U}}}$-álgebra separável. O resultado, agora, decorre do Teorema 1.3 abaixo.

(1.3) TEOREMA: Seja S uma R-álgebra. São equivalentes:

i) S é uma R-álgebra não ramificada

ii) Para todo ideal primo P de R tal que $P = Q \cap R$, para algum ideal primo Q de S, tem-se que $S_P/_{PS_P}$ é uma $R_P/_{PR_P}$-álgebra separável.

DEMONSTRAÇÃO:

i) $\Longrightarrow$ ii) Observemos inicialmente, que se P é um ideal

primo de R, então R_P é um anel local de ideal maximal PR_P. Além disso, para cada ideal primo Q de S tal que $Q \cap R = P$ temos $R - P \subset S - Q$ e, por conseguinte,

$$(PS_P)(S_P)_{QS_P} = PS_Q \quad , \quad (QS_P)(S_P)_{QS_P} = QS_Q \quad \text{e}$$

$$\frac{(S_P)_{QS_P}}{(QS_P)(S_P)_{QS_P}} = \frac{S_Q}{QS_Q} \quad \text{(ver Apêndice, Prop. (A-5)).}$$

Isto posto, podemos supor, sem perda de generalidade, que R é um anel local de ideal maximal P e, neste caso, $\frac{S_P}{PS_P} \simeq \frac{S}{PS}$ e $R/P = R_P/PR_P$ (ver Apêndice, Prop. (A-7)).

Seja Q um ideal primo de S tal que $Q \cap R = P$. O quociente S/Q é uma R/P-álgebra de integridade com corpo de frações S_Q/QS_Q. Como S_Q/QS_Q é uma extensão finita de R/P segue-se que S/Q é integral sobre R/P e consequentemente é um corpo, obviamente coincidente com S_Q/QS_Q. Isto prova que todo ideal primo Q de S tal que $Q \cap R = P$ é maximal. Sejam $Q_1,\ldots,Q_t$ os únicos ideais primos de S satisfazendo $Q_i \cap R = P$ e mostremos que $PS = Q_1 \cap \ldots \cap Q_t$. Obviamente, $PS \subseteq Q_1 \cap \ldots \cap Q_t$. Mostraremos a igualdade, verificando-a localmente para todo ideal maximal Q de S (ver Apêndice, Prop. (A-8)). Se $Q = Q_i$ para algum $1 \leq i \leq t$, da maximalidade dos Q_j segue-se que $Q_j S_{Q_i} = S_{Q_i}$, para todo $j \neq i$ e, consequentemente,

$(Q_1 \cap \ldots \cap Q_t)S_{Q_i} = Q_1S_{Q_i} \cap \ldots \cap Q_iS_{Q_i} \cap \ldots \cap Q_tS_{Q_i} = Q_iS_{Q_i} =$
$= PS_{Q_i}$ (pois Q_i é não ramificado). Se $Q \neq Q_i$, para todo $i = 1,\ldots,t$, claramente temos:

$PS_Q = S_Q = (Q_1S_Q) \cap \ldots \cap (Q_tS_Q) = (Q_1 \cap \ldots \cap Q_t)S_Q$.

Portanto $PS = Q_1 \cap \ldots \cap Q_t$ e como os Q_i são comaximais, temos $S/_{PS} = S/_{Q_1S} \oplus \ldots \oplus S/_{Q_tS}$ (ver Apêndice, Prop. (A-10)). O resultado, agora, segue do fato que $S/_{Q_iS} = S_{Q_i}/_{Q_iS_{Q_i}}$ (ver Apêndice, Prop. (A-7)) e do Corolário 2.6 do capítulo I.

ii) $\Longrightarrow$ i) Levando-se em consideração as identificações do início desta demonstração e a bijeção entre os ideais primos de S_P e os ideais primos Q de S tais que $Q \cap R = P$ (ver Apêndice, Prop. (A-6)), podemos supor novamente, sem perda de generalidade, que R é um anel local de ideal maximal P. Por hipótese, $S_P/_{PS_P} = S/_{PS}$ é uma $R/_P$-álgebra separável. Logo $\frac{S}{PS} = L_1 \oplus \ldots \oplus L_t$ onde cada L_i é um corpo extensão separável e finita de $R/_P$ (cf. Corolário 2.6 do Capítulo I). Sejam $m_i = L_1 \oplus \ldots \oplus L_{i-1} \oplus \{0\} \oplus L_{i+1} \oplus \ldots \oplus L_t$, $1 \leq i \leq t$, os únicos ideais primos (e obviamente maximais) de $\frac{S}{PS}$ e sejam $Q_i \subset S$, $1 \leq i \leq t$, os únicos ideais primos de S contendo PS e tais que $\frac{Q_i}{PS} = m_i$. Da maximalidade de P em R segue-se que $Q_i \cap R = P$. Além disso, é fácil de ver que $\frac{S}{Q_i} = L_i$, $1 \leq i \leq t$. Disto seque-se que $\frac{S}{\bigcap\limits_{1 \leq i \leq t} Q_i} = \frac{S}{Q_1} \oplus \ldots \oplus \frac{S}{Q_t} = L_1 \oplus \ldots \oplus L_t = \frac{S}{PS}$.

Como $PS \subset \bigcap_{1 \leq i \leq t} Q_i$, segue-se a igualdade e, consequentemente, $PS_{Q_j} = (\bigcap_{1 \leq i \leq t} Q_i)S_{Q_j} = Q_j S_{Q_j}$, para todo $j = 1,\ldots,t$. ∎

Como consequência imediata deste teorema e da Proposição 2.6 do Capítulo II, temos a seguinte proposição:

(1.4) PROPOSIÇÃO: Se S é uma R-álgebra separável então S é não ramificada.

DEMONSTRAÇÃO: Basta observar que para todo primo P de R , $S_P/PS_P = S \otimes_R R_P/PR_P$. O resultado agora, decorre trivialmente da Proposição 2.6 do Capítulo II e do Teorema 1.3 acima. ∎

A questão que agora se coloca naturalmente é a seguinte: "vale a recíproca da Proposição 1.4 ?". Não temos uma resposta afirmativa para esta questão e nem tampouco um contra-exemplo.

Contudo, temos os seguintes resultados:

(1.5) TEOREMA: Seja S uma R-álgebra finitamente gerada como R-álgebra. São equivalentes:

i) S é separável

ii) S é não ramificada.

DEMONSTRAÇÃO: Resta apenas verificar que ii) $\Longrightarrow$ i) e isto decorre do Teorema 1.3 acima e do Teorema 2.14 do Capítulo II. ∎

(1.6) TEOREMA: Seja S um anel noetheriano e uma R-álgebra tal que $J(S) = \ker(S \otimes_R S \xrightarrow{\phi} S)$ é um ideal finitamente gerado de $S \otimes_R S$. São equivalentes:

i) S é separável

ii) S é não ramificada

iii) Todo ideal maximal de S é não ramificado

iv) Toda R-derivação de S em um S-módulo finitamente gerado é nula.

Para a demonstração deste teorema necessitamos dos seguintes dois lemas:

(1.7) LEMA: Seja S um anel noetheriano e uma R-álgebra tal que todo ideal maximal de S é não ramificado. Então toda R-derivação d de S em um S-módulo E finitamente gerado é nula.

DEMONSTRAÇÃO: Seja M um ideal maximal de S e $m = M \cap R$. Denotemos por E_M o S_M-módulo $E \otimes_S S_M$ e por $d_M : S_M \longrightarrow E_M$ a derivação induzida por $d : S \longrightarrow E$. Desde que M é não ramificado, $mS_M = MS_M$. Desde que d é uma derivação sobre R, d_M é uma derivação sobre R_m tal que $d_M(MS_M) = d_M(mS_M) \subset mE_M = ME_M$. Portanto d_M induz uma derivação $\overline{d}_M : S_M/MS_M \longrightarrow E_M/ME_M$ sobre R_m/mR_m. De M não ramificado segue-se que S_M/MS_M é um corpo extensão separável e finita de R_m/mR_m e, consequentemente, $\overline{d}_M = 0$ (cf. Teorema 3.4 do Cap. I). Portanto $d_M(S_M) \subset ME_M$.

Disto seque-se que $d_M(MS_M) = d_M(mS_M) \subset md_M(S_M) \subset mME_M \subset M^2E_M$ e consequentemente, d_M induz também uma derivação $\bar{d}_M : S_M/MS_M \longrightarrow E_M/M^2E_M$. Pelo mesmo argumento usado acima segue-se que $\bar{d}_M = 0$, ou seja, $d_M(S_M) \subset M^2E_M$. A repetição desse mesmo argumento leva-nos a concluir que $d_M(S_M) \subset \cap M^iE_M = 0$ (ver Apêndice, Prop. (A-11)). ∎

(1.8) LEMA: Seja I um ideal finitamente gerado de R tal que $I^2 = I$. Então existe $x \in I$ tal que $yx = x$, para todo $y \in I$ e $I = (x)$.

DEMONSTRAÇÃO: Seja $I = (x_1,\ldots,x_n)$. De $I = I^2$ segue-se que $x_i = \sum_{k,j=1}^{n} \lambda_{kj} x_k x_j = \sum_j c_{ij} x_j$ com $c_{ij} = \lambda_{kj} x_k \in I$, para todo $i = 1,\ldots,n$. Consequentemente, temos

$$\sum_j (\delta_{ij} - c_{ij})x_j = 0 \quad \text{onde} \quad \delta_{ij} = \begin{cases} 1 & \text{se } j = i \\ 0 & \text{se } j \neq i \end{cases}.$$

Considerando $D = (d_{ij})$, com $d_{ij} = \delta_{ij} - c_{ij}$, obtemos

$$D \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{e, portanto, det } D \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Desde que $\det D = 1 - x$ para algum $x \in I$, concluímos que $y(1 - x) = 0$, ou seja, $yx = x$, para todo $y \in I$. Agora, é imediato ver que $I = (x)$. ∎

DEMONSTRAÇÃO DO TEOREMA 1.6:

i) $\Longrightarrow$ ii) pela proposição 1.4

ii) $\Longrightarrow$ iii) óbvio

iii) $\Longrightarrow$ iv) pelo lema 1.7

iv) $\Longrightarrow$ i) Para mostrar a separabilidade de S é suficiente verificar que a sequência exata

$0 \longrightarrow J(S) \longrightarrow S \otimes_R S \xrightarrow{\phi} S \longrightarrow 0$ cinde (cf. Teorema 1.1 do Cap. II). Observemos inicialmente que para qualquer S-módulo E, $\mathrm{Hom}_S(J(S)/J(S)^2, E)$ é isomorfo ao grupo $\mathrm{Der}_R(S,E)$ das R-derivações de S em E. Considerando $E = J(S)/J(S)^2$ e observando que $J(S)/J(S)^2$ é um S-módulo finitamente gerado, pois $J(S)$ o é como $S \otimes_R S$-módulo (ver a demonstração do teorema 2.14 do Cap. II), temos que $\mathrm{Hom}_S(J(S)/J(S)^2, J(S)/J(S)^2) = 0$ o que implica $J(S)/J(S)^2 = 0$ ou $J(S) = J(S)^2$. Desde que $J(S)$ é finitamente gerado, do Lema 1.8 decorre, então, que existe $x_o \in J(S)$ tal que $yx_o = y$, para todo $y \in J(S)$. Definimos, então, o homomorfismo de $S \otimes_R S$-módulos $p : S \otimes_R S \longrightarrow J(S)$ dado por $p(1) = x_o$. De $p(y) = yp(1) = yx_o = y$, para todo $y \in J(S)$, segue que a sequência exata de $S \otimes_R S$-módulos, dada acima, cinde. ∎

§2. RAMIFICAÇÃO E DIFERENTE

(2.1) DEFINIÇÃO: Sejam S uma R-álgebra e $\phi : S \otimes_R S \longrightarrow S$ o

homomorfismo de $S \otimes_R S$-módulos dado por $\phi(x \otimes y) = xy$. Seja $J(S) = \text{Ker}\ \phi$ e N o anulador de $J(S)$ em $S \otimes_R S$. O ideal $\phi(N)$ em S é chamado o *diferente homológico* da R-álgebra S e denotado por $\mathcal{D}_{S/R}$.

Pode ser visto facilmente, a partir das diversas definições equivalentes de separabilidade dados no Teorema 1.1 do Capítulo II, que uma R-álgebra S é separável se, e somente se, $\mathcal{D}_{S/R} = S$.

Consequentemente, se S é uma R-álgebra nas condições do Teorema 1.5 ou do Teorema 1.6 o mesmo pode ser afirmado sobre a não ramificação de S, isto é, S é não ramificado se, e somente se, $\mathcal{D}_{S/R} = S$.

Indo um pouco mais além, damos a seguir um resultado que permite decidir via diferente (obviamente dentro das condições do Teorema) quando um dado ideal de uma R-álgebra é não ramificado.

(2.2) TEOREMA: Seja S uma R-álgebra satisfazendo uma das seguintes condições:

i) S é uma R-álgebra finitamente gerada como R-módulo.

ii) R e S estão nas condições do Teorema 1.6.

Então, um ideal primo Q de S é não ramificado se, e somente se, Q não contém $\mathcal{D}_{S/R}$.

DEMONSTRAÇÃO: Sejam Q um ideal primo de S, $P = Q \cap R$,

$U = S - Q$ e $V = R - P$. Então S_U é uma R_V-álgebra, $S_U \otimes_R S_U = S_U \otimes_{R_V} S_U$, $J(S_U) = \ker(\bar{\phi} : S_U \otimes_{R_V} S_U \longrightarrow S_U)$, e $N_{U\otimes U}$ é o anulador de $J(S_U)$. Mais ainda, S_U e R_V estão nas condições de i) ou ii) se S e R, respectivamente, também estão.

Suponhamos que Q não contém $\mathcal{D}_{S/R}$. Então $(\mathcal{D}_{S/R})_U = S_U = \bar{\phi}(N_{U\otimes U})$ e, portanto, S_U é R_V-separável. Da Proposição 1.4 decorre que S_U é não ramificada e, agora, é fácil ver que Q é não ramificado.

Reciprocamente, suponhamos que Q não é ramificado. Então QS_U é não ramificado sobre R_V. No caso i) temos então S_U/PS_U extensão separável de R_V/PR_V e, portanto pelo Teorema 2.13 do Capítulo II decorre que S_U é R_V-separável. No caso ii) desde que QS_U é o único ideal maximal de S_U, decorre do Teorema 1.6 que S_U é, também R_V-separável. Em ambos os casos, portanto, temos $(\mathcal{D}_{S/R})_U = \bar{\phi}(N_{U\otimes U}) = S_U$, o que acarreta que Q não contém $\mathcal{D}_{S/R}$. ∎

APÊNDICE

Em todo este apêndice a letra R designará um anel comutativo com elemento identidade.

(A-1) PROPOSIÇÃO: ([KO], Lemme I.1.1). Sejam A um anel e M um R-módulo. As seguintes afirmações são equivalentes:

a) M é isomorfo a um somando direto de um R-módulo livre.

b) Toda sequência exata de R-módulos

$0 \longrightarrow L \longrightarrow N \xrightarrow{\varphi} M \longrightarrow 0$ cinde; isto é, existe um homomorfismo de R-módulos $\rho : M \longrightarrow N$ tal que $\varphi \circ \rho = 1_M$.

c) Para toda aplicação sobrejetiva de R-módulos $\varphi : N \longrightarrow N'$ a aplicação induzida $\varphi' : \mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_R(M,N')$ também é sobrejetiva.

d) Existe um conjunto $\{m_i, f_i : i \in I\}$ com $m_i \in M$ e $f_i \in M^* = \mathrm{Hom}_R(M,R)$, tal que

1) para todo $m \in M$, $f_i(m) = 0$, exceto para um número finito de $i \in I$.

2) para todo $m \in M$, $\sum_{i \in I} f_i(m) m_i = m$.

Todo R-módulo M que satisfaz uma das propriedades equivalentes da Proposição (A-1) é chamado R-*módulo projetivo*. Além disso, se o conjunto I considerado em d), for finito, dizemos também que M é finitamente gerado. O conjunto $\{x_i, f_i : i \in I\}$ é

chamado *base projetiva* de M sobre R.

(A-2) PROPOSIÇÃO: ([KO], Lemme I.2.2). Sejam M um R-módulo finitamente gerado e I um ideal de R tal que IM = M. Então existe um elemento $a \in I$ tal que $(1 - a)M = 0$.

(A-3) COROLÁRIO: (Lema de Nakayama) ([KO], Corollaire I.2.3). Seja I um ideal de R. São equivalentes:

i) $I \subset rad(R)$

ii) $1 + I$ é um subgrupo do grupo das unidades de R. Além disso, para todo R-módulo finitamente gerado **M e todo submódulo N de M**

iii) IM = M implica M = 0

iv) **M = IM + N** implica N = M.

(A-4) COROLÁRIO: ([KO], Corollaire I.2.4). Todo endomorfismo sobrejetivo de um R-módulo finitamente gerado é um isomorfismo.

(A-5) PROPOSIÇÃO: ([B], Ch. II, §2, nº 3, Prop. 7). Sejam U e V sistemas multiplicativos de R. Seja $V' = \{\frac{v}{u} : v \in V, u \in U\} \subseteq$ $\subseteq U^{-1}R = R_U$.

i) Existe um único isomorfismo j do anel $(UV)^{-1}R = R_{UV}$ sobre o anel $V'^{-1}(U^{-1}R) = (R_U)_{V'}$ tal que o diagrama

$$\begin{array}{ccc} R & \xrightarrow{i_R^U} & U^{-1}R = R_U \\ \Big\downarrow{\scriptstyle i_R^{UV}} & & \Big\downarrow{\scriptstyle i_{R_U}^{V'}} \\ (UV)^{-1}R = R_{UV} & \xrightarrow{j} & V'^{-1}(U^{-1}R) = (U_U)_{V'} \end{array}$$

é comutativo.

ii) Seja M um R-módulo. Existe um isomorfismo k do R_{UV}-módulo $(UV)^{-1}M = M_{UV}$ sobre o $R(U)_{V'}$-módulo $V'^{-1}(U^{-1}M) = (M_U)_{V'}$ tal que o diagrama

$$\begin{array}{ccc} M & \xrightarrow{i_M^U} & M \\ \Big\downarrow{\scriptstyle i_M^{UV}} & & \Big\downarrow{\scriptstyle i_{M_U}^{V'}} \\ M_{UV} & \xrightarrow{k} & (M_U)_{V'} \end{array}$$

é comutativo.

(A-6) PROPOSIÇÃO: ([B], Ch. II, §2, nº 5, Prop. 11 ou [AMD], Prop. 3.11). Seja U um sistema multiplicativo de R. Os ideais primos de $U^{-1}R = R_U$ estão em correspondência bijetora ($P \longrightarrow U^{-1}P = P$) com os ideais primos de R que não interceptam U.

(A-7) PROPOSIÇÃO: ([B], Ch. II, §3, Prop. 9). Sejam m um ideal maximal de R e M um R-módulo. O homomorfismo canônico $M \longrightarrow M_m/mM_m$ é sobrejetivo, tem núcleo ηM e define um isomorfismo de M/mM sobre M_m/mM_m.

(A-8) PROPOSIÇÃO: ([KO], Corollaire 3.4).

a) Sejam M e N R-módulos e $\varphi : M \longrightarrow N$ um homomorfismo de R-módulos. Então φ é injetor (resp. sobrejetor) se, e somente se, o homomorfismo $\varphi_m : M_m \longrightarrow N_m$ é injetor (resp. sobrejetor), para todo ideal maximal m de R.

b) Sejam M e N submódulos de um R-módulo P. Então $M = N$ se, e somente se, $N_m = M_m$, para todo ideal maximal m de R.

Um R-módulo M é chamado de *apresentação finita* se existe uma sequência exata

$$F_1 \longrightarrow F_o \longrightarrow M \longrightarrow 0$$

onde F_o e F_1 são R-módulos finitamente gerados e F_o é livre

Um R-módulo N é chamado *plano* se toda sequência exata de R-módulos

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$$

induz uma sequência exata

$$N \otimes_R M' \xrightarrow{1 \otimes \alpha} N \otimes_R M \xrightarrow{1 \otimes \beta} N \otimes_R M''$$

(A-9) PRCPOSIÇÃO: ([KO], Lemme I.4.1). Sejam A_j , i=1,2, R-álgebras e M_i, N_i , A_i-módulos. O homomorfismo canônico

$$\mathrm{Hom}_{A_1}(M_1,N_1) \otimes_R \mathrm{Hom}_{A_2}(M_2,N_2) \longrightarrow \mathrm{Hom}_{A_1 \otimes_R A_2}(M_1 \otimes_R M_2, N_1 \otimes_R N_2)$$

induzido pela aplicação R-bilinear $(f_1,f_2) \longrightarrow f_1 \otimes f_2$ é um isomorfismo nos seguintes casos:

a) M_i é um A_i-módulo projetivo e finitamente gerado, i=1,2.

b) M_1 e N_1 são projetivos e finitamente gerado sobre A_1, A_1 é plano e M_2 é de apresentação finita sobre A_2.

(A-10) PROPOSIÇÃO: ([AMD], Prop.1.10). Sejam $I_1,\ldots,I_n$ ideais de R. Seja $\varphi : R \longrightarrow \prod_{i=1}^{n} (R/I_i)$ o homomorfismo de anéis dado por $\varphi(x) = (x + I_1,\ldots,x + I_n)$.

a) Se I_i e I_j são coprimos, para $i \neq j$, então $\prod_{1\leq i\leq n} I_i = \bigcap_{1\leq i\leq n} I_i$.

b) φ é sobrejetor $\iff$ I_i, I_j são coprimos, para $i \neq j$.

c) φ é injetor $\iff$ $\bigcap_{1\leq i\leq n} I_i = (0)$.

(A-11) PROPOSIÇÃO: ([AMD], Corol.10.19). Sejam R um anel noetheriano , I um ideal de R contido em rad(R) e seja M um R-módulo finitamente gerado. Então $\bigcap_n I^n M = 0$.

(A-12) PROPOSIÇÃO: ([E], Corolário 14.5). Sejam $m \in \mathbb{Z}$, $m \geq 1$, $\phi_m \in \mathbf{Z}[x]$ o correspondente polinômio ciclotômico e ξ_m uma raiz m-ésima primitiva da unidade. Seja $q \in \mathbf{Z}$ um número primo tal que q não divide m. Sejam $f_1,\ldots,f_r \in \mathbf{Z}[x]$ polinômios mônicos tais que suas imagens $\bar{f}_i$ módulo $q\mathbf{Z}[x]$ são irredutíveis em $\mathbf{Z}[x]/_{q\mathbf{Z}[x]} = \mathbf{F}_q[x]$ e $\phi_m \equiv f_1 \ldots f_r (\text{mod. } q\,\mathbf{Z}[x])$. Então:

a) $q\mathbf{Z}[\xi_m] = \mathcal{B}_1 \ldots \mathcal{B}_r$, onde $\mathcal{B}_j = (q, f_j(\xi_m))$, $1 \leq j \leq r$, são os ideais primos de $\mathbf{Z}[\xi_m]$ tais que $\mathcal{B}_i \cap \mathbf{Z} = (q)$.

b) $\mathbf{Z}[\xi_m] / \mathcal{B}_j = \mathbf{F}_q(\bar{\gamma}_j)$ para alguma raiz $\bar{\gamma}_j$ de $\bar{f}_j$, $1 \leq j \leq r$.

BIBLIOGRAFIA

[AB] - M. AUSLANDER, D. BUCHSBAUM; On ramification theory in noetherian rings, Am. J. Math. 81 (1959), 749-765.

[AMD] - M.F. ATIYAH, I.G. MACDONALD; Introduction to commutative Algebra, Addison-Wesley, 1969.

[B] - N. BOURBAKI; Algèbre Commutative, Chapitre I et II, Hermann, 1961.

[CR] - C.W. CURTIS, I. REINER; Representation theory of finite groups and associative algebras, Interscience, 1962.

[E] - O. ENDLER; Teoria dos números algébricos, Projeto Euclides, IMPA, 1986.

[F] - B. FELZENZSWALB; Álgebras de dimensão finita, IMPA, 1979.

[KO] - M.A. KNUS, M. OJANGUREN; Théorie de la descente et Algèbres d'Azumaya, L.N. in Math. 389, Springer-Verlag, 1974.

[OS] - M. ORZECH, C. SMALL; The Brawer Group of Commutative Rings, Marcel Dekker, 1975.

[RE] - I. REINER; Maximal Orders, Academic Press, 1975.

[RI] - P. RIBEMBOIM; Rings and Modules, Wiley, 1969.

[S] - P. SAMUEL; Théorie algebrique de nombres, Hermann, 1971.

[W] - S.S.S. WANG; Separable algebras and free cubic extensions, PhD - Thesis, Cornell University, 1975.