Universidade Federal do Rio Grande do Sul
Instituto de Matemática

EXTENSÕES SEPARÁVEIS DE ANÉIS COMUTATIVOS

Dissertação de Mestrado *

CYDARA SPERB CAVEDON

Porto Alegre, novembro de 1981.

* Este trabalho foi realizado com bolsas de estudo do CNPq e CAPES

Dissertação realizada sob a orientação do Dr. MIGUEL A. FERRERO e apresentada ao Instituto de Matemática da UFRGS em preenchimento parcial dos requisitos para a obtenção do título de Mestre em Matemática.

AGRADECIMENTO

a todos os professores integrantes do Curso de Pós-Graduação deste Instituto, em especial a meu orientador, Miguel Ferrero, por todo o envolvimento e dedicação com que sempre me atendeu.

SUMÁRIO

CAPÍTULO IV

APRESENTAÇÃO

Este trabalho de dissertação constitui-se basicamente do estudo de polinômios separáveis sobre anéis comutativos com unidade, ou, equivalentemente, de álgebras separáveis que são quocientes de um anel de polinômios.

Os capítulos I, II e III referem-se a conteúdos que são pré-requisito a tal estudo. No Capítulo I desenvolvemos os conteúdos básicos utilizados, tais como produto tensorial, módulos projetivos, posto de módulos projetivos e finitamente gerados, Teoria de Galois de Corpos, etc. O segundo capítulo contém definição e propriedades de álgebras separáveis sobre um anel comutativo com unidade. Nele é mostrado que este conceito de separabilidade é uma generalização do conceito de separabilidade envolvido na Teoria de Corpos. No Capítulo III, apresentamos um estudo detalhado sobre Extensões Galoisianas de Anéis Comutativos.

O objetivo central deste trabalho é desenvolvido no Capítulo IV. Nele, basicamente, apresentamos caracterizações distintas para a separabilidade de polinômios, e este conteúdo está baseado fundamentalmente nos trabalhos de Elkins, Janusz e Nagahara (ver bibliografia).

Fazemos a seguinte convenção: uma citação do tipo I.4.5 representa o 5º resultado da 4ª seção do Capítulo I, enquanto que 4.5 representa o 5º resultado da 4ª seção do capítulo que está sendo apresentado no momento.

CAPÍTULO I

INTRODUÇÃO

Neste capítulo apresentamos alguns dos conceitos e resultados que serão utilizados ao longo deste trabalho. Muitos outros, no entanto, são supostos conhecidos pelo leitor, como, por exemplo, conceitos e resultados básicos de Teoria de Gupós e Teoria de Anéis. Algumas questões referentes a tais assuntos podem, no entanto, ser consultadas em [10] e [25]. Ao longo de todo este capítulo, a maioria dos resultados citados não são acompanhados da respectiva demonstração. O leitor pode consultar as referências que serão feitas oportunamente.

Em todo este trabalho, os anéis considerados têm unidade. Quando necessário, a unidade de um anel A será denotada por 1_A. Além disso, supomos que todo subanel considerado tem unidade igual à unidade do anel que o contém e todo homomorfismo de anéis envia a unidade na unidade.

Ainda, $U(A)$ e $Aut(A)$ representam, respectivamente, o conjunto dos elementos inversíveis e o conjunto de todos os automorfismos do anel A. O anel dos inteiros é denotado por Z e ∂f denota o grau de um polinômio f.

Os assuntos abordados nesse primeiro capítulo são: módulos, os functores Hom e Produto Tensorial, definição e exemplos de álgebras, posto de módulos projetivos, extensões de Galois de corpos comutativos e anéis semi-simples. A menos de menção em contrário, os anéis aqui considerados não são necessariamente comutativos.

§ 1. MÓDULOS

Se R é um anel (com unidade), um R-MÓDULO À ESQUERDA M é um grupo abeliano (com notação aditiva), no qual está definida uma aplicação $R \times M \to M$, denominada OPERAÇÃO EXTERNA DO R-MÓDULO, que associa a cada par $(r, m) \in R \times M$ um elemento de M que denotamos por $r.m$ (ou simplesmente rm) e que satisfaz as seguintes condições:

a) $r.(r'.m) = (rr').m$

b) $r.(m+m') = r.m + r.m'$

c) $(r+r').m = r.m + r'.m$

d) $1_R.m = m$, para cada $r, r' \in R$, $m, m' \in M$.

Assim, se S é um subanel de R, então R é um S-módulo, onde a operação externa é a própria multiplicação do anel R. Ainda, qualquer grupo abeliano é um módulo sobre o anel dos inteiros.

Analogamente, define-se R-MÓDULO À DIREITA. No entanto, a menos de menção em contrário, o termo R-MÓDULO significará para nós R-módulo à esquerda.

É fácil verificar que se T é um anel e $\phi : R \to T$ é um homomorfismo de anéis, então T é um R-módulo e todo T-módulo M é também um R-módulo, se definimos $r.m = (r.1_T).m$, para cada $r \in R$, $m \in M$. Neste caso, dizemos que M é o R-MÓDULO INDUZIDO (PELA ESTRUTURA DE T-MÓDULO).

Um subgrupo aditivo N do grupo $(M, +)$ é um SUBMÓDULO do R-módulo M se $r.n \in N$, para cada $r \in R$, $n \in N$. Se N_1 e N_2 são submódulos de um R-módulo M então o conjunto $N_1 + N_2 = \{n_1 + n_2 \mid n_1 \in N_1, n_2 \in N_2\}$ é também um R-submódulo de M, e é denominado SUBMÓDULO SOMA DE N_1 e N_2. Ainda, dizemos que um R-submódulo N de M é um R-SOMANDO DIRETO de M se existe um R-submódulo N' de M tal que $N \oplus N' = M$ ($\oplus$ representa uma soma direta, isto é, $N + N' = M$ e $N \cap N' = (0)$).

A seguinte proposição é de fácil demonstração.

Proposição 1.1 (Lei Modular)

Se M e N são dois R-módulos e M' é um R-submódulo de M então $M' \cap (M \oplus N) = M' \oplus (M' \cap N)$.

Se M e N são dois R-módulos, dizemos que uma aplicação $f: M \to N$ é um R-HOMOMORFISMO DE M em N se f é um homomorfismo dos grupos subjascentes tal que $f(r.m) = r.f(m)$, para cada $r \in R$, $m \in M$. Quando um R-homomorfismo $f : M \to N$ é uma aplicação injetora, então dizemos que f é um R-MONOMORFISMO e, se f é sobrejetora, então a aplicação é denominada R-EPIMORFISMO. No caso em que f é uma bijeção então ela é dita um R-ISOMORFISMO. A notação $\mathrm{Hom}_R(M, N)$ representa o conjunto de todos os R-homomorfismos de M em N.

Quando possível, utilizaremos apenas o termo homomorfismo, ao invés de R-homomorfismo.

Podemos observar que se M e N são dois R-módulos então o conjunto $\mathrm{Hom}_R(M, N)$ é um grupo abeliano, se considerarmos a adição usual de funções. Além disso, se R é um anel comutativo então M e N são R-módulos à esquerda e à direita, e $\mathrm{Hom}_R(M, N)$ torna-se um R-módulo, se definirmos $(r.f)(m) = r.f(m)$, para cada $r \in R$, $m \in M$, $f \in \mathrm{Hom}_R(M, N)$, como é fácil verificar.

Uma seqüência de R-módulos M_i com $i \in I$ e R-homomorfismos $f_i : M_{i-1} \to M_i$, para cada $i \in I$ (onde I denota um conjunto enumerável de índices), $\ldots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \ldots$, é denominada uma SEQÜÊNCIA EXATA se $\mathrm{Im}\, f_i = \mathrm{Ker}\, f_{i+1}$, para cada $i \in I$. Em particular, a seqüência $0 \to M \xrightarrow{f} N$ é exata se e só se f é um monomorfismo, enquanto que a seqüência $M \xrightarrow{g} N \to 0$ é exata se e só se g é um epimorfismo. Assim, $0 \to M \xrightarrow{f} N \to 0$ é uma seqüência exata se e só se f é um R-isomorfismo.

Uma seqüência de R-módulos e R-homomorfismos da forma $0 \to M \xrightarrow{f} N \xrightarrow{g} L \to 0$ é denominada SEQÜÊNCIA CURTA, e é dita EXATA À ESQUERDA se f é um monomorfismo e $\mathrm{Im}\, f = \mathrm{Ker}\, g$. Tal seqüência é dita ainda EXATA À DIREITA se g é um epimorfismo e $\mathrm{Im}\, f = \mathrm{Ker}\, g$, e é simplesmente EXATA se for exata à esquerda e à direita.

Dizemos que uma seqüência exata curta de R-módulos e R-homomorfismos $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ CINDE se o R-submódulo $N' = \mathrm{Im}\, f = \mathrm{Ker}\, g$ de N é um R-somando direto de M . Com respeito a esta definição, temos o seguinte resultado, cuja prova

pode ser encontrada em [15].

Proposição 1.2:

Dada uma seqüência exata de R-módulos e R-homomorfismos $0 \to M \xrightarrow{f} N \xrightarrow{g} L \to 0$, as seguintes condições são equivalentes:

(a) a seqüência cinde;

(b) existe um homomorfismo $\psi : N \to M$ tal que $\psi \circ f = id_M$;

(c) existe um homomorfismo $\phi : L \to N$ tal que $g \circ \phi = id_L$;

(d) existem R-homomorfismos $\psi : N \to M$ e $\phi : L \to N$ tais que $\psi \circ f = id_M$ e $g \circ \phi = id_L$ e $f \circ \psi + \phi \circ g = id_N$.

Nestas condições, $N \simeq M \oplus L$ como R-módulos.

Se m é um elemento de um R-módulo M então o conjunto de todos os "múltiplos" da forma $r.m$ com $r \in R$ é um R-submódulo de M, denotado por $R.m$. Se $M = \sum_{i \in I} R.m_i$, onde I é um conjunto de índices qualquer, então o conjunto $\{m_i\}_{i \in I}$ é denominado CONJUNTO DE GERADORES DE M. Isto significa que cada elemento de M pode ser expresso (não necessariamente de maneira única) como uma combinação linear finita dos elementos $m_i (i \in I)$. Se M possui um conjunto finito de geradores então ele é dito um R-MÓDULO FINITAMENTE GERADO.

Dizemos que um R-módulo M é LIVRE se ele é isomorfo a uma soma direta de R-módulos isomorfos a R, ou seja,

$M \simeq \bigoplus_{i \in I} M_i$, onde $M_i \simeq R$, para cada $i \in I$, onde I é um conjunto de índices. Neste caso, é comum utilizarmos a notação $R^{(I)}$ para $\bigoplus_{i \in I} M_i$. Ainda, se I é um conjunto finito com n elementos, a soma $R \oplus \ldots \oplus R$ (n somandos) é denotada por $R^{(n)}$.

Lema 1.3:

Um R-módulo M é livre se e só se existe um subconjunto $\{b_i\}_{i \in I}$ de M (para algum conjunto de índices I) que satisfaz as seguintes condições:

(a) $M = \sum_{i \in I} R.b_i$, ou seja, todo elemento $m \in M$ pode ser escrito na forma $m = \sum_{j \in I'} r_j.b_j$, onde cada $r_j \in R$ e I' é um subconjunto finito de I ;

(b) para cada subconjunto finito $I' \subset I$, $\sum_{i \in I'} r_i.b_i = 0$ implica $r_i = 0$, para cada $i \in I'$.

Neste caso, o conjunto gerador $\{b_i\}_{i \in I}$ é denominado BASE de M . Ainda, a decomposição dada no item (a) é única, para cada $m \in M$.

Quando R é um anel comutativo, pode-se mostrar que se um R-módulo livre M tem uma base finita com n elementos, então qualquer outra base de M tem também n elementos. Neste caso, este inteiro n é denominado POSTO DE M (ver § 4). Ainda, é claro que um módulo sobre um corpo é um espaço vetorial e, portanto, é livre.

A prova da seguinte porposição pode também ser encontrada em [25]:

Proposição 1.4:

Se R é um anel comutativo e se L_1 e L_2 são dois R-módulos livres de posto respectivamente iguais a m e n, então $\mathrm{Hom}_R(L_1,L_2)$ e $M_{m\times n}(R)$ são R-módulos isomorfos e livres, de posto igual a mn.

Concentramos agora nossa atenção nos chamados módulos projetivos.

Proposição 1.5:

Seja M um R-módulo. As seguintes condições são equivalentes:

(i) M é isomorfo a um R-somando direto de algum R-módulo livre;

(ii) toda seqüência exata de R-módulos e R-homomorfismos da forma $0 \to L \xrightarrow{f} N \xrightarrow{g} M \to 0$ é uma seqüência que cinde;

(iii) para cada diagrama de R-módulos e R-homomorfismos da forma

$$\begin{array}{ccc} & & M \\ & & \downarrow g \\ L & \xrightarrow{f} & N \end{array} \to 0$$

, onde f é um R-epimorfismo, existe um R-homomorfismo $h : M \to L$ que torna o diagrama comutativo, ou seja, tal que $fh = g$;

(iv) existe um conjunto de elementos $m_i \in M$ e de R-homomorfismos $f_i : M \to R$, onde $i \in I$ (I é um conjunto de índices) tais que:

(a) para cada $m \in M$, $f_i(m) = 0$ quase sempre (isto é, com exceção de um número finito de índices $i \in I$);

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

Além disso, tal conjunto de índices I pode ser escolhido finito se e só se M é um R-módulo finitamente gerado.

Dizemos que M é um R-MÓDULO PROJETIVO (ou, simplesmente, que M é R-PROJETIVO) se é satisfeita alguma das condições equivalentes da proposição anterior.

É claro então que todo módulo livre é projetivo. Ainda, da alínea (iii) da proposição anterior, é fácil ver que se existe um R-epimorfismo $f : R \to M$ então M é R-projetivo se e só se existe um R-homomorfismo $h : M \to R$ tal que $fh = id_M$.

O conjunto de elementos $m_i \in M$ e R-homomorfismos $f_i : M \to R$ ($i \in I$) dados na alínea (iv) da proposição anterior, são chamadas COORDENADAS PROJETIVAS DO R-MÓDULO M.

Listamos a seguir mais algumas propriedades de módulos finitamente gerados e de módulos projetivos. Maiores detalhes podem ser encontrados nas referências citadas.

Proposição 1.6 (Transitividade de módulos finitamente gerados e projetivos)

Sejam S um anel e $\phi : R \to S$ um homomorfismo de anéis. Seja M um S-módulo. Então:

(i) se M é projetivo sobre S e S é projetivo sobre R então M é projetivo sobre R;

(ii) se M é finitamente gerado sobre S e S é também finitamente gerado sobre R então M é finitamente gerado sobre R;

(iii) se M é finitamente gerado como R-módulo então é também finitamente gerado como S-módulo.

Proposição 1.7:

Seja M um R-módulo e seja N um R-somando direto de M . Então:

(i) se M é um R-módulo projetivo então N é também um R-módulo projetivo;

(ii) se M é um R-módulo finitamente gerado então N é também R-finitamente gerado.

Mais propriedades serão dadas na próxima seção.

Para encerrar esta seção, lembramos que se M é um R-módulo, então o R-ANULADOR DE M é o subanel de R formado pelos elementos $r \in R$ que satisfazem $r.M = 0$, ou seja,

$An_R(M) = \{r \in R \mid r.M = 0\}$. Se $An_R(M) = 0$, então M é dito um R-MÓDULO FIEL. Quando R é um anel comutativo e sem idempotentes próprios (i.e., os únicos idempotentes de R são 0 e 1) então é válida a seguinte proposição (ver corolário 1.11, capítulo 1, de [7]).

Proposição 1.8:

Se R é um anel comutativo sem idempotentes próprios então todo R-módulo não nulo, finitamente gerado e projetivo é fiel.

§ 2 . CATEGORIAS E FUNTORES DE MÓDULOS

Neste trabalho fazemos uso das categorias cujos objetos são módulos. Omitimos então a definição geral de

CATEGORIA e nos restringimos apenas a categorias de módulos sobre um dado anel. Assim, por exemplo, dado um anel com unidade R, ${}_R\mathcal{M}$ denota a categoria dos R-módulos à esquerda. Ou seja, os objetos de ${}_R\mathcal{M}$ são os R-módulos à esquerda e os morfismos são os elementos de $\mathrm{Hom}_R(M,N)$, i.é, os R-homomorfismos de M em N (onde M e N são dois quaisquer R-módulos à esquerda). Analogamente, $\mathcal{M}_R$ denota a categoria dos R-módulos à direita e dos R-homomorfismos entre tais R-módulos.

Sejam $\mathcal{C}$ e $\mathcal{D}$ duas categorias de módulos. Um FUNTOR COVARIANTE DE $\mathcal{C}$ EM $\mathcal{D}$ é uma correspondência F que associa a cada módulo M de $\mathcal{C}$ um módulo $F(M)$ de $\mathcal{D}$ e a cada homomorfismo $f : M \to N$ de $\mathcal{C}$ um homomorfismo $F(f) : F(M) \to F(N)$ de $\mathcal{D}$, de tal modo que:

(i) $F(\mathrm{id}_M) = \mathrm{id}_{F(M)}$

(ii) se f,g são homomorfismos de $\mathcal{C}$ tais que o produto fg está definido, então $F(fg) = F(f)F(g)$.

Um funtor F de $\mathcal{C}$ em $\mathcal{D}$ é dito EXATO À ESQUERDA se para toda seqüência exata de módulos em $\mathcal{C}$ da forma $0 \to L \to M \to N \to 0$, a seqüência $0 \to F(L) \to F(M) \to F(N)$ é também exata em $\mathcal{D}$. Analogamente, F é dito um FUNTOR EXATO À DIREITA se para toda seqüência exata de módulos e homomorfismos de $\mathcal{C}$ $0 \to L \to M \to N \to 0$, a seqüência $F(L) \to F(M) \to F(N) \to 0$ é também uma seqüência exata em $\mathcal{D}$. Se F é um funtor exato à direita e também à esquerda então dizemos simplesmente que F é EXATO. Ou seja, F é exato se transforma seqüências exatas curtas em seqüências exatas curtas.

De maneira análoga podemos definir funtor contravariante: se $\mathcal{C}$ e $\mathcal{D}$ são duas categorias de módulos, en-

tão um FUNTOR CONTRAVARIANTE DE C EM $\mathcal{D}$ é uma correspondência F' que associa a cada módulo $M \in C$ um módulo $F'(M) \in \mathcal{D}$ e a cada homomorfismo $f : M \to N$ de C um homomorfismo $F'(f) : F(N) \to F(M)$, de tal modo que

(i) $F'(id_M) = id_{F'(M)}$;

(ii) se f,g são homomorfismos de C tais que o produto fg está definido então $F'(fg) = F'(g)F'(f)$.

A exatidão de um funtor contravariante define-se de maneira análoga.

Neste trabalho, consideraremos vários exemplos de funtores.

Suponhamos agora que F e F' são dois funtores covariantes de uma categoria de módulos C em outra categoria de módulos $\mathcal{D}$. Dizemos que F e F' são FUNTORES NATURALMENTE EQUIVALENTES se, para todo módulo M de C existe um isomorfismo $\phi_M : F(M) \to F'(M)$ em $\mathcal{D}$ tal que, para cada par de módulos M,N de C e para cada homomorfismo $f \in \mathrm{Hom}_C(M, N)$, o diagrama

$$\begin{array}{ccc} F(M) & \xrightarrow{F(f)} & F(N) \\ {\scriptstyle \phi_M}\downarrow & & \downarrow{\scriptstyle \phi_N} \\ F'(M) & \xrightarrow{F'(f)} & F'(N) \end{array}$$

é comutativo.

Restringimos agora nossa atenção a dois funtores que serão utilizados por nós: o produto tensorial e o Hom.

A. PRODUTO TENSORIAL

Sejam M um R-módulo à direita, N um R-módulo à esquerda e L um grupo abeliano arbitrário. Uma aplicação $f : M \times N \to L$ é dita uma FORMA R-BILINEAR se

i) $f(m+m',n) = f(m,n) + f(m',n)$

ii) $f(m,n+n') = f(m,n) + f(m,n')$

iii) $f(m.r,n) = f(m,r.n)$, para cada $m,m' \in M$, $n,n' \in N$, $r \in R$.

Proposição 2.1 (Propriedade Universal do Produto Tensorial)

Sejam M um R-módulo à direita e N um R-módulo à esquerda. Então existe um grupo abeliano, que vamos denotar por $M \otimes_R N$, e uma única aplicação R-bilinear $g : M \times N \to M \otimes_R N$ com a seguinte propriedade: se G é um grupo abeliano arbitrário e $f : M \times N \to G$ é uma forma R-bilinear, então existe um único homomorfismo de R-módulos $f^* : M \otimes_R N \to G$ tal que $f^* g(m,n) = f(m,n)$, para cada $m \in M$, $n \in N$. Além disso, tal grupo $M \otimes_R N$ é único, salvo isomorfismo. Indicaremos cada imagem $g(m,n)$ por $m \otimes n$.

O grupo abeliano $M \otimes_R N$ dado na proposição acima é denominado PRODUTO TENSORIAL DE M E N e é gerado pelos elementos da forma $m \otimes n$, com $m \in M$, $n \in N$. Além disso, como a aplicação g é uma forma R-bilinear, são válidas as seguintes propriedades:

a) $(m + m') \otimes n = m \otimes n + m' \otimes n$

b) $m \otimes (n + n') = m \otimes n + m \otimes n'$

c) $m.r \otimes n = m \otimes r.n$, para cada $m,m' \in M$, $n,n' \in N$, $r \in R$.

Às vezes pode ser possível dotar um produto tensorial $M \otimes_R N$ de uma estrutura de módulo, como vemos a seguir.

Dado um anel S , denotemos por ${}_R M_S$ a categoria cujos objetos são os módulos N que são R-módulos à esquerda, S-módulos à direita e que satisfazem ainda a seguinte propriedade: para cada $r \in R$, $s \in S$, $n \in N$, $(r.n).s = r.(n.s)$. Os morfismos de ${}_R M_S$ são os homomorfismos de grupos que são R-homomorfismos à esquerda e S-homomorfismos à direita. Neste caso, os objetos de ${}_R M_S$ são denominados também de R-S-BIMÓDULOS.

Desta maneira, se M é um R-módulo à direita e se $N \in {}_R M_S$, então o produto tensorial $M \otimes_R N$ tem uma estrutura de S-módulo à direita, cuja operação externa é dada por $(\sum_{i=1}^{n} m_i \otimes n_i).s = \sum_{i=1}^{n} m_i \otimes n_i.s$, para cada $\sum_{i=1}^{n} m_i \otimes n_i \in M \otimes_R N$, $s \in S$.

É claro, portanto, que se R é um anel comutativo, então o produto tensorial $M \otimes_R N$ é um R-módulo à esquerda e à direita, já que cada R-módulo é um R-R-bimódulo.

NOTA: Geralmente, daremos uma definição envolvendo elementos de um produto tensorial $M \otimes_R N$ em termos dos geradores $m \otimes n$. De fato, estaremos utilizando a propriedade universal do produto tensorial para estender esta definição, por linearidade, a um elemento arbitrário $\sum_{i=1}^{n} m_i \otimes n_i \in M \otimes_R N$. Por exemplo, a de-

finição acima da operação externa do S-módulo $M \otimes_R N$ poderia ter sido dado apenas em termos dos geradores, i.e., $(m \otimes n).s = m \otimes n.s$, para cada $m \otimes n \in M \otimes_R N$, $s \in S$, da seguinte maneira. Fixado $s \in S$, a aplicação $f_s : M \times N \to M \otimes_R N$ dada por $f_s(m,n) = m \otimes n.s$ é uma forma R-bilinear e, portanto, existe um único R-homomorfismo $\overline{f}_s : M \otimes_R N \to M \otimes_R N$ tal que $\overline{f}_s(m \otimes n) = (f_s \circ g)(m,n) = m \otimes n.s$, para cada $m \otimes n \in M \otimes_R N$. Então, sendo $\overline{f}_s$ um homomorfismo, é claro que

$$\left(\sum_{i=1}^{n} m_i \otimes n_i \right).s = \sum_{i=1}^{n} m_i \otimes n_i.s \text{ , para cada } \sum_{i=1}^{n} m_i \otimes n_i \in M \otimes_R N .$$

A seguir listamos algumas propriedades que são resultados conhecidos sobre produto tensorial:

1. Se R e S são anéis e $L \in {}_R M$, $M \in {}_R M_S$, $N \in {}_S M$, então os grupos abelianos $(L \otimes_R M) \otimes_S N$ e $L \otimes_R (M \otimes_S N)$ são isomorfos, através da aplicação $(\ell \otimes m) \otimes n \to \ell \otimes (m \otimes n)$, para cada $(\ell \otimes m) \otimes n \in (L \otimes_R M) \otimes_S N$, como é fácil verificar.

2. Para qualquer anel R e $M \in {}_R M$, os grupos M e $R \otimes_R M$ são isomorfos, através da aplicação $r \otimes m \to r.m$, para cada $r \otimes m \in R \otimes_R M$, cuja aplicação inversa é dada por $m \to 1 \otimes m$, para cada $m \in M$, como é fácil constatar.

3. Dados $M, M' \in {}_R M$, $N, N' \in {}_R M$ e dois homomorfismos $f \in \mathrm{Hom}_R(M,M')$ e $g \in \mathrm{Hom}_R(N,N')$, pode-se mostrar que a aplicação $m \otimes n \mapsto f(m) \otimes g(n) \in M' \otimes_R N'$, para cada $m \otimes n \in M \otimes N$, é bem definida e é um homomorfismo de grupos de $M \otimes_R N$ em

$M' \otimes_R N'$. Costumamos denotar esta aplicação por $f \otimes g$.

4. O produto tensorial "distribui-se" sobre uma soma direta. Mais precisamente, se $\{M_i\}_{i \in I}$ e $\{N_j\}_{j \in J}$ são coleções de R-módulos à direita e à esquerda, respectivamente (onde I e J são conjuntos de índices), então

$$\left(\bigoplus_{i \in I} M_i \right) \otimes_R \left(\bigoplus_{j \in J} N_j \right) \simeq \bigoplus_{\substack{i \in I \\ j \in J}} (M_i \otimes_R N_j)$$

5. Se fixarmos um R-módulo à direita M , então $M \otimes_R ( )$ pode ser considerado um funtor covariante da categoria ${}_R\mathcal{M}$ na categoria dos grupos abelianos (ou seja, na categoria ${}_Z\mathcal{M}$ dos módulos sobre o anel dos inteiros). De fato, a cada $N \in {}_R\mathcal{M}$ associamos o Z-módulo $M \otimes_R N$ e a cada $f \in \mathrm{Hom}_R(N,N')$ o homomorfismo $id_M \otimes f \in \mathrm{Hom}_Z(M \otimes_R N , M \otimes_R N')$. Analogamente, $( ) \otimes_R N$ é um funtor de $\mathcal{M}_R$ em ${}_Z\mathcal{M}$, como é fácil verificar.

A seguinte proposição é verificada, e sua prova pode ser encontrada em [2] (prop. 2.18, cap. 2) ou em [24] .

Proposição 2.2:

i) Se $0 \to N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3 \to 0$ é uma seqüência exata de R-módulos à esquerda então a seqüência

$M \otimes_R N_1 \xrightarrow{id_M \otimes f} M \otimes_R N_2 \xrightarrow{id_M \otimes g} M \otimes_R N_3 \to 0$ é também exata, para cada R-módulo à direita M . Ou seja, $M \otimes_R ( )$ é um funtor exato à direita;

(ii) se $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ é uma seqüência exa

ta de R-módulos à direita, então a seqüência

$M_1 \otimes_R N \xrightarrow{f \otimes id_M} M_2 \otimes_R N \xrightarrow{g \otimes id_M} M_3 \otimes_R N \to 0$ é também exata, para cada R-módulo à esquerda N. Ou seja, $(\ ) \otimes_R N$ é um funtor exato à direita;

(iii) se $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ é uma seqüência exata e cinde, então a seqüência

$0 \to M_1 \otimes_R N \xrightarrow{f \otimes id_M} M_2 \otimes_R N \xrightarrow{g \otimes id_M} M_3 \otimes_R N \to 0$ é também exata e cinde, para cada R-módulo à esquerda N.

Se $(\ ) \otimes_R M$ é um funtor exato, i.e., se $(\ ) \otimes_R M$ é também um funtor exato à esquerda, dizemos que M é um R-módulo PLANO. Definição análoga é feita para módulos à direita.

Nem todo R-módulo à esquerda é plano. No entanto, é válida a seguinte

Proposição 2.3:

Todo módulo livre é plano. Mas ainda, todo módulo projetivo é plano.

No caso de ser R um anel comutativo, é válida a seguinte

Proposição 2.4:

Se R é um anel comutativo, $M \in {}_R M$ e $N \in {}_R M$, então

i) se M e N são R-módulos finitamente gerados,

então $M \otimes_R N$ é também um R-módulo finitamente gerado;

ii) se M e N são R-projetivos então $M \otimes_R N$ é também R-projetivo.

Mais detalhes sobre produto tensorial podem ser encontrados em [5].

B. O **FUNTOR** HOM

Se M e N são dois R-módulos, então o conjunto $\mathrm{Hom}_R(M,N)$ dos R-homomorfismos de M em N é um grupo abeliano, se considerarmos a adição usual de funções. Além disso, se M (ou N) é um bimódulo, por exemplo, se $M \in {}_R M_S$, para algum anel S, então $\mathrm{Hom}_R(M,N)$ pode ser tornado um S-módulo à esquerda, se definimos $(s.f)(m) = f(m.s)$, para cada $s \in S$, $m \in M$, $f \in \mathrm{Hom}_R(M,N)$. Para apresentar um segundo exemplo, denotamos por ${}_{R-S}M$ a categoria de todos os módulos à esquerda sobre R e também sobre S, com a seguinte propriedade: se $M \in {}_{R-S}M$, então $r.(s.m) = s.(r.m)$, para cada $r \in R$, $s \in S$, $m \in M$. Então, neste caso, $\mathrm{Hom}_R(M,N)$ é também um S-módulo à direita, onde a operação externa é dada por $(f.s)(m) = f(s.m)$, para cada $s \in S$, $m \in M$, $f \in \mathrm{Hom}_R(M,N)$.

Ainda, como último exemplo, se $N \in {}_{R-S}M$, então $\mathrm{Hom}_R(M,N)$ tem uma estrutura de S-módulo à esquerda, cuja operação externa é dada por $(s.f)(m) = s.f(m)$, para cada $s \in S$, $m \in M$, $f \in \mathrm{Hom}_R(M,N)$.

Portanto, é claro que, se R é um anel comutativo, então $\mathrm{Hom}_R(M,N)$ é um R-módulo à esquerda e à direita.

Fixado um R-módulo M, podemos considerar o funtor $\mathrm{Hom}_R(M,-)$ que associa a cada R-módulo N o grupo abeliano $\mathrm{Hom}_R(M,N)$ e, a cada R-homomorfismo $f : N \to N'$ a aplicação $\overline{f} = \mathrm{Hom}_R(id_M, f) : \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M,N')$, dada por $\mathrm{Hom}_R(id_M, f)(g) = f \circ g$, para cada $g \in \mathrm{Hom}_R(M,N)$.

Analogamente, pode-se definir o funtor $\mathrm{Hom}_R(-,N)$ da categoria ${}_R\mathcal{M}$ na categoria dos grupos abelianos ${}_Z\mathcal{M}$. Este funtor é contravariante, como é fácil verificar.

A prova da proposição a seguir pode ser encontrada em [2] (prop. 2.9, cap. 2).

Proposição 2.5:

i) seja $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ uma seqüência de R-módulos e R-homomorfismos. Então ela é uma seqüência exata se e só se, para cada R-módulo N, a seqüência induzida $0 \to \mathrm{Hom}_R(M'',N) \xrightarrow{\overline{g}} \mathrm{Hom}_R(M,N) \xrightarrow{\overline{f}} \mathrm{Hom}_R(M',N)$ é exata. Em outras palavras, $\mathrm{Hom}_R(-,N)$ é um funtor contravariante exato à esquerda, para cada R-módulo N.

ii) seja $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ uma seqüência de R-módulos e R-homomorfismos. Então esta seqüência é exata se e só se, para cada R-módulo M, a seqüência induzida $0 \to \mathrm{Hom}_R(M,N') \xrightarrow{\overline{f}} \mathrm{Hom}_R(M,N) \xrightarrow{\overline{g}} \mathrm{Hom}_R(M,N'')$ é exata. Ou seja, $\mathrm{Hom}_R(M,-)$ é um funtor covariante exato à esquerda.

iii) se $0 \to N' \to N \to N'' \to 0$ é uma seqüência exata e cinde então a seqüência $0 \to \mathrm{Hom}_R(M,N') \xrightarrow{\overline{f}} \mathrm{Hom}_R(M,N) \xrightarrow{\overline{g}} \mathrm{Hom}_R(M,N'') \to 0$ é também exata e cinde, para cada R-módulo M.

Vemos então que $\mathrm{Hom}_R(M,-)$ não é necessariamente um funtor exato à direita. De fato, $\mathrm{Hom}_R(M,-)$ é exato se e só se M é um R-módulo projetivo.

Outras propriedades que serão utilizadas também neste trabalho são as seguintes:

1. Se $M_1,\ldots,M_n$, $N_1,\ldots,N_k$ são R-módulos quaisquer, então $\mathrm{Hom}_R\left(\bigoplus_{i=1}^{n} M_i , \bigoplus_{j=1}^{k} N_j\right) \simeq \bigoplus_{i,j} \mathrm{Hom}_R(M_i,N_j)$.

2. Para cada R-módulo M , $\mathrm{Hom}_R(R,M) \simeq M$, através da aplicação $f \mapsto f(1_R)$, para cada $f \in \mathrm{Hom}_R(R,M)$.

Mais detalhes podem ser encontrados em [24].

§ 3 . DEFINIÇÃO, EXEMPLOS E PROPRIEDADES DAS ÁLGEBRAS

Nesta seção, R denota um anel comutativo (com unidade). Dizemos que um anel A é uma ÁLGEBRA SOBRE R (ou simplesmente, uma R-ÁLGEBRA), se existe um homomorfismo de anéis θ de R no centro do anel A . Se, além disso, A é um anel comutativo, dizemos que A é uma R-ÁLGEBRA COMUTATIVA.

É fácil ver que uma R-álgebra A pode ser considerada um R-módulo à esquerda e à direita. De fato, se $\theta : R \to A$ é o homomorfismo que caracteriza A como R-álgebra,

definimos $r.a = \theta(r)a$ e $a.r = a\,\theta(r)$, para todo $r \in R$ e $a \in A$. Reciprocamente, se A é um R-módulo que satisfaz $r.(a_1 a_2) = (r.a_1)a_2 = a_1(r . a_2)$, para todo $r \in R$ e $a_1, a_2 \in A$, então a aplicação $r \mapsto r.1_A$, para todo $r \in R$, é um homomorfismo de anéis de R no centro de A , como é fácil verificar. Logo, A é uma R-álgebra.

Assim, é válida a seguinte

Proposição 3.1:

Um anel A é uma R-álgebra se e só se A é um R-módulo que satisfaz $r.(a_1 a_2) = (r.a_1)a_2 = a_1(r.a_2)$, para todo $r \in R$ e $a_1, a_2 \in A$.

Apresentemos agora alguns exemplos de R-álgebras:

1. É óbvio que o próprio anel R é uma R-álgebra, via o homomorfismo identidade. Mais geralmente, $R^{(n)} = R \oplus \ldots \oplus R$ (n cópias do anel R) é também uma R-álgebra, via a aplicação diagonal, que associa a cada $r \in R$, a n-upla $(r, r, \ldots, r)$. Esta mesma aplicação diagonal torna o anel $R^{\infty} = R \times R \times \ldots$, das seqüências infinitas, uma R-álgebra.

2. Também o anel $M_n(R)$ das matrizes quadradas de ordem $n \times n$ sobre R é uma R-álgebra. De fato, basta-nos considerar o homomorfismo de anéis que associa a cada elemento $r \in R$ a matriz diagonal rI de $M_n(R)$, onde I representa a matriz unidade de $M_n(R)$.

3. Dados um grupo multiplicativo G e um anel com unidade S , lembramos que o ANEL DE GRUPO DE G SOBRE S

é o conjunto $S[G]$ formado pelas séries formais $\sum_{g \in G} s_g g$, onde cada s_g é um elemento do anel S, e onde o conjunto $\{g \in G \mid s_g \neq 0\}$ é finito. Neste conjunto, estão definidas a operação de adição por $\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G} (r_g + s_g) g$, para todo $\sum_{g \in G} r_g g$, $\sum_{g \in G} s_g g \in S[G]$, e a de multiplicação por $(r_g g)(s_h h) = (r_g s_h)(g h)$, para todos $r_g, s_h \in S$ e $g, h \in G$, junto com uma lei distributiva.

É fácil ver que $S[G]$ tem unidade, e que é um anel comutativo se e só se S é um anel comutativo e G um grupo abeliano. Ainda, é fácil verificar que, definindo o produto externo por

$$s\left(\sum_{g \in G} s_g g\right) = \sum_{g \in G} (s s_g) g \quad , \text{ para todo}$$

$s, s_g \in S$ e $g \in G$, $S[G]$ torna-se um S-módulo livre, com base formada pelos elementos de G. Finalmente, o anel de grupo $R[G]$ é uma R-álgebra, denominada ÁLGEBRA DE GRUPO DE G SOBRE R.

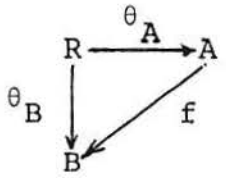
4. É óbvio que o anel de polinômios $R[X]$ com indeterminada X e coeficientes em R é uma R-álgebra, via a aplicação inclusão.

5. Seja W um sistema multiplicativo de R. Então o anel localizado R_W, formado pelos elementos da forma $r/_W$ com $r \in R$, $w \in W$, é um R-módulo à esquerda, cuja operação externa é dada por $r'.r/_W = (r\,r')/_W$, para cada $r, r' \in R$, $w \in W$. Além disso, sendo R um anel comutativo, torna-se óbvio

que R_W é uma R-álgebra comutativa (ver § 4) .

Uma SUBÁLGEBRA de uma R-álgebra A é um subanel S do anel A e que é, ao mesmo tempo, uma R-álgebra, via o mesmo homomorfismo θ que define a R-álgebra A (i.e., S é um subanel de A e um submódulo do R-módulo à esquerda A) .

Dadas duas R-álgebras A e B , dizemos que uma aplicação $f : A \to B$ é um HOMOMORFISMO DE R-ÁLGEBRAS se f é um homomorfismo de anéis e também de R-módulos. Equivalentemente, se $\theta_A : R \to A$ e $\theta_B : R \to B$ definem as estruturas de R-álgebras de A e B , respectivamente, então um homomorfismo de R-álgebras de A em B é um homomorfismo de anéis $f : A \to B$ tal que o seguinte diagrama é comutativo:



Podemos observar agora que, se B e C são anéis comutativos, se A é uma B-álgebra e B é uma C-álgebra, então é claro que A é uma C-álgebra. Ainda, é fácil ver que, se A e B são duas R-álgebras, definindo um produto em $A \otimes_R B$ por $(a \otimes b)(a' \otimes b') = a\,a' \otimes b\,b'$, para cada $a \otimes b$, $a' \otimes b' \in A \otimes_R B$, $A \otimes_R B$ é uma R-álgebra. Portanto, se A e B são R-álgebras comutativas, as estruturas naturais de A-módulo e B-módulo de $A \otimes_R B$ fazem com que este anel possa ser considerado uma álgebra sobre A e B , respectivamente.

Dados dois anéis A e B , relembramos que um

A-B-bimódulo é um grupo abeliano dotado de estruturas de A-módulo à esquerda e B-módulo à direita, satisfazendo ainda a seguinte propriedade:

(i) $(a.m).b = a.(m.b)$, para cada $a \in A$, $b \in B$, $m \in M$.

Se, no entanto, A e B são ainda R-álgebras, então um A-B-bimódulo M que satisfaz

(ii) $r.m = m.r$, para cada $r \in R$, $m \in M$ (isto é, as estruturas de R-módulo induzidas em M coincidem), é denominado um A-B-BIMÓDULO SOBRE R .

No caso de termos $A = B$, um A-A-bimódulo sobre R é também denominado A/R-MÓDULO BILATERAL. (Esta nomenclatura será empregada no próximo capítulo).

Suponhamos agora que A é um anel. Denotemos por A^0 o anel definido da seguinte maneira:
$A = A^0$ como conjuntos (i.e., existe uma correspondência biunívoca entre os elementos de A e A^0 . Denotemos por x^0 o elemento de A^0 que é o correpondente de $x \in A$). Definimos adição em A^0 da mesma maneira que no anel A , isto é, $a^0 + b^0 = (a + b)^0$, para $a^0, b^0 \in A^0$, e definimos também neste conjunto um produto, da seguinte maneira: $a^0 b^0 = (b\,a)^0$, para cada $a^0, b^0 \in A^0$.

Com estas operações, é fácil verificar que A^0 é também um anel, denominado ANEL OPOSTO A A . Ainda, se A é uma R-álgebra, temos que A^0 é também uma R-álgebra, denominada ÁLGEBRA OPOSTA A A , e, se A é uma R-álgebra comutativa, então $A^0 = A$.

A definição da álgebra oposta A^0 nos permite

considerar o produto tensorial $A \otimes_R A^0$, que sabemos ser uma R-álgebra. Denotamos tal R-álgebra por A^e , e a denominamos ÁLGEBRA ENVOLVENTE DE A .

A partir de agora não faremos mais distinção entre um elemento $a \in A$ e seu correpondente $a^0 \in A^0$, indicando ambos por a , simplesmente. Logo, o produto em A^e está definido por $(a \otimes b)(a' \otimes b') = a\,a' \otimes b'\,b$, para cada $a \otimes b$, $a' \otimes b' \in A^e$.

Façamos agora algumas observações sobre os A-B-bimódulos sobre R e A/R-módulos bilaterais que nos serão úteis no próximo capítulo.

1. Sejam A e B duas R-álgebras e M um grupo abeliano. Então se M tem uma estrutura de $A \otimes_R B^0$-módulo à esquerda, pode-se definir sobre M uma estrutura de A-B-bimódulo sobre R . É válida também a recíproca. De fato, se M é um $A \otimes_R B^0$-módulo à esquerda, então é possível definir uma estrutura de A-B-bimódulo sobre R , através das igualdades $a.m = (a \otimes 1).m$ e $m.b = (1 \otimes b).m$, para cada $a \in A$, $b \in B$, $m \in M$, como é fácil verificar. Se M é um A-B-bimódulo sobre R , então, definindo uma operação externa por $(a \otimes b).m = a.m.b$, para cada $a \otimes b \in A \otimes_R B^0$, $m \in M$, é imediato que M é um $A \otimes_R B^0$-módulo à esquerda.

Portanto, em particular, vemos que um grupo abeliano M tem uma estrutura de A/R-módulo bilateral se e só se M tem uma estrutura de A^e-módulo à esquerda.

Dados uma R-álgebra A e um A/R-módulo bilateral M , denotamos por M^A o R-submódulo de M formado pelos

elementos $m \in M$ tais que $a.m = m.a$, para cada $a \in A$, ou seja,

$$M^A = \{m \in M \mid \forall a \in A \ , \ a.m = m.a\} \ .$$

Podemos então considerar a correspondência $(\ )^A$, que associa a cada A/R-módulo bilateral M o R-submódulo M^A , e a cada homomorfismo $f : M \to N$ de A/R-módulos bilaterais o homomorfismo de R-módulos $f|_{M^A} : M^A \to N^A$, onde $f|_{M^A}$ representa a restrição de f ao R-submódulo M^A .

Com referência a esta aplicação, temos o seguinte resultado, cuja prova deixamos a cargo do leitor:

2. Se A é uma R-álgebra, a aplicação $(\ )^A$ é um funtor covariante da categoria dos A/R-módulos bilaterais na categoria dos R-módulos.

Se A é uma R-álgebra e $g : M \to N$ é um homomorfismo de A/R-módulos bilaterais, então sabemos que existe uma aplicação $\overline{g} : \mathrm{Hom}_{A^e}(A,M) \to \mathrm{Hom}_{A^e}(A,N)$, dada por $\overline{g}(h) = g \circ h$, para cada $h \in \mathrm{Hom}_{A^e}(A,M)$. Considerando esta aplicação, podemos mostrar o seguinte

Lema 3.2

Sejam A uma R-álgebra e M um A/R-módulo bilateral. Então os R-módulos M^A e $\mathrm{Hom}_{A^e}(A,M)$ são isomorfos. Ainda, se N é também um A/R-módulo bilateral e g é um A^e-homomorfismo de M em N , então o seguinte diagrama de

R-módulos é comutativo, onde as setas verticais são os isomorfismos correspondentes:

$$\begin{array}{ccc} \mathrm{Hom}_{A^e}(A,M) & \xrightarrow{\bar{g}} & \mathrm{Hom}_{A^e}(A,N) \\ \downarrow & & \downarrow \\ M^A & \xrightarrow{g\,|_{M^A}} & N^A \end{array}$$

Ou seja, os funtores $(\ )^A$ e $\mathrm{Hom}_{A^e}(A,-)$ são naturalmente equivalentes.

Prova:

Consideremos a aplicação $\phi_M : \mathrm{Hom}_{A^e}(A,M) \to M^A$ dada por $\phi_M(f) = f(1)$, para cada homomorfismo $f \in \mathrm{Hom}_{A^e}(A,M)$. É fácil ver que ϕ_M é um isomorfismo de R-módulos, cujo isomorfismo inverso é a aplicação que associa a cada $m \in M$ o homomorfismo $f_m : A \to M$, dado por $f_m(a) = a.m$, para cada $a \in A$. O resto é de fácil verificação. □

O seguinte corolário é claro:

Corolário 3.3:

Se A é uma R-álgebra então o funtor $\mathrm{Hom}_{A^e}(A,-)$ é exato se e só se o funtor $(\ )^A$ é exato.

Ainda, como toda R-álgebra A é um A/R-módulo bilateral, e como A^A é exatamente o centro de A, também é evidente o seguinte

Corolário 3.4:

Se A é uma R-álgebra, então existe um R-isomorfismo canônico entre $\mathrm{Hom}_{A^e}(A,A)$ e $Z(A)$, onde $Z(A)$ denota o centro do anel A.

Apresentamos, a seguir, um resultado que envolve o conceito de produto tensorial e de álgebra:

Proposição 3.5:

Se M é um R-módulo projetivo (finitamente gerado), então, para qualquer R-álgebra B, $B \otimes_R M$ é um B-módulo projetivo (finitamente gerado).

Apresentamos agora o conceito da função traço, que será utilizada nos capítulos III e IV.

Sejam A uma R-álgebra e M um A-módulo à esquerda que é finitamente gerado e projetivo como R-módulo. Sejam $x_1,\ldots,x_n \in M$ e $f_1,\ldots,f_n \in \mathrm{Hom}_R(M,R)$ coordenadas projetivas do R-módulo M. Então a aplicação $t_M : A \to R$ dada por $t_M(x) = \sum_{i=1}^{n} f_i(x\,x_i)$, para cada $x \in A$, é um homomorfismo de R-módulos, como é fácil verificar, e é denominada APLICAÇÃO TRAÇO DE A EM R INDUZIDA POR M.

Observemos que a aplicação traço t_M dada acima independente da escolha das coordenadas projetivas do R-módulo M. De fato, se $y_1,\ldots,y_m \in M$ e $g_1,\ldots,g_m$ $\mathrm{Hom}_R(A,R)$ são também coordenadas projetivas do R-módulo M, então, para

cada $i \in \{1,2,\ldots,n\}$, $x_i = \sum_{j=1}^{m} g_j(x_i)y_j$. Portanto, para cada $x \in A$,

$$t_M(x) = \sum_{i=1}^{n} f_i(x\,x_i) = \sum_{i=1}^{n} f_i(x \sum_{j=1}^{m} g_j(x_i)y_j) =$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{m} g_j(x_i)f_i(x\,y_j) = \sum_{j=1}^{m} g_j(x_i \sum_{i=1}^{n} f_i(x\,y_j)) =$$

$$= \sum_{j=1}^{m} g_j(\sum_{i=1}^{n} f_i(x\,y_j)x_i) = \sum_{j=1}^{m} g_j(x\,y_j) \quad .$$

Além disso, é fácil ver que se M pode ser escrito como soma direta de R-módulos $M = M_1 \oplus M_2$, então $t_M = t_{M_1} + t_{M_2}$, onde t_{M_1} é a restrição da função traço t ao submódulo M_1 e t_{M_2} é a restrição de t ao submódulo M_2 .

§ 4 . LOCALIZAÇÃO E POSTO DE MÓDULOS PROJETIVOS E FINITAMENTE GERADOS.

Na seção 1 vimos que se R é um anel comutativo então todas as bases de um R-módulo livre e finitamente gerado L têm um mesmo número de elementos, e que este número é chamado posto de L .

O que vamos mostrar nesta seção é que o conceito de posto de um módulo livre sobre um anel comutativo pode ser generalizado para módulos projetivos e finitamente gerados sobre um anel comutativo que não possui idempotentes próprios. Para tal, necessitamos do conceito de módulos e anéis de quocientes, que passamos a revisar brevemente. No que segue, R denota um anel comutativo e $\otimes$ significa $\otimes_R$.

Dizemos que um anel (comutativo) R é um ANEL LOCAL se ele contém apenas um ideal maximal. Uma das propriedades mais úteis de um anel local é o fato de que os módulos projetivos sobre tais anéis são livres. Provamos este fato para módulos projetivos e finitamente gerados. Façamos antes, no entanto, algumas observações.

Se A é um ideal de um anel R , então é fácil ver que, para cada R-módulo M , o conjunto

$A.M = \{\sum_{i=1}^{n} a_i.m_i \mid a_i \in A, m_i \in M\}$ é um R-submódulo de M , e então podemos considerar o R-módulo quociente $M/_{A.M}$. É fácil ver ainda que, definindo uma operação externa por $(r + A).(m + A.m) = r.m + A.M$, para cada $r \in R$, $m \in M$, $M/_{A.M}$ é também um $R/_A$ - módulo.

Suponhamos agora que M é um R-módulo finitamente gerado. Então é claro que o R-módulo $M/_{A.M}$ é também finitamente gerado. É fácil ver também que o mesmo conjunto gerador do R-módulo $M/_{A.M}$ gera o $R/_A$-módulo $M/_{A.M}$.

Se M é um R-módulo projetivo e $\{x_i\}_{i \in I} \subset M$ e $\{f_i : M \to R\}_{i \in I} \subset \mathrm{Hom}_R(M,R)$ são coordenadas projetivas do R-módulo M , para algum conjunto de índices I , então é fácil ver que as aplicações lineares $g_i : M/_{A.M} \to R/_A$ dadas por $g_i(m + A.M) = f_i(m) + A$ são homomorfismos de $R/_A$-módulos, para cada $i \in I$ e que, junto com os elementos $x_i + A.M \in M/_{A.M}$, definem um sistema de coordenadas projetivas de $M/_{A.M}$ sobre $R/_A$.

Finalmente, podemos observar que, se A é um ideal maximal de R e se M é um R-módulo finitamente gerado e projetivo, então, sendo $R/_A$ um corpo, temos que $M/_{A.M}$ é um $R/_A$-módulo livre.

Para a próxima proposição, necessitamos do seguinte

Lema 4.1 (Lema de Nakayama generalizado):

Se R é um anel comutativo e M é um R-módulo finitamente gerado, então um ideal A de R verifica a propriedade $A.M = M$ se e só se $A + \mathrm{An}_R(M) = R$.

Prova:

Suponhamos que $M = R.m_1 + \ldots + R.m_n$, onde

$m_1,\ldots,m_n \in M$, e que o ideal A de R satisfaz a igualdade $A.M = M$. Como $An_R(M)$ é um ideal de R , é suficiente mostrarmos que $1_R \in A + An_R(M)$, para concluirmos que $A + An_R(M) = R$. Para tal, consideremos os submódulos $M_i = R.m_i + R.m_{i+1} + \ldots + R.m_n$, para cada $i \in \{1,2,\ldots,n\}$, e seja $M_{n+1} = 0$. Vamos mostrar que, para cada $i \in \{1,2,\ldots,n+1\}$, existe $a_i \in A$ tal que $(1 - a_i).M \subset M_i$. Utilizemos indução sobre i .

Pondo $a_1 = 0$, é claro que $(1 - a_1).M = M = M_1$. Seja $k \in \{1,2,\ldots,n\}$ e suponhamos que exista $a_k \in A$ tal que $(1 - a_k).M \subset M_k$. Então $(1 - a_k).M = (1 - a_k)A.M =$ $= A(1 - a_k).M \subset A.M_k = A.m_k + A.m_{k+1} + \ldots + A.m_n$. Assim, existem elementos $a_{kj} \in A$, para cada $j \in \{k,\ldots,n\}$, tais que $(1 - a_k).m_k = \sum_{j=k}^{n} a_{kj}.m_j = a_{kk}.m_k + \sum_{j=k+1}^{n} a_{kj}.m_j$, e, portanto, $(1 - a_k - a_{kk}).m_k = \sum_{j=k+1}^{n} a_{kj}.m_j \in M_{k+1}$, donde vemos que $(1 - a_k)(1 - a_k - a_{kk}).M \subset (1 - a_k - a_{kk}).M_k \subset M_{k+1}$. Pondo então $a_{k+1} = 2\,a_k + a_{kk} - a_k^{\,2} - a_k\,a_{kk}$, é fácil ver que $a_{k+1} \in A$ e $1 - a_{k+1} = (1 - a_k - a_{kk})(1 - a_k)$, e, portanto, $(1 - a_{k+1}).M \subset M_{k+1}$, ficando assim completo o processo de indução.

Concluimos então que existe em A um elemento a_{n+1} tal que $(1 - a_{n+1}).M \subset M_{n+1} = 0$, ou seja, $1 - a_{n+1} \in An_R(M)$. Logo, $1_R \in A + An_R(M)$.

Para provar a recíproca, suponhamos que $A + An_R(M) = R$, e mostremos que $A.M = M$. É claro que $A.M \subset M$.

Sejam $a \in A$ e $r \in An_R(M)$ tais que $a + r = 1_R$. Então, para cada $m \in M$, $m = 1.m = (a + r).m = a.m + r.m = a.m \in A.M$. Assim, $M \subset A.M$, o que completa a prova. □

Proposição 4.2:

Seja R um anel local com ideal maximal M. Então todo R-módulo finitamente gerado e projetivo é livre. Além disso, se $\{m_1 + M.M, \ldots, m_n + M.M\}$ é uma base do $R/_M$-módulo livre $M/_{M.M}$, então $\{m_1, \ldots, m_n\}$ é uma base de M.

Prova:

Consideremos a aplicação $\psi : R^{(n)} \to M$, dada por $\psi(\alpha_1, \ldots, \alpha_n) = \sum_{i=1}^{n} \alpha_i.m_i$, para cada $(\alpha_1, \ldots, \alpha_n) \in R^{(n)}$. É claro que ψ é um homomorfismo de R-módulos. Vamos mostrar que é um R-isomorfismo entre $R^{(n)}$ e M.

Pelas considerações feitas anteriormente, sabemos que o quociente $M/_{R.m_1+\ldots+R.m_n}$ é um R-módulo finitamente gerado. Além disso, sendo que $M/_{M.M} = R.(m_1 + M.M) + \ldots + R.(m_n + M.M)$, $R.(m_1 + M.M) + \ldots + R.(m_n + M.M) + M.M = M$, ou seja, $R.m_1 + \ldots + R.m_n + M.M = M$. Assim, $M.(M/_{R.m_1+\ldots+R.m_n}) = (M.M + R.m_1 + \ldots + R.m_n)/_{R.m_1+\ldots+R.m_n} = M/_{R.m_1+\ldots+R.m_n}$, e então, aplicando o Lema de Nakayama, vemos que $M/_{R.m_1+\ldots+R.m_n} = 0$. Ou seja, $M = R.m_1 + \ldots + R.m_n$, donde segue-se que ψ é um epimorfismo.

Suponhamos agora que $(\alpha_1,\ldots,\alpha_n)$ Ker ψ . Então $\sum_{i=1}^{n} \alpha_i.m_i = 0$, donde segue-se que $\sum_{i=1}^{n} (\alpha_i+M)\cdot(m_i+M.M) = M.M = \overline{0} \in M/_{M.M}$. Sendo $\{m_i + M.M\}_{i=1}^{n}$ uma base do módulo livre $M/_{M.M}$, temos necessariamente que $\alpha_i + M = M$, ou ainda, $\alpha_i \in M$, para cada $i \in \{1,2,\ldots,n\}$. Assim, vemos que Ker $\psi \subset M.R^{(n)}$.

Formamos agora a seguinte seqüência exata de R-módulos $0 \to \text{Ker } \psi \hookrightarrow R^{(n)} \xrightarrow{\psi} M \to 0$ que cinde, uma vez que M é um R-módulo projetivo. Então Ker ψ é um R-somando direto de $R^{(n)}$, e segue que Ker ψ é um R-módulo finitamente gerado. Mas como Ker $\psi \subset M.R^{(n)}$, podemos escrever, aplicando a lei modular, Ker $\psi \subset M.R^{(n)} \cap$ Ker ψ = $M.(\text{Ker } \psi \oplus L) \cap \text{Ker } \psi$ = $(M.\text{ Ker } \psi \oplus M.L) \cap \text{Ker } \psi = M.\text{Ker } \psi$. Logo, Ker $\psi = M.\text{Ker } \psi$, e aplicando novamente o Lema de Nakayama, conclui-se que Ker $\psi = 0$. Logo, ψ é também um R-monomorfismo, o que completa a prova. □

Dizemos que um subconjunto W de $R - \{0\}$ é um SISTEMA MULTIPLICATIVO de R se

i) $1_R \in W$;

ii) $w\,w' \in W$, para cada par de elementos $w,w' \in W$.

Como exemplos de sistemas multiplicativos, podemos citar o conjunto formado por todas as potências não negativas de um elemento não nilpotente de R e o conjunto formado por todos os elementos de R que não pertencem a um

dado ideal primo (próprio) deste anel.

Se M é um R-módulo e W é um sistema multiplicativo de R então é possível definir uma relação em $M \times W$, da seguinte maneira: $(m_1,w_1) \sim (m_2,w_2)$ se e só se existe $w \in W$ tal que $w.(w_1.m_2 - w_2.m_1) = 0$, para cada par de elementos $(m_1,w_1),(m_2,w_2) \in M \times W$. É fácil ver que esta relação é de equivalência. A classe de equivalência de um elemento $(m,w) \in M \times W$ é denotada por $m/_w$, e o conjunto destas classes é denotado por M_W. Neste conjunto M_W, definimos soma e produto externo por $m_1/_{w_1} + m_2/_{w_2} = (w_2.m_1 + w_1.m_2)/_{w_1w_2}$ e $r.(m/_w) = r.m/_w$, para cada $r \in R$ e m_1/w_1, $m_2/w_2 \in M_W$. Tais aplicações estão bem definidas e dotam M_W de uma estrutura de R-módulo. Tal R-módulo é chamado MÓDULO DE QUOCIENTES ou MÓDULO DE FRAÇÕES.

Se, além disso, M é uma R-álgebra, então podemos também definir um produto em M_W por $(m_1/_{w_1})(m_2/_{w_2}) = (m_1m_2)/_{(w_1w_2)}$, para cada par de classes $m_1/_{w_1}$, $m_2/_{w_2} \in M_W$. Com esta operação, M_W torna-se uma R-álgebra, como é fácil verificar. Em particular, a R-álgebra R_W é denominada ANEL DE QUOCIENTES DE R, e pode-se verificar que cada inversível deste anel é da forma $w_1/_{w_2}$, com $w_1,w_2 \in W$. Se tomamos ainda $W = R - P$, onde P é um ideal primo de R, denotamos R_W por R_P. Ou seja, $R_P = \{r/_s \mid r \in R, s \notin P\}$.

Assim, por exemplo, temos que o conjunto $PR_P = \{pr/_s \mid r \in R, s \notin P, p \in P\} = \{r/_s \mid r \in P, s \notin P\}$ é um ideal de R_P, e tem a propriedade de que todo elemento fora

dele é inversível em R_P , como é fácil verificar. Ou seja, $P R_P$ é um ideal maximal de R_P . Mais ainda, ele é o único maximal. Assim, R_P é um anel local, chamado ANEL LOCALIZADO DE A PELO IDEAL PRIMO P , cujo ideal maximal é $P R_P$.

Estabelecemos agora alguns resultados que nos serão úteis nesta seção e outros que serão utilizados nos capítulos que seguem.

Lema 4.3:

Sejam W e W' sistemas multiplicativos de R , tais que $W \subset W'$. Então a aplicação de R_W em $R_{W'}$ dada por $r/_w \to r/_w$, para cada $r/_w \in R_W$ é um homomorfismo de anéis (e, portanto, induz em $R_{W'}$ uma estrutura de R_W-álgebra). Além disso, $R_{W'}$ é isomorfo a $(R_W)_{W'R_W}$, onde $W'R_W = \{w'/_w \in R_W \mid w' \in W'\}$ é um sistema multiplicativo de R_W .

Prova:

É fácil ver que, do fato de ser W um subconjunto de W' , temos que a aplicação dada acima está bem definida e é um homomorfismo de anéis. Ainda, é claro que $W'R_W$ é um sistema multiplicativo de R_W . Para provar que $R_{W'}$ e $(R_W)_{W'R_W}$ são anéis isomorfos, basta-nos considerar a aplicação que associa a cada $r/_{w'} \in R_{W'}$ a classe $(r/_1)/_{(w'/_1)}$ de $(R_W)_{W'R_W}$, como é fácil verificar. □

Se W é um sistema multiplicativo de R e M é um R-módulo, então o módulo de quocientes M_W é um R_W-módulo, onde a operação externa é dada por $(r/_w).(m/_{w'}) = r.m/_{ww'}$, para cada $r/_w \in R_W$, $m/_{w'} \in M_W$. Além disso, a aplicação $\alpha : M_W \to R_W \otimes M$ definida por $\alpha(m/_w) = 1/_w \otimes m$, para cada $m/_w \in M_W$, está bem definida e é um isomorfismo de R_W-módulos, cujo isomorfismo inverso é a aplicação $\beta : R_W \otimes M \to M_W$, dada por $\beta(r/_w \otimes m) = r.m/_w$, para cada $r/_w \otimes m \in R_W \otimes M$. Este isomorfismo é canônico, no seguinte sentido.

Fixado um sistema multiplicativo W de R, podemos considerar o funtor $(\ )_W$ da categoria dos R-módulos na categoria dos R_W-módulos, a saber: a cada R-módulo M está associado o R_W-módulo M_W, e a cada R-homomorfismo $f : M \to M'$ está associado o R_W-homomorfismo $f_W : M_W \to M'_W$, definido por $f_W(m/_w) = f(m)/_w$, para cada $m/_w \in M_W$. Por outro lado, sendo R_W um R-módulo, podemos considerar o funtor $R_W \otimes \_\_$ da categoria dos R-módulos na categoria dos R_W-módulos à esquerda. O isomorfismo acima verifica a propriedade de que se $f : M \to M'$ é um homomorfismo de R-módulos, então o seguinte diagrama é comutativo:

$$\begin{array}{ccc} M_W & \xrightarrow{f_W} & M'_W \\ \downarrow & & \downarrow \\ R_W \otimes M & \xrightarrow{id \otimes f} & R_W \otimes M' \end{array}$$

Logo, os funtores $R_W \otimes \_\_$ e $(\ )_W$ são naturalmente equivalentes e portanto, a partir de agora, não faremos

mais distinção entre eles.

Com referência a tais funtores equivalentes, temos o seguinte

Lema 4.4:

Se W é um sistema multiplicativo de R, então o funtor $R_W \otimes \_\_$ é um funtor exato (ou ainda, R_W é um R-módulo plano).

Prova:

Resta-nos apenas mostrar que, se $0 \to M \xrightarrow{f} M'$ é uma seqüência exata de R-módulos, então a seqüência de R_W-módulos dada por $0 \to R_W \otimes M \xrightarrow{id \otimes f} R_W \otimes M'$ é também exata (ou, equivalentemente, que a seqüência $0 \to M_W \xrightarrow{f_W} M'_W$ é também exata). De fato, suponhamos que $f_W(m/_w) = 0$, para algum $m/_w \in M_W$. Então, existe um elemento $w' \in W$ tal que $w'(w.0 - 1.f(m)) = 0$, ou seja, $0 = w'.f(m) = f(w'.m)$, o que implica $w'.m = 0$, já que f é um monomorfismo, por hipótese. Mas então $m/_w = 0$, o que completa a prova. □

Proposição 4.5:

Seja M um R-módulo tal que, para cada ideal maximal M de R, $M_M = 0$. Então $M = 0$.

Prova:

Para cada ideal maximal M de R e para cada

$m \in M$, sabemos, por hipótese, que $m/_1 = 0 \in M_M$. Ou seja, para cada ideal maximal M , existe um elemento $w_M \notin M$ tal que $w_M.m = 0$. Assim, $w_M \notin M$ e $w_M \in An_R(m)$ (onde $An_R(m)$ representa o anulador do R-módulo gerado pelo elemento m). Podemos então concluir que $An_R(m)$ não é um subconjunto de nenhum ideal maximal de R . Mas então, sendo também um ideal, temos que a única possibilidade é $An_R(m) = R$. Em particular, $1_R.m = 0$, ou seja, $m = 0$, o que completa a prova. □

Lema 4.6:

Se M é um R-módulo finitamente gerado e se W é um sistema multiplicativo de R então $M_W = 0$ se e só se existe algum elemento $w \in W$ tal que $w.M = 0$.

Prova:

É claro que se $w.M = 0$, para algum $w \in W$, então $m/_{w'} = 0$, para cada $m/_{w'} \in R_W$. Reciprocamente, se $M_W = 0$ e se $M = R.m_1 + \ldots + R.m_n$, então, para cada $i \in \{1,2,\ldots,n\}$, temos que $m_i/_1 = 0$. Ou seja, existe $w_i \in W$ tal que $w_i.m_i = 0$, $(i=1,2,\ldots,n)$. Pondo então $w = w_1 w_2 \ldots w_n$, é fácil ver que $w.M = 0$. □

Passemos agora à formulação do conceito de posto de um módulo finitamente gerado e projetivo. Para tal, vamos supor que M é um R-módulo finitamente gerado e projetivo. Então sabemos que, para cada ideal primo P de R , R_P

é um anel local e é também uma R-álgebra. Assim, por 3.5, temos que $M_P \simeq R_P \otimes M$ é um R_P-módulo finitamente gerado e projetivo. Logo, por 4.2, vemos que M_P é um R_P-módulo livre. Portanto, existe um inteiro positivo n_P tal que $R_P \otimes M \simeq M_P$ é isomorfo a n_P cópias do anel R_P. Tal inteiro n_P é dito P-POSTO DO R-MÓDULO M, e é denotado por $\text{posto}_P M$.

Dizemos que M tem POSTO (CONSTANTE) igual a n se e só se, para cada ideal primo P de R, $\text{posto}_P M = n$. Neste caso, escrevemos $\text{posto}_R M = n$.

Proposição 4.7:

Sejam S uma R-álgebra comutativa e M um R-módulo finitamente gerado e projetivo de posto constante. Então o S-módulo finitamente gerado e projetivo $M \otimes S$ tem posto constante, e $\text{posto}_S(M \otimes S) = \text{posto}_R M$.

Prova:

Seja P um ideal primo de S. É fácil ver que $p = \{x \in R \mid x.1_S \in P\}$ é um ideal primo de R, e $(R - p).1_S \subset S - P$. Então a operação $(r/_p).(s/_{p'}) = r.s/_{p.p'}$, para cada $r \in R$, $p \notin p$, $s \in S$, $p' \notin P$, está bem definida e, por 4.3, dota S_P de uma estrutura de R_p-álgebra, como é fácil verificar.

Portanto (pelos isomorfismos estabelecidos na seção 2), temos que, se $n = \text{posto}_R M$, $(M \otimes_R S)_P \simeq (M \otimes_R S) \otimes_S S_P \simeq$

$\simeq M \otimes_R (S \otimes_S S_P) \simeq M \otimes_R S_P \simeq M \otimes_R (R_p \otimes_{R_p} S_P) \simeq (M \otimes_R R_p) \otimes_{R_p} S_P \simeq$

$$\simeq M_p \otimes_{R_p} S_p \simeq R_p^{(n)} \otimes_{R_p} S_p \simeq (R_p \otimes_{R_p} S_p)^{(n)} \simeq (S_p)^{(n)} ,$$

ou seja, para qualquer ideal primo P de S, $(M \otimes_R S)_p \simeq (S_p)^{(n)}$ e, portanto, $\text{posto}_S(M \otimes_R S) = n = \text{posto}_R M$. □

A seguinte proposição pode ser mostrada facilmente, e sua prova fica a cargo do leitor.

Proposição 4.8:

Sejam M e N dois R-módulos finitamente gerados e projetivos, e seja P um ideal primo de R . Então:

(i) $\text{posto}_P(M \oplus N) = \text{posto}_P M + \text{posto}_P N$

(ii) $\text{posto}_P(M \otimes N) = (\text{posto}_P M)(\text{posto}_P N)$

(iii) $\text{posto}_P\ (\text{Hom}_R(M , N)) = (\text{posto}_P M)(\text{posto}_P N)$

Queremos mostrar a seguir que, quando R é um anel sem idempotentes próprios, então o posto de qualquer R-módulo finitamente gerado e projetivo é constante. No entanto, precisamos antes fazer algumas considerações.

O conjunto de todos os ideais primos do anel comutativo R é denominado ESPECTRO DE R , e é denotado por $\text{Spec}(R)$. Para cada subconjunto L de R , denotemos por $h(L)$ o subconjunto de $\text{Spec}(R)$ formado por todos os ideais primos de R que contêm L . Ou seja: $h(L) = \{P \in \text{Spec}(R) \mid P \supset L\}$. Neste conjunto $\text{Spec}(R)$ está definida a chamada TOPOLOGIA DE ZARISKI, como vemos no seguinte

Lema 4.9:

$\text{Spec}(R)$ é um espaço topológico, se considera-

mos como fechados os conjuntos da forma $h(L)$.

Prova:

É claro que $h(\phi) = Spec(R)$, $h(R) = \phi$, e que $\bigcap_{i \in I} h(L_i) = \{P \in Spec(R) \mid P \supset L_i \ (i \in I)\} = \{P \in Spec(R) \mid P \supset \bigcup_{i \in I} L_i\} = h(\bigcup_{i \in I} L_i)$.

Além disso, sendo $h(L)$ conjunto de ideais primos, para cada subconjunto L de R , segue-se que, se L_1 e L_2 são dois subconjuntos arbitrários de R , então $h(L_1) \cup h(L_2) = \{P \in Spec(R) \mid P \supset L_1 \text{ ou } P \supset L_2\} = h\{\ell_1 \ell_2 \mid \ell_1 \in L_1 \text{ e } \ell_2 \in L$

Assim, $Spec(R)$ é um espaço topológico. □

NOTA: Toda vez que nos referirmos ao espaço topológico $Spec(R)$ ou à topologia de $Spec(R)$, estaremos nos referindo à topologia de Zariski, definida acima.

Antes de analisarmos em que caso o espaço $Spec(R)$ é conexo, lembramos um resultado sobre ideais comaxiais.

Dados um anel (comutativo) R e dois ideais A_1 e A_2 de R , dizemos que A_1 e A_2 são IDEAIS COMAXIAIS se $A_1 + A_2 = R$.

A prova do lema a seguir pode ser encontrada em [5] .

Lema 4.10:

Se A_1 e A_2 são ideais comaxiais de R então A_1^m e A_2^n são também ideais comaxiais, para quaisquer inteiros m e n, e $A_1^m \cap A_2^n = A_1^m A_2^n$.

Para a próxima prova necessitamos ainda da proposição a seguir, cuja prova pode ser encontrada em [2] (ver prop. 1.8).

Proposição 4.11:

A intersecção de todos ideais primos de um anel comutativo é exatamente o ideal formado por todos os elementos nilpotentes do anel dado.

Proposição 4.12:

O espaço topológico Spec(R) é conexo se e só se R possui apenas idempotentes triviais.

Prova:

Lembramos aqui que um espaço é desconexo se e só se existem dois subconjuntos não vazios, fechados e disjuntos do espaço cuja união é todo o espaço.

Suponhamos então que R possui um idempotente próprio e, e provemos que Spec(R) é desconexo. Para tal, consideremos os fechados h(e) e h(1-e) (onde h(x) denota o conjunto h({x})). É fácil ver que tais conjuntos são não vazios, já que $Re \neq R$ e $R(1-e) \neq R$.

Como $(1-e)e=0$, cada ideal primo do $Spec(R)$ contém um dos elementos $1-e$ ou e . Assim, $h(e)\cup h(1-e)=Spec(R)$ Além disso, como $1=(1-e)+e$, é claro que $h(e)$ e $h(1-e)$ são conjuntos disjuntos. Logo, $Spec(R)$ é um espaço desconexo.

Reciprocamente, suponhamos que $Spec(R)$ é um espaço desconexo. Ou seja, existem dois subconjuntos L_1 e L_2 de R tais que $h(L_1)$ e $h(L_2)$ são disjuntos, não vazios e cuja união é exatamente $Spec(R)$. Sejam $A_1=\bigcap_{P\in h(L_1)} P$ e $A_2=\bigcap_{P\in h(L_2)} P$. Então é fácil ver que $h(A_1)=h(L_1)\neq\phi$ e $h(A_2)=h(L_2)\neq\phi$, donde, $A_1\neq R$ e $A_2\neq R$. Ainda, $h(A_1)\cap h(A_2)=h(L_1)\cap h(L_2)=\phi$, ou seja, não existem ideais primos de R que contenham os ideais A_1 e A_2 simultaneamente. Logo, $A_1+A_2=R$, i.e., A_1 e A_2 são ideais comaxiais. Além disso, como $h(A_1)\cup h(A_2)=Spec(R)$, por hipótese, é claro que $A_1\cap A_2$ é a intersecçãode todos os ideais primos de R . Assim, pela proposição anterior, $A_1\cap A_2$ é o ideal formado por todos os elementos nilpotentes de R .

Ainda, como A_1 e A_2 são ideais comaxiais, existem $a_1\in A_1$, $a_2\in A_2$, tais que $1=a_1+a_2$. Logo, $R=Ra_1+Ra_2$, i.e., Ra_1 e Ra_2 são também ideais comaxiais. Além disso, $a_1a_2\in A_1\cap A_2$ e, portanto, é um elemento nilpotente. Seja m um inteiro positivo tal que $(a_1a_2)^m=0$. Então $Ra_1^m\cap Ra_2^m=0$ e, pelo último lema, Ra_1^m e Ra_2^m

são ideais comaxiais. Portanto, $R = Ra_1^m \oplus Ra_2^m$, e esta decomposição é não trivial. De fato, se, por exemplo, $Ra_1^m = 0$ então a_1 é um elemento nilpotente e, portanto, é também um elemento de A_2. Então $1 = a_1 + a_2 \in A_2$, uma contradição.

Ou seja, $R = Ra_1^m \oplus Ra_2^m$ é uma decomposição não trivial de R em uma soma direta de ideais. Mas então é fácil ver que, neste caso, R possui idempotentes próprios (de fato, se $1 = e + e'$, onde $e \in Ra_1^m$, e' Ra_2^m então é fácil ver que e e e' são idempotentes próprios de R), o que completa a prova. □

Já sabemos que se M é um R-módulo finitamente gerado e projetivo e se P é um ideal primo de R, então M_P é um R_P-módulo livre. A proposição a seguir mostra que existem sistemas multiplicativos que são subconjuntos bem menores do que os sistemas da forma $R - P$, onde P é um ideal primo de R, e tais que a mesma propriedade é válida.

Proposição 4.13:

Sejam M um R-módulo finitamente gerado e projetivo e P um ideal primo de R. Então existe um elemento $\alpha \in R - P$ tal que $M_{(\alpha)} \simeq R_{(\alpha)} \otimes M$ é um $R_{(\alpha)}$-módulo livre e finitamente gerado, onde (α) representa o sistema multiplicativo de R formado por todas as potências não negativas do elemento α.

Prova:

Consideremos o R_P-módulo livre M_P, e suponhamos que $\{m_1/_{\alpha_1},\ldots,m_n/_{\alpha_n}\}$ é uma base de M_P sobre R_P. É fácil ver que $\{m_1/_1,\ldots,m_n/_1\}$ é também uma base de M_P sobre R_P.

Além disso, a aplicação $\Phi : R^{(n)} \to M$ dada por $\Phi(r_1,\ldots,r_n) = \sum_{i=1}^{n} r_i.m_i$ é um R-homomorfismo, como é fácil verificar. A seqüência de R-módulos $0 \to \text{Ker } \Phi \hookrightarrow R^{(n)} \xrightarrow{\Phi} M \to M/_{\text{Im } \Phi} \to 0$ é exata e, como R_P é um R-módulo plano, vem que $0 \to (\text{Ker } \Phi)_P \to (R^{(n)})_P \to M_P \to (M/_{\text{Im } \Phi})_P \to 0$ é também uma seqüência exata de R_P-módulos. Mas observemos que $\Phi(e_i) = m_i$, para cada $i \in \{1,2,\ldots,n\}$, (onde $\{e_i\}_{i=1}^{n}$ é a base canônica de $R^{(n)}$), e então o homomorfismo induzido $\Phi_P : (R^{(n)})_P \to M_P$ leva base em base. Portanto, ele é um isomorfismo de R_P-módulos. Assim, vem que $(\text{Ker } \Phi)_P = 0$ e $(M/_{\text{Im } \Phi})_P = 0$.

Além disso, como M é um R-módulo finitamente gerado, $M/_{\text{Im } \Phi}$ é também um R-módulo finitamente gerado. Então, por 4.6, existe um elemento $\beta \in R - P$ tal que $\beta.M/_{\text{Im } \Phi} = 0$. Portanto, $(M/_{\text{Im } \Phi})_{(\beta)} = 0$.

Obtemos assim, de (*), a seguinte seqüência exata

$$0 \to (\text{Ker } \phi)_{(\beta)} \hookrightarrow (R^{(n)})_{(\beta)} \to M_{(\beta)} \to 0$$

de $R_{(\beta)}$-módulos à esquerda. Além disso, sendo M um R-módulo

projetivo, $M_{(\beta)} \simeq R_{(\beta)} \otimes M$ é um $R_{(\beta)}$-módulo projetivo. Assim, a seqüência acima cinde, donde $(\mathrm{Ker}\,\phi)_{(\beta)}$ é um $R_{(\beta)}$-módulo finitamente gerado.

Como $(\beta) \subset R - P$, aplicando 4.2, concluimos que R_P é uma $R_{(\beta)}$-álgebra. Assim, temos que

$$(\mathrm{Ker}\,\Phi)_{(\beta)} \otimes_{R_{(\beta)}} R_P \simeq (\mathrm{Ker}\,\Phi \otimes R_{(\beta)}) \otimes_{R_{(\beta)}} R_P \simeq \mathrm{Ker}\,\Phi \otimes (R_{(\beta)} \otimes_{R_{(\beta)}} R_P) \simeq$$

$$\simeq \mathrm{Ker}\,\Phi \times R_P \simeq (\mathrm{Ker}\,\Phi)_P = 0 \ .$$

Portanto, $[(\mathrm{Ker}\,\Phi)_{(\beta)}]_P = 0$. Novamente, aplicando 4.6, vemos que existe um elemento $\mu/\beta^k \in R_{(\beta)} - PR_{(\beta)}$ tal que $(\mu/\beta^k).[\mathrm{Ker}\,\Phi_{(\beta)}] = 0$. É fácil ver ainda que $[R_{(\beta)}]_{(\mu/1)}$ é um anel isomorfo a $R_{(\mu\beta)}$. Então podemos escrever

$$0 = [\mathrm{Ker}\,\Phi_{(\beta)}]_{(\mu/1)} \simeq (\mathrm{Ker}\,\Phi \otimes R_{(\beta)}) \otimes_{R_{(\beta)}} (R_{(\beta)})_{(\mu/1)} \simeq \mathrm{Ker}\,\Phi \otimes R_{(\mu\beta)} \simeq$$

$$\simeq (\mathrm{Ker}\,\phi)_{(\mu\beta)} \ .$$

Além disso, como $\beta[M/_{\mathrm{Im}\,\phi}] = 0$, é claro que $(M/_{\mathrm{Im}\,\phi})_{(\mu\beta)} = 0$. Então, novamente de (*), obtemos a seguinte seqüência exata de $R_{(\mu\beta)}$-módulos

$$0 \to (R^{(n)})_{(\mu\beta)} \to M_{(\mu\beta)} \to 0 \ .$$

Assim, pondo $\alpha = \mu\beta$, temos que $M_{(\alpha)}$ é um $R_{(\alpha)}$-módulo livre e finitamente gerado. □

Seja M um R-módulo finitamente gerado e projetivo e sejam $\alpha \in R$ e P um ideal primo de R tais que

$\alpha \notin P$ e $M_{(\alpha)}$ é um $R_{(\alpha)}$-módulo livre de posto (constante) igual a m. Observemos então que R_P é uma $R_{(\alpha)}$-álgebra e $M \otimes R_P \simeq M \otimes R_{(\alpha)} \otimes_{R_{(\alpha)}} R_P \simeq M_{(\alpha)} \otimes_{R_{(\alpha)}} R_P \simeq [R_{(\alpha)}]^{(m)} \otimes_{R_{(\alpha)}} R_P \simeq$ $\simeq [R_{(\alpha)} \otimes_{R_{(\alpha)}} R_P]^{(m)} \simeq [R_P]^{(m)}$, ou seja, M é um R-módulo tal que $\text{posto}_P M = m$.

Denotando por N o conjunto dos inteiros positivos, podemos provar agora o seguinte

Corolário 4.14:

Seja M um R-módulo finitamente gerado e projetivo. A aplicação $\psi : \text{Spec}(R) \to N$ dada por $\psi(P) = \text{posto}_P(M)$, para cada $P \in \text{Spec}(R)$, é uma aplicação contínua, quando consideramos N dotado da topologia discreta.

Prova:

Seja P um ideal primo qualquer de R, e suponhamos $\text{posto}_P M = n$. Pela proposição anterior, existe um elemento $\alpha \in R - P$ tal que $M_{(\alpha)}$ é um $R_{(\alpha)}$-módulo livre de posto finito. Além disso, pela observação anterior, sabemos que tal posto é igual a n. Consideremos então o conjunto aberto $\text{Spec}(R) - h(\alpha)$, conjunto ao qual P pertence, e vejamos que a imagem por ψ é exatamente n. De fato, se P' é um outro ideal primo pertencente a $\text{Spec}(R) - h(\alpha)$, então, como $\alpha \notin P'$ pela observação anterior, vemos que $\text{posto}_{P'} M = n = \text{posto}_P M$. Então concluimos que a imagem inversa de um inteiro não nega

tivo n é vazia ou é um conjunto aberto do tipo $Spec(R) - h(\alpha)$ do espaço $Spec(R)$. Logo ψ é uma aplicação contínua. □

Considerando a aplicação ψ dada no corolário acima, podemos mostrar o seguinte

Teorema 4.15:

Seja R um anel comutativo sem idempotentes próprios. Então cada R-módulo finitamente gerado e projetivo M tem posto constante (ou seja, existe um inteiro não negativo m tal que, para cada ideal primo P de R , $posto_P M = m$) .

Prova:

De fato, se m e n são imagens distintas de ψ em relação a tal R-módulo M , então é fácil ver que $Spec(R) = \psi^{-1}(n) \cup \psi^{-1}(K)$, onde $K = N - \{n\}$. Ou seja, como $m \in K$, obtemos uma decomposição não trivial de $Spec(R)$ como união de dois abertos disjuntos, uma contradição, uma vez que $Spec(R)$ é um espaço conexo.

§ 5 . EXTENSÕES SEPARÁVEIS E EXTENSÕES DE GALOIS DE CORPOS

Nesta seção, apresentamos os resultados básicos de extensões separáveis e extensões de Galois de corpos. No entanto, omitiremos aqui a maioria das provas destes resultados, uma vez que esta teoria é generalizada nos capítulos II e III. Mais detalhes podem ser encontrados em [1] , [10] e [27] .

Em toda esta seção, E e K denotam dois corpos (comutativos) arbitrários. Quando $E \supset K$, $[E : K]$ denota a dimensão do espaço vetorial E sobre K , e dizemos que E é uma EXTENSÃO DE K . Se $[E : K] < \infty$, dizemos que E é uma EXTENSÃO FINITA de K . Além disso, $K[X]$ representa o anel de polinômios sobre uma indeterminada X e com coeficientes no corpo K , e G denota um grupo multiplicativo arbitrário.

Se E é uma extensão do corpo K e F é um corpo tal que $K \subset F \subset E$, então F é dito um CORPO INTERMEDIÁRIO ENTRE E e K .

No que segue, faremos uso do seguinte resultado cuja prova pode ser encontrada na bibliografia citada:

Se E é uma extensão de K , F é um corpo intermediário entre E e K e se as extensões E sobre F e F sobre K são finitas então E é também uma extensão finita de K . Reciprocamente, se $[E : K]$ é finita, então $[E : F]$ e $[F : K]$ são finitas e vale $[E : K] = [E:F][F:K]$.

Dizemos que um polinômio $f(X) \in K[X]$ DECOMPÕE-SE LINEARMENTE SOBRE $K[X]$ se $f(X)$ pode ser expresso como um produto de fatores lineares $f(X) = k(X - \alpha_1)\ldots(X - \alpha_n)$, onde $k, \alpha_1, \ldots, \alpha_n \in K$. Neste caso, os zeros de $f(X)$ em K são

precisamente $\alpha_1,\ldots,\alpha_n$.

É claro que, dado qualquer polinômio $f(X) \in K[X]$, é sempre possível encontrar um corpo $E \supset K$ onde $f(X)$ se decompõe linearmente. (De fato, basta-nos tomar E como sendo o fecho algébrico de K). Mais ainda, o resultado abaixo nos mostra que a extensão E citada pode até ser tomada de dimensão finita sobre K , e sua prova encontra-se em [10] .

Proposição 5.1:

Seja $f(X) \in K[X]$ um polinômio arbitrário, de grau $n \geqslant 1$. Então existe um corpo E , extensão de K , tal que $f(X)$ decompõe-se linearmente sobre $E[X]$ e $[E : K] \leqslant n!$.

Seja $f(X) \in K[X]$. Dizemos que um corpo E , extensão de K, é um CORPO DE DECOMPOSIÇÃO (ou CORPO DE RAÍZES) de f sobre K se:

(i) $f(X)$ decompõe-se linearmente sobre $E[X]$;

(ii) se E' é um corpo tal que $K \subset E' \subset E$ e $f(X)$ decompõe-se linearmente sobre $E'[X]$, então $E' = E$.

Portanto, pela proposição acima, podemos afirmar que o corpo de decomposição E de qualquer polinômio $f(X) \in K[X]$ de grau $n \geqslant 1$ existe e tem dimensão finita sobre K : $[E : K] \leqslant n!$.

É óbvio também que, se E é um corpo de decomposição de $f(X) \in K[X]$ então $E = K(\alpha_1,\ldots,\alpha_n)$, onde $\alpha_1,\ldots,\alpha_n$ são as raízes de $f(X)$ no fecho algébrico $\overline{K}$ de K (i.e., E pode ser obtido pela adjunção a K das raízes $\alpha_1,\ldots,\alpha_n$ de $f(X)$ em $\overline{K}$).

Sejam K e K' dois corpos, $\sigma : K \to K'$ um isomorfismo de corpos e $f(X) \in K[X]$ um polinômio irredutível. Suponhamos que o polinômio $g(X) \in K'[X]$ é o correspondente de $f(X)$ por σ. Então é fácil ver que $g(X)$ é um polinômio irredutível de $K'[X]$.

Se α é uma raiz de $f(X)$ no fecho algébrico de K e β é uma raiz de $g(X)$ no fecho algébrico de K', e se $F = K(\alpha)$ e $F' = K'(\beta)$ são as extensões obtidas pelas adjunções de α e β respectivamente, então pode-se mostrar que o isomorfismo σ pode ser estendido a um isomorfismo $\overline{\sigma} : F \to F'$ tal que $\overline{\sigma}(\alpha) = \beta$. Utilizando este fato, prova-se, então, que se E é um corpo de decomposição de f sobre K e E' é um corpo de decomposição de g sobre K' então o isomorfismo σ pode ser estendido a um isomorfismo σ' de E em E'. Além disso, σ' transforma as raízes de $f(X)$ em E nas raízes de $g(X)$ em E'.

Como uma conseqüência importante deste fato obtém-se o seguinte

Teorema 5.2:

O corpo de decomposição de um polinômio qualquer $f(X) \in K[X]$ é único, a menos de isomorfismos.

O teorema acima justifica então fazermos alusão ao corpo de decomposição de um polinômio, e não a um corpo de decomposição.

Ainda, este teorema nos assegura que a decomposição de um polinômio em fatores lineares independe do

corpo considerado. Ou seja, se $E \in E'$ são dois corpos extensões de K tais que um polinômio arbitrário $f(X) \in K[X]$ decompõe-se linearmente em $E[X]$ e $E'[X]$, então é fácil ver que existe uma correspondência biunívoca entre as raízes de $f(X)$ em E e em E' que preserva a multiplicidade das mesmas.

Dizemos que um polinômio $f(X) \in K[X]$ é um POLINÔMIO SEPARÁVEL SOBRE K se $f(X)$ não possui raízes múltiplas num corpo de decomposição de f sobre K. Ou seja, no corpo de decomposição de f sobre K, $f(X)$ é da forma $k(X-\alpha_1)\ldots(X-\alpha_n)$ onde as raízes $\alpha_1,\ldots,\alpha_n$ são todas distintas.

Para polinômios sobre o corpo dos reais, existe um método standard para detectar raízes múltiplas: a diferenciação. Tal método pode ser generalizado para corpos arbitrários, definindo-se derivação de maneira formal, como segue.

Seja $f(X) = a_nX^n + \ldots + a_1X + a_0$ um polinômio de $K[X]$. Então denominamos DERIVADA FORMAL DE f o polinômio $Df(X) = na_n X^{n-1} + \ldots + 2a_2X + a_1 \in K[X]$. Então é fácil provar que um polinômio não nulo $f(X) \in K[X]$ tem uma raiz múltipla no corpo de decomposição E de f sobre K se e só se $f(X)$ e $Df(X)$ têm um fator comum de grau maior ou igual a 1 em $E[X]$.

A seguinte proposição caracteriza os polinômios irredutíveis que são separáveis em $K[X]$:

Proposição 5.3:

(i) Se K é um corpo de característica zero, então todo polinômio irredutível de $K[X]$ é separável sobre K.

(ii) Se K é corpo de característica $p > 0$, então um polinômio irredutível de $K[X]$ é não separável sobre K se e só se ele é da forma $g(X^p)$, para algum polinômio $g(X) \in K[X]$.

Dado um corpo E extensão de K, sabemos que um elemento $\alpha \in E$ é ALGÉBRICO sobre K se existe um polinômio $g(X) \in K[X]$ tal que $g(\alpha) = 0$. Neste caso, mostra-se que existe um polinômio $f(X) \in K[X]$ com carater minimal para esta propriedade, isto é, $f(\alpha) = 0$ e, se $g(\alpha) = 0$, para algum polinômio $g(X) \in K[X]$, então $f(X)$ divide $g(X)$ em $K[X]$. Tal polinômio $f(X)$ é denominado POLINÔMIO MINIMAL DE α. Dizemos ainda que α é um ELEMENTO SEPARÁVEL SOBRE K se o seu polinômio minimal é um polinômio separável sobre K. Uma extensão algébrica E de K é SEPARÁVEL SOBRE K se todo elemento de E é separável sobre K.

Observação: Alguns autores utilizam outra definição para polinômio separável sobre um corpo (ver, por exemplo, [1]). De acordo com esta outra definição, um polinômio $f(X) \in K[X]$ é dito separável sobre K se cada fator irredutível $g(X)$ de $f(X)$ em $K[X]$ não possui raízes múltiplas no corpo de decomposição de f sobre K. Assim, por exemplo, se K é um corpo de característica zero, então qualquer potência

de um polinômio irredutível de $K[X]$ seria um polinômio separável sobre K. No entanto, veremos, no capítulo IV, que a definição de polinômio separável sobre $R[X]$, onde R é um anel comutativo com unidade não generaliza a definição dada por Emil Artin em [1], e sim é uma generalização da definição dada inicialmente.

Antes de definirmos extensão de Galois de um corpo K, necessitamos de alguns conceitos preliminares, que passamos a apresentar. Lembramos que, nesta seção, G denota um grupo multiplicativo.

Dizemos que um homomorfismo de grupos $\sigma : G \to K^*$ (onde K^* denota o grupo multiplicativo $K - \{0\}$) é um CARACTER DE G EM K. Logo, pela definição, $\sigma(x) \neq 0$, para todo $x \in G$.

Sejam agora $\sigma_1,\ldots,\sigma_n$ caracteres de G em K, e $a_1,\ldots,a_n$ elementos do corpo K. A aplicação $\sum_{i=1}^{n} a_i\sigma_i : G \to K$ dada por $(\sum_{i=1}^{n} a_i\sigma_i)(x) = \sum_{i=1}^{n} a_i\sigma_i(x)$, para cada $x \in G$, é denominada COMBINAÇÃO LINEAR dos caracteres $\sigma_1,\ldots,\sigma_n$ com coeficientes $a_1,\ldots,a_n$, e é fácil ver que ela não é necessariamenteum caracter.

Suponhamos que $\sigma_1,\ldots,\sigma_n$ são caracteres de G em K. Então, se existem elementos $a_1,\ldots,a_n$ não todos nulos no corpo K e tais que a combinação linear $\sum_{i=1}^{n} a_i\sigma_i$ é a aplicação nula, então dizemos que os caracteres dados são LINEARMENTE DEPENDENTES (ou, simplesmente,

DEPENDENTES). Em caso contrário, $\sigma_1,\ldots,\sigma_n$ são ditos caracteres LINEARMENTE INDEPENDENTES (ou, simplesmente, INDEPENDENTES). Ou seja, $\sigma_1,\ldots,\sigma_n$ são independentes se a única possibilidade de ocorrer $\sum_{i=1}^{n} a_i\sigma_i = 0$ é quando cada a_i $(i=1,2,\ldots,n)$ é nulo.

O seguinte resultado é fundamental para o que segue, e sua prova pode ser encontrada em [1].

"Se $\sigma_1,\ldots,\sigma_n$ são caracteres de G em K distintos dois a dois, então eles são caracteres independentes."

Portanto, no caso em que o grupo G é da forma E* (i.e., E - {0}) , para algum corpo E , torna-se óbvia a seguinte

Proposição 5.4:

Sejam $\sigma_1,\ldots,\sigma_n$ isomorfismos distintos dois a dois do corpo E no corpo K . Então $\sigma_1,\ldots,\sigma_n$ são caracteres independentes de E* em K .

A partir de agora, quando $\sigma_1,\ldots,\sigma_n$ são caracteres distintos dois a dois, diremos apenas que $\sigma_1,\ldots,\sigma_n$ são caracteres distintos.

Suponhamos agora que $\sigma_1,\ldots,\sigma_n$ são isomorfismos do corpo E no corpo K . Dizemos que um elemento $a \in E$ é um PONTO FIXO de $\sigma_1,\ldots,\sigma_n$ se $\sigma_1(a) = \ldots = \sigma_n(a)$. Se E = K e se, para algum $i \in \{1,2,\ldots,n\}$, σ_i é a identidade

em K, então $a \in K$ é um ponto fixo se $\sigma_j(a) = a$, para cada $j \in \{1,2,\ldots,n\}$, o que justifica a denominação de ponto fixo.

Se $\sigma_1,\ldots,\sigma_n$ são isomorfismos do corpo E no corpo K então o conjunto dos pontos fixos de $\sigma_1,\ldots,\sigma_n$ é um subcorpo de E, como é fácil verificar, e é chamado CORPO FIXO DE $\sigma_1,\ldots,\sigma_n$.

O resultado abaixo é de fundamental importância no que segue, e sua prova pode ser encontrada em [10].

Proposição 5.5:

Se $\sigma_1,\ldots,\sigma_n$ são isomorfismos (dois a dois) distintos do corpo E no corpo K e se F é um subcorpo de E contido no corpo fixo de $\sigma_1,\ldots,\sigma_n$ então a dimensão de E como espaço vetorial sobre F é maior ou igual a n.

Como conseqüência desta proposição, pode-se mostrar que se $\sigma_1,\ldots,\sigma_n$ são automorfismos distintos do corpo E e se K é o corpo fixo de $\sigma_1,\ldots,\sigma_n$ então a dimensão de E como espaço vetorial sobre K não é menor do que n.

Suponhamos agora que K é um subcorpo de E e que σ é um automorfismo de E. Dizemos que σ DEIXA K FIXO se, para cada $k \in K$, $\sigma(k) = k$, ou seja, $\sigma|_K = id_K$. É fácil então verificar que, se K é um subcorpo de E, en-

tão o conjunto dos automorfismos de E que deixam fixo K é um subgrupo de $Aut(E)$, o grupo dos automorfismos de E.

Se G é um grupo de automorfismos de E (i.e., um subgrupo de $Aut(E)$), então o corpo fixo de G é denotado por E^G, ou seja,

$$E^G = \{x \in E \mid \forall \sigma \in G, \ \sigma(x) = x\}.$$

Observação: Podemos notar que o grupo G dos automorfismos de E que deixam fixo K é determinado pelo corpo K, e $K \subset E^G$. No entanto, não ocorre, necessariamente, que o corpo fixo de G é exatamente K. Damos a seguir um exemplo que ilustra tal fato:

Sejam $K = Q$ e $E = Q(\sqrt[3]{2}) = \{\alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2\sqrt[3]{4} : \alpha_0, \alpha_1, \alpha_2 \in Q\}$, (onde $\sqrt[3]{2}$ denota a raiz cúbica real de 2). Se σ é um automorfismo de $Q(\sqrt[3]{2})$ que deixa fixo Q, então, como $[\sigma(\sqrt[3]{2})]^3 = \sigma(\sqrt[3]{2}^3) = \sigma(2) = 2$, concluimos que $\sigma(\sqrt[3]{2})$ deve também ser uma raiz cúbica de 2. Como a única raiz cúbica de 2 pertence a $Q(\sqrt[3]{2})$ é $\sqrt[3]{2}$, segue-se que $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ e, portanto, $\sigma = id_E$. Ou seja, o único automorfismo de E que deixa Q fixo é a identidade. Logo, $G = Aut(E) = \{id_E\}$ e $E^G = E \supsetneq K = Q$.

Suponhamos que E é um corpo extensão de K, e que G é um grupo de automorfismos de E. Dizemos então que E é uma EXTENSÃO DE GALOIS DE K se o corpo fixo E^G for exatamente igual a K e se a dimensão do espaço vetorial E

sobre K for finita (ou, em outras palavras, E é uma extensão finita de K). Neste caso, nos referimos ao grupo G dado acima como o GRUPO DE GALOIS DE E SOBRE K.

Então, pelos resultados anteriores, é fácil ver que, se E é uma extensão de Galois de K, o grupo de Galois de E sobre K é finito. Ainda, analisando estes mesmos resultados, poderíamos nos perguntar se a dimensão de E sobre K é exatamente igual à ordem de G. De fato, isto acontece quando $K = E^G$, como estabelece a seguinte

Proposição 5.6:

Seja G um grupo finito de ordem n de automorfismos do corpo E, e seja $K = E^G$. Então a dimensão de E como espaço vetorial sobre K é n.

Da proposição acima, torna-se evidente que se G é um grupo finito de automorfismos de E, então E é uma extensão de Galois do corpo fixo $K = E^G$, e $[E : K] = o(G)$, onde $o(G)$ denota a ordem do grupo G. Além disso, todo automorfismo de E que deixa fixo K está em G. Portanto, o grupo de Galois de E sobre K está univocamente determinado. Pode-se ver também que se E é uma extensão finita de K, então E é uma extensão de Galois de K se e só se o número de automorfismos de E que deixam K fixo é $[E : K]$.

Vejamos agora uma relação entre as extensões Galoisianas de corpos e as extensões separáveis de um corpo K. Nosso objetivo é enunciar o Teorema Fundamental da Teoria de Galois para corpos.

Proposição 5.7:

Seja E uma extensão de Galois de K. Então E é também uma extensão separável de K. Além disso, cada elemento de E é raiz de um polinômio separável e irredutível sobre K que se fatora linearmente em $E[X]$.

Finalmente, o seguinte teorema caracteriza as extensões de Galois:

Teorema 5.8:

Uma extensão E do corpo K é uma extensão de Galois de K se e só se E é o corpo de decomposição de algum polinômio separável $f(X) \in K[X]$.

Prova:

Suponhamos que E é uma extensão de Galois de K, e seja t a dimensão de E sobre K. Seja $\{\omega_1,\ldots,\omega_t\}$ uma K-base de E. Então a proposição acima nos assegura que cada ω_i $(i=1,2,\ldots,t)$ é raiz de algum polinômio $f_i(X) \in K[X]$, separável e irredutível sobre K.

Sejam agora $\alpha_1,\ldots,\alpha_n$ todas as raízes distintas de $f_1(X),\ldots,f_t(X)$, no corpo de decomposição do polinômio $f_1(X)\, f_2(X) \ldots f_t(X)$. É fácil ver então que o polinômio $f(X) = (X-\alpha_1)\ldots(X-\alpha_n)$ é um elemento de $K[X]$, já que cada automorfismo do grupo de Galois permuta as raízes $\alpha_1,\ldots,\alpha_n$ de $f(X)$. Portanto, $f(X)$ é um polinômio separável sobre K.

É claro que E contém o corpo de decomposição F de $f(X)$ sobre K. Ainda, como cada ω_i $(i=1,2,\ldots,t)$ é raiz de $f(X)$, temos que cada ω_i é um elemento de F. Logo, concluimos que E é exatamente o corpo F, o qual é o corpo de decomposição do polinômio separável $f(X)$.

Reciprocamente, se E é o corpo de decomposição de um polinômio $f(X) \in K[X]$ separável sobre K, então é claro que $E = K(\alpha_1,\ldots,\alpha_n)$, onde $\alpha_1,\ldots,\alpha_n$ são as raízes distintas de $f(X)$ em E que estão fora de K. Para mostrar que E é uma extensão de Galois de K, utilizemos indução sobre n.

Se $n = 0$ então $E = K$, que é trivialmente uma extensão de Galois de K. Suponhamos agora que $n \geqslant 1$ e que, se E é um corpo de decomposição de um polinômio separável sobre um subcorpo K' de E com um número de raízes fora de K' menor do que n (i.e., $E = K'(\alpha'_1,\ldots,\alpha'_r)$, com $r < n$) então E é uma extensão de Galois de K'.

Como $f(X)$ tem pelo menos uma raiz fora de K, é claro que, na decomposição de $f(X)$ em fatores irredutíveis em $K[X]$, aparece algum polinômio $f_1(X) \in K[X]$ de grau maior do que 1. Seja $s = \partial f_1(X) > 1$. Então alguma raiz α_i de $f(X)$, $(i=1,2,\ldots,n)$, é raiz de $f_1(X)$. Podemos supor, sem perda de generalidade, que α_1 é esta raiz. Então α_1 é um elemento algébrico sobre K e $f_1(X)$ é o seu polinômio minimal. Além disso, $[K(\alpha_1) : K] = s$ (ver [27]).

Consideremos agora $K' = K(\alpha_1)$. Então é claro

que $f(X)$ é um polinômio separável também sobre K', e $E = K'(\alpha_2,\ldots,\alpha_n)$ é ainda o corpo de decomposição de $f(X)$ sobre K'. Mas agora $f(X)$, considerado como polinômio separável sobre K', tem no máximo $n-1$ raízes fora de K'. Portanto, pela hipótese de indução, E é uma extensão de Galois de K', donde segue-se que $[E : K']$ é finito. Então, $[E : K] = [E : K'][K' : K]$ é também finito. Assim, E é uma extensão finita de K.

Para mostrar que E é uma extensão de Galois de K, resta-nos mostrar que o grupo G de automorfismos de E que deixam K fixo tem exatamente K como corpo fixo. Por hipótese, $\partial f_1(X) = s$. Suponhamos então que $a_1 = \alpha_1, a_2, \ldots, a_s$ são as raízes de $f_1(X)$ (fora de K, já que $f_1(X)$ é irredutível sobre K). Então, pelos resultados anteriores, existem s isomorfismos distintos $\sigma_i : K(\alpha_1) \to K(a_i)$ $(i=1,2,\ldots,s)$ que são extensões da id_K (e caracterizados por $\sigma_i(\alpha_1) = a_i$). Além disso, tais isomorfismos podem ser estendidos a automorfismos de E, automorfismos estes que vamos representar por $\overline{\sigma}_i$ $(i=1,2,\ldots,s)$. Então é claro que cada extensão $\overline{\sigma}_i$ deixa K fixo, ou seja, $\overline{\sigma}_i \in G$, para cada $i \in \{1,2,\ldots,s\}$.

Seja $e \in E^G$. Queremos mostrar que e é um elemento de K. Observemos antes que tal elemento e não pode estar fora de $K(\alpha_1)$. De fato, como E é extensão de Galois de $K(\alpha_1)$, o corpo fixo do grupo de Galois G' desta extensão é exatamente $K(\alpha_1)$. Portanto, dizer que e não está

em $K(\alpha_1)$ significa dizer que existe um automorfismo $\delta \in G'$ tal que $\delta(e) \neq e$. Uma contradição, já que $G' \subset G$.

Portanto, $e \in K(\alpha_1)$, e pode ser escrito na forma $e = c_0 + c_1\alpha_1 + \ldots + c_{s-1}\alpha_1^{s-1}$, com $c_i \in K$, para cada $i \in \{0,1,\ldots,s-1\}$. Assim, para cada $j \in \{1,2,\ldots,s\}$, $e = \bar{\sigma}_j(e) = \sum_{i=0}^{s-1} c_i \bar{\sigma}_j(\alpha_1)^i = \sum_{i=0}^{s-1} c_i a_j^i$.

Então o polinômio $p(X)$ de grau $s-1$ dado por $p(X) = c_{s-1}X^{s-1} + \ldots + c_1X + (c_0 - e) \in E[X]$ tem pelo menos s raízes distintas em E (a saber: $a_1, a_2, \ldots, a_s$) , o que implica que $p(X)$ é identicamente nulo, ou seja, $e = c_0 \in K$, o que completa a prova. □

Para terminar, enunciamos agora o Teorema Fundamental da Teoria de Galois para corpos. Sua prova pode ser encontrada em [1] ou [10], ou também no capítulo III.

Seja E uma extensão de Galois de K , com grupo de Galois G . Denotando por $\mathcal{G}(G)$ o conjunto de todos os subgrupos de G e por $\mathcal{C}(K,E)$ o conjunto de todos os corpos intermediários entre K e E , então, a cada corpo intermediário $F \in \mathcal{C}(K,E)$, podemos associar o subgrupo $G_F = \{\sigma \in G \mid \sigma_{|F} = id_F\}$ de G . Reciprocamente, a cada subgrupo H de G podemos fazer corresponder um corpo intermediário entre K e E , a saber, o corpo fixo de E por H , E^H .

Tal correspondência entre os conjuntos $\mathcal{G}(G)$ e $\mathcal{C}(K,E)$ é biunívoca, como vemos a seguir.

Teorema 5.9:

Se E é uma extensão de Galois de K com grupo de Galois G, então:

(i) a correspondência anterior entre $G(G)$ e $C(K,E)$ é uma correspondência 1-1 (usualmente chamada de CORRESPONDÊNCIA DA TEORIA DE GALOIS). Mais ainda, para cada corpo intermediário F entre K e E, a extensão E sobre F é uma extensão de Galois, cujo grupo de Galois é G_F;

(ii) um corpo intermediário $F \in C(K,E)$ é uma extensão de Galois de K se e só se o subgrupo G_F de G é normal em G. Neste caso, o grupo de Galois desta extensão é isomorfo a G/G_F;

(iii) para cada corpo intermediário $F \in C(K,E)$, $[E : F] = o(G_F)$ (onde $o(G_F)$ denota a ordem do grupo G_F), e $[F : K]$ é igual ao índice de G_F em G.

NOTA: Com tal correspondência da teoria de Galois, é claro que $G_E = G$ e $G_K = \{id_E\}$.

§ 6. MÓDULOS E ANÉIS SEMI-SIMPLES

Nesta seção, fazemos um resumo de conceitos e resultados que vamos necessitar neste trabalho sobre módulos e anéis semi-simples. Maiores detalhes, porém, podem ser encontrados em [25].

No que segue, R denota um anel com unidade e M um R-módulo à esquerda. No entanto, todas as definições e resultados podem ser obtidos similarmente quando M é um R-módulo à direita.

Dizemos que M é um R-MÓDULO SIMPLES ou IRREDUTÍVEL se M é não nulo e se os únicos submódulos de M são (0) e M (i.e., M não possui submódulos próprios). O anel R é dito SIMPLES se ele próprio, considerado como R-módulo à esquerda, é simples. Ainda, M é dito um R-MÓDULO SEMI-SIMPLES se é uma soma direta de R-módulos simples.

Teorema 6.1:

Para que um R-módulo M seja semi-simples é necessário e suficiente que cada R-submódulo de M seja um somando direto de M .

Prova:

Suponhamos $M = \bigoplus_{\alpha \in \Lambda} M_\alpha$, onde Λ é um conjunto de índices e M_α é um R-módulo simples, para cada $\alpha \in \Lambda$. Para cada subconjunto $\Gamma \subset \Lambda$, coloquemos $M_\Gamma = \bigoplus_{\alpha \in \Gamma} M_\alpha$, e denotemos por M_ϕ o submódulo nulo de M : $M_\phi = (0)$.

Seja N um submódulo de M , e consideremos o conjunto $S_N = \{\Gamma \subset \Lambda \mid M_\Gamma \cap N = (0)\}$. É fácil verificar que S_N é um conjunto indutivo. Logo, pelo Lema de Zorn, existe em S_N um elemento maximal, que vamos denotar por Δ . Assim, $M_\Delta \cap N = (0)$. Queremos mostrar que $M_\Delta \oplus N = M$.

Observemos que se $\alpha \in \Lambda - \Delta$ então é claro que

$\Delta \cup \{\alpha\} \notin S_N$, pelo carater maximal de Δ . Logo, $(M_\alpha + M_\Delta) \cap N \neq (0)$, ou seja, existem elementos $m \in M_\Delta$, $m_\alpha \in M_\alpha$, $n \in N$ tais que $n \neq 0$ e $m + m_\alpha = n$, donde $m_\alpha = n - m \in M_\Delta + N$. Logo, $(M_\Delta + N) \cap M_\alpha \neq (0)$. (De fato, se $m_\alpha = 0$, então $n = m \in M_\Delta \cap N = (0)$, uma contradição). Assim, como $(M_\Delta + N) \cap M_\alpha$ é um submódulo não nulo de M_α (que é um módulo simples) temos necessariamente $(M_\Delta + N) \cap M_\alpha = M_\alpha$.

Concluimos que se α é um elemento arbitrário de $\Lambda - \Delta$, então $M_\alpha \subset (M_\Delta + N)$. Assim $M = \bigoplus_{\alpha \in \Lambda} M_\alpha \subset M_\Delta + N$, donde segue que $M = M_\Delta + N$.

Para mostrar a recíproca, suponhamos que todo R-submódulo de M é um somando direto de M , e sejam N e P submódulos de M tais que P é também um submódulo de N . Então sabemos que $M = P \oplus Q$, para algum submódulo Q de M . Aplicando a lei modular, podemos escrever $N = M \cap N = (P \oplus Q) \cap N = P \oplus (Q \cap N)$, ou seja, P é também um somando direto do A-módulo N . Mas como P é um submódulo arbitrário de N , concluimos que N tem a mesma propriedade de M , (i.e., todo submódulo de N é um somando direto de N).

Mostremos agora que cada submódulo não nulo N de M contém um módulo simples. Para tal, suponhamos que $x \in N$ é um elemento não nulo. Podemos considerar a família F formada por todos os submódulos N' de N tais que $x \notin N'$. É fácil verificar que F é um conjunto indutivo e, portanto, admite um elemento maximal, que será denotado

por P . Então P é um submódulo de N que não comtém o elemento x de N . Mas $N = P \oplus Q$ para algum submódulo Q de N . Vamos mostrar que Q é um módulo simples.

De fato, se Q' é um submódulo próprio de Q , pela observação feita sobre todos os submódulos de M , vemos que Q' é um somando direto de Q , ou seja, existe T , um submódulo de Q , tal que $Q = Q' \oplus T$. Assim, $N = P \oplus Q = P \oplus Q' \oplus T$. Pelo carater maximal de P , $P \oplus Q'$ e $P \oplus T$ são submódulos não pertencentes a F , ou seja, $x \in (P \oplus Q') \cap (P \oplus T)$. Então, podemos escrever: $x = p + q' = p' + t$, para determinados elementos $p, p' \in P$, $q' \in Q'$, $t \in T$. Assim, $p - p' = t - q' \in P \cap (T \oplus Q') =$ $= P \cap Q = (0)$, ou seja, $t = q' \in T \cap Q' = (0)$, ou ainda, $x = p \in P$, uma contradição. Logo, Q é um módulo simples.

Finalmente, mostremos que M é uma soma direta de módulos simples. Se S denota o conjunto de todas as famílias da forma $\{S_\alpha\}_{\alpha \in \Gamma}$ onde cada S_α é um R-submódulo simples de M e $\sum_{\alpha \in T} S_\alpha$ é uma soma direta, então é fácil verificar que S é também um conjunto indutivo. Sejam $\{S_\beta\}_{\beta \in \Gamma'}$ seu elemento maximal, $N = \bigoplus_{\beta \in \Gamma'} S_\beta$ e P o submódulo de M tal que $M = N \oplus P$.

Observemos agora que se P é não nulo, então ele contém algum submódulo simples P' que é ainda um somando direto de P . Mas então neste caso é fácil verificar que $N + P$ é também uma soma direta de módulos simples, o que contraria o carater maximal da família $\{S_\beta\}_{\beta \in \Gamma'}$. Logo, $M = N = \bigoplus_{\beta \in \Gamma'} S_\beta$, o que completa a prova. □

Apresentamos a seguir um resultado que caracteriza os anéis semi-simples. Observe-se que com o teorema anterior prova-se facilmente a equivalência (a)⇔(b) , uma vez que os R-submódulos de um anel R são exatamente seus ideais. O resto da prova pode ser encontrada em [25] (ver teorema 5.1, cap. 6) . Para a definição de módulo injetivo, pode-se consultar também [15] .

Teorema 6.2:

Seja R um anel com unidade. As seguintes condições são equivalentes:

(a) R é um R-módulo à esquerda semi-simples;

(b) cada ideal à esquerda de R é um somando direto de R ;

(c) cada R-módulo à esquerda é injetivo;

(d) todo R-módulo à esquerda é semi-simples;

(e) toda seqüência exata $0 \to M' \to M \to M'' \to 0$ de R-módulos à esquerda cinde;

(f) todo R-módulo à esquerda é projetivo;

Quando um anel R verifica alguma, e, portanto, todas, as condições do teorema acima, então ele é denominado um ANEL SEMI-SIMPLES.

Um elemento a de um anel R é dito NILPOTENTE se existe algum inteiro n tal que $a^n = 0$. Um ideal à esquerda I de R é dito NILPOTENTE se existe um inteiro m tal que $I^m = 0$. (Ou seja, para cada $x_1, \ldots, x_m \in I$, $x_1 x_2 \ldots x_m = 0$).

Lema 6.3:

Se R é um anel semi-simples, então, para todo ideal à esquerda I de R, existe um elemento idempotente $e \in I$ tal que $Ie = Ae = I$ e $I(1-e) = 0$.

Prova:

Como R é semi-simples, sabemos que, se I é um ideal à esquerda de R , então existe um ideal à esquerda I' de R tal que $R = I \oplus I'$. Sejam $e \in I$, $e' \in I'$ tais que $1 = e + e'$. Então, para cada $x \in I$, $x = xe + xe'$, donde segue-se que $xe = x$ e $xe' = 0$, ou seja, $Re \subset I \subset Ie \subset Re$. Assim, $Ie = Re = I$. Além disso, da igualdade $xe' = 0$, é fácil ver que $I(1-e) = 0$. □

Lembrando que o radical de Jacobson $J(R)$ de um anel com unidade R é a intersecção de todos os ideais maximais à esquerda de R , podemos mostrar a seguinte

Proposição 6.4:

Se R é um anel semi-simples,então o radical de Jacobson $J(R)$ de R é nulo.

Prova:

Sabemos que $J(R)$ é um ideal à esquerda de R . Então, pelo lema anterior, existe um idempotente $e \in J(R)$ tal que $x(1-e) = 0$, para cada $x \in R$. Mas como $e \in J(R)$, $1-e$ é um elemento inversível, donde segue-se que $x = 0$, o que completa a prova. □

Proposição 6.5:

Todo ideal à esquerda nilpotente de um anel arbitrário R está contido no radical de Jacobson de R.

Prova:

De fato, se I é um ideal à esquerda nilpotente de R e M é um ideal maximal à esquerda de R, então $I + M = M$ ou $I + M = R$. Observemos que, se $I + M = R$, então $1 = i + m$, para algum $i \in I$, $m \in M$. Mas como $i \in I$ é um elemento nilpotente, $m = 1 - i$ é um elemento inversível (cujo inverso é $1 + i + \ldots + i^{n-1}$, se $i^n = 0$), uma contradição, já que $m \in M$.

Então $I + M = M$, donde segue-se que $I \subset M$. Como M é um ideal maximal à esquerda arbitrário, temos $I \subset \bigcap_{\substack{M \text{ maximal} \\ \text{à esquerda}}} M = J(R)$. □

Corolário 6.6:

Um anel semi-simples não contém ideais nilpotentes à esquerda, além do trivial.

Deste corolário, é fácil mostrar a seguinte

Proposição 6.7:

Se R é um anel comutativo e semi-simples, então R não possui elementos nilpotentes.

Prova:

De fato, se $x \in R$ é um elemento nilpotente e se $n \in \mathbb{Z}$ é tal que $x^n = 0$, então $(Rx)^n = R^n x^n = 0$. Ou seja, o ideal Rx é um ideal à esquerda nilpotente e, portanto, pelo

corolário acima, $Rx = 0$. Logo, $x = 0$. □

Da prova acima fica claro que se R não contém elementos nilpotentes então não contém ideais nilpotentes não triviais, mas a recíproca só é válida se R é um anel comutativo.

CAPÍTULO II

ÁLGEBRAS SEPARÁVEIS E EXTENSÕES SEPARÁVEIS DE ANÉIS

Neste capítulo, apresentamos a teoria fundamental das álgebras separáveis, e supomos que todo o anel considerado tem unidade e todo homomorfismo de anéis leva unidade em unidade. Ainda, R denota um anel comutativo com unidade, e o símbolo $\otimes$ significa $\otimes_R$.

§ 1 . DEFINIÇÃO E EXEMPLOS DE ÁLGEBRAS SEPARÁVEIS

Antes de apresentar o conceito de álgebra separável, definimos derivação e derivação interior.

Sejam A uma R-álgebra e M um A/R-módulo bilateral. Uma R-DERIVAÇÃO $\partial : A \to M$ é uma aplicação R-linear (i.e., um homomorfismo de R-módulos) que satisfaz:

$$\partial(ab) = \partial(a).b + a.\partial(b) \quad , \text{ para todo } a,b \in A .$$

Então é fácil ver que, neste caso, $\partial(R.1_A) = 0$.

Denotamos por $Der_R(A,M)$ o conjunto de todas as R-derivações da R-álgebra A no A/R-módulo bilateral M .

Tal conjunto é um R-módulo à esquerda se consideramos a adição de funções e a operação externa dada por $(r.\partial)(a) = r.\partial(a)$, para cada $r \in R$, $\partial \in Der_R(A,M)$, $a \in A$, como é fácil verificar.

Dizemos que uma R-derivação $\partial : A \to M$ é INTERIOR se existe um $m \in M$ tal que $\partial(a) = a.m - m.a$, para cada $a \in A$. Denotamos por $Derint_R(A,M)$ o conjunto das R-derivações interiores da R-álgebra A no A/R-módulo bilateral M . É fácil ver que este conjunto é um R-submódulo de $Der_R(A,M)$.

Sejam A uma R-álgebra e A^e sua álgebra envolvente. A aplicação linear $\mu : A^e \to A$ definida por

$$\mu(a \otimes b) = ab \text{ , para cada } a \otimes b \in A^e \text{ ,}$$

está bem definida e é um homomorfismo de A^e-módulos à esquerda (ou, equivalentemente, de A/R-módulos bilaterais). De fato, considerando a aplicação $h : A \times A^0 \to A$, definida por $h(a,b) = ab$, para todo par $(a,b) \in A \times A^0$, temos claramente que h é uma forma bilinear. Logo, pela propriedade universal do produto tensorial sobre R , sabemos que existe um único homomorfismo $\overline{h} : A \otimes A^0 \to A$ tal que $\overline{h}(a \otimes b) = h(a,b) = ab$, para todo $a \otimes b \in A^e$. Agora é claro que $\overline{h} = \mu$. É fácil ver ainda que o homomorfismo μ é um epimorfismo de A^e-módulos. Tal aplicação é denominada HOMOMORFISMO CONTRAÇÃO .

Consideremos agora o núcleo do homomorfismo μ e o denotemos por J . Então podemos formar a seguinte seqüência exata de A^e-módulos à esquerda

$$0 \to J \xrightarrow{i} A^e \xrightarrow{\mu} A \to 0 \qquad [1]$$

onde i representa a inclusão canônica.

Além disso, para cada $a \in A$, $a \otimes 1 - 1 \otimes a$ é um elemento de J , já que $\mu(a \otimes 1 - 1 \otimes a) = a - a = 0$. Reciprocamente, se $\sum_{i=1}^{n} a_i \otimes b_i$ é um elemento de J , então é claro que $\sum_{i=1}^{n} a_i b_i = 0$ e, portanto,

$$0 = 0 \otimes 1 = \sum_{i=1}^{n} a_i b_i \otimes 1 \text{ , donde temos que}$$

$$\sum_{i=1}^{n} a_i \otimes b_i = \sum_{i=1}^{n} a_i \otimes b_i - \left(\sum_{i=1}^{n} a_i b_i \otimes 1 \right) = \sum_{i=1}^{n} (a_i \otimes 1)\left[1 \otimes b_i - b_i \otimes 1\right]$$

Podemos concluir, então, que J é exatamente o ideal gerado por todos os elementos da forma $1 \otimes a - a \otimes 1$, com $a \in A$.

A partir de agora, denotaremos o homomorfismo contração pelo símbolo μ , e J denotará sempre seu núcleo.

Observemos agora que a aplicação $\delta : A \to J$ definida por $\delta(a) = a \otimes 1 - 1 \otimes a$, para cada $a \in A$, é uma R-derivação. De fato, para cada $a, b \in A$, $r \in R$,

$$\delta(r.a + b) = (r.a + b) \otimes 1 - 1 \otimes (r.a + b) = r.a \otimes 1 + b \otimes 1 - 1 \otimes r.a - 1 \otimes b =$$

$$= r.(a \otimes 1 - 1 \otimes a) + (b \otimes 1 - 1 \otimes b) = r.\delta(a) + \delta(b) \quad \text{e}$$

$$\delta(ab) = ab \otimes 1 - 1 \otimes ab = ab \otimes 1 - a \otimes b + a \otimes b - 1 \otimes ab =$$

$$= a.(b \otimes 1 - 1 \otimes b) + (a \otimes 1 - 1 \otimes a).b = a.\delta(b) + \delta(a).b .$$

Além disso, se M é um A/R-módulo bilateral, então uma R-derivação $\partial : A \to M$ é interior se e só se existe um elemento $m \in M$ tal que $\partial(a) = \delta(a).m$, para cada $a \in A$, como é fácil verificar.

Para mostrar o teorema que caracteriza as álgebras separáveis, necessitamos do seguinte

Lema 1.1:

Sejam A e B anéis e M,N dois módulos da categoria ${}_A^{M}{}_B$. Então M é um somando direto de r cópias do A-B-bimódulo N se e só se existem aplicações $f_1,\ldots,f_r$ de M em N e $g_1,\ldots,g_r$ de N em M , todas elas homomorfismos de A-B-bimódulos, tais que $\sum_{i=1}^{r} g_i \circ f_i = id_M$.

Prova:

Suponhamos que M é um somando direto de $N^{(r)}$. Denotemos por π e j , respectivamente, os homomorfismos projeção canônica de $N^{(r)}$ em M e a inclusão canônica de M em $N^{(r)}$. Para cada $s \in \{1,2,\ldots,r\}$, sejam $i_s : N \to N^{(r)}$ a inclusão canônica de N no s-ésimo somando de $N^{(r)}$ e $\pi_s : N^{(r)} \to N$ a projeção canônica de $N^{(r)}$ no s-ésimo somando N . Então, pondo $g_s = \pi \circ i_s$ e $f_s = \pi_s \circ j$, para cada $s \in \{1,2,\ldots,r\}$, vem que $\sum_{s=1}^{r} g_s \circ f_s = \sum_{s=1}^{r} \pi \circ i_s \circ \pi_s \circ j =$

$= \pi \circ id_{N^{(r)}} \circ j = id_M$.

Para mostrar a recíproca, consideramos a aplicação $\pi : N^{(r)} \to M$ dada por $\pi(n_1,\ldots,n_r) = \sum_{i=1}^{r} g_i(n_i)$, para cada r-upla $(n_1,\ldots,n_r) \in N^{(r)}$. Então, considerando também

o homomorfismo $j : M \to N^{(r)}$ dado por $j(m) = (f_1(m), \ldots, f_r(m))$, é fácil verificar que $\pi \circ j = id_M$, ou seja, M é um somando direto de $N^{(r)}$, como A-B-bimódulo. □

Teorema 1.2:

Seja A uma R-álgebra. Então as seguintes condições são equivalentes:

(i) A é um A^e-módulo projetivo;

(ii) a seqüência exata de A^e-módulos à esquerda

$$0 \to J \xrightarrow{i} A^e \xrightarrow{\mu} A \to 0 \quad \text{cinde;}$$

(iii) existe um elemento $e \in A^e$ tal que $\mu(e) = 1$ e $Je = 0$;

(iv) existem elementos $x_i, y_i \in A$ $(i=1,2,\ldots,n)$, tais que $\sum_{i=1}^{n} x_i y_i = 1$ e $\sum_{i=1}^{n} x x_i \otimes y_i = \sum_{i=1}^{n} x_i \otimes y_i x$, para cada $x \in A$;

(v) A, considerado como A-módulo bilateral, é isomorfo a um somando direto de um número finito de cópias do A-módulo bilateral $A^e = A \otimes A^0$;

(vi) a derivação $\delta : A \to J$, definida por $\delta(a) = a \otimes 1 - 1 \otimes a$, para cada $a \in A$, é interior;

(vii) para cada A/R-módulo bilateral M, toda R-derivação $\partial : A \to M$ é interior.

Prova:

É claro que (i) e (ii) são equivalentes.

Suponhamos que a seqüência exata $0 \to J \xrightarrow{i} A^e \xrightarrow{\mu} A \to 0$ cinde, e seja $\nu : A \to A^e$ um homomorfismo de A^e-módulos à esquerda tal que $\mu\nu = id_A$. Pondo $e = \nu(1)$, temos que $\mu(e) = \mu\nu(1) = 1$. Além disso, para cada gerador $1 \otimes a - a \otimes 1 \in J$, $(1 \otimes a - a \otimes 1)e = (1 \otimes a - a \otimes 1)\nu(1) = \nu[(1 \otimes a).1 - (a \otimes 1).1] = \nu(a - a) = 0$. Logo, $Je = 0$ e, portanto, (ii) implica (iii).

Reciprocamente, se $e \in A^e$ representa o elemento dado em (iii), consideremos a aplicação $\nu : A \to A^e$ definida por $\nu(a) = (a \otimes 1)e$, para todo elemento $a \in A$. Utilizando a hipótese de que $Je = 0$, vemos facilmente que ν é um homomorfismo de A^e-módulos. Além disso, para todo $a \in A$, $\mu\nu(a) = \mu[(a \otimes 1)e] = (a \otimes 1)\mu(e) = a$, ou seja, $\mu\nu = id_A$. Portanto, a seqüência exata [1] de A^e-módulos à esquerda cinde. Assim, (iii) implica (ii).

É fácil ver que (iii) e (iv) são equivalentes. De fato, um elemento $e = \sum_{i=1}^{n} x_i \otimes y_i \in A^e$ é tal que $\mu(e) = 1$ e $Je = 0$ se e só se $\sum_{i=1}^{n} x_i y_i = 1$ e, para cada $x \in A$, $(x \otimes 1 - 1 \otimes x) \sum_{i=1}^{n} x_i \otimes y_i = 0$, ou ainda, $\sum_{i=1}^{n} x_i y_i = 1$ e $\sum_{i=1}^{n} x x_i \otimes y_i = \sum_{i=1}^{n} x_i \otimes y_i x$, para cada $x \in A$. A recíproca é também evidente.

É óbvio que (ii) implica (v) e que (vii) implica (vi).

Suponhamos então que A é isomorfo a um somando direto de r cópias de A^e. Então, pelo lema anterior, existem homomorfismos de A^e-módulos à esquerda $f_1, \ldots, f_r$

de A em A^e e $g_1,\ldots,g_r$ de A^e em A, tais que $\sum_{i=1}^{r} g_i f_i = id_A$.

Suponhamos agora que, para cada $i \in \{1,2,\ldots,r\}$, $f_i(1) = \sum_j a_j^{(i)} \otimes b_j^{(i)} \in A^e$ e $g_i(1\otimes 1) = c_i$. Então, para todo $r \in R$, $i \in \{1,2,\ldots,r\}$, $rc_i = g_i(r\otimes 1) = g_i(1\otimes r) = g_i(1\otimes 1)r = c_i r$, e, portanto, a aplicação linear dada por $a\otimes b \mapsto ac_i \otimes b$, para cada $a\otimes b \in A^e$ está bem definida e é um homomorfismo de A^e-módulos.

Além disso, para todo $x \in A$,

$$(x\otimes 1)(\sum_j a_j^{(i)} \otimes b_j^{(i)}) = (x\otimes 1) f_i(1) = f_i(x) = f_i(1)(1\otimes x) =$$

$$= (\sum_j a_j^{(i)} \otimes b_j^{(i)})(1\otimes x) .$$

Portanto, como

$$\sum_{i,j} a_j^{(i)} c_i b_j^{(i)} = \sum_i g_i(\sum_j a_j^{(i)} \otimes b_j^{(i)}) = (\sum_i g_i f_i)(1) = 1 ,$$

concluimos que o elemento $\sum_{i,j} a_j^{(i)} c_i \otimes b_j^{(i)} \in A^e$ satisfaz as condições estabelecidas em (iii), ou seja, (v) implica (iii).

Suponhamos agora que a R-derivação $\delta : A \to J$ dada em (vi) é interior. Então existe um elemento $\sum_{i=1}^{n} a_i \otimes b_i \in J$ tal que, para cada $x \in A$,

$$\delta(x) = x \sum_{i=1}^{n} a_i \otimes b_i - \sum_{i=1}^{n} a_i \otimes b_i x , \text{ ou seja,}$$

$$(x\otimes 1 - 1\otimes x) = x \sum_{i=1}^{n} a_i \otimes b_i - \sum_{i=1}^{n} a_i \otimes b_i x .$$ Portanto, para

cada $x \in A$,

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

Assim, pondo $e = 1\otimes 1 - \sum_{i=1}^{n} a_i \otimes b_i$, temos que $ex = xe$, para cada $x \in A$, e $\mu(e) = 1 - \sum_{i=1}^{n} a_i b_i = 1$. Consequentemente, o elemento $e \in A^e$ satisfaz as condições estabelecidas em (iii), ou seja, (vi) implica (iii).

Finalmente, mostremos que (iii) implica (vii). De fato, se $e = \sum_{i=1}^{n} x_i \otimes y_i \in A^e$ é o elemento dado em (iii), então sabemos que, para cada $x \in A$, $\sum_{i=1}^{n} x x_i \otimes y_i = \sum_{i=1}^{n} x_i \otimes y_i x$. Além disso, se M é um A/R-módulo bilateral e $\partial : A \to M$ é uma R-derivação, então sabemos que a aplicação $\partial \otimes id : A \otimes A^0 \to M \otimes A^0$ dada por $(\partial \otimes id)(a \otimes b) = \partial(a) \otimes b$, para cada $a \otimes b \in A^e$, está bem definida e, portanto, para cada $x \in A$,

$$\sum_{i=1}^{n} \partial(x x_i) \otimes y_i = \sum_{i=1}^{n} \partial(x_i) \otimes y_i x \quad .$$

Ainda, considerando a aplicação $\phi : M \otimes A^0 \to M$ definida por $\phi(m \otimes a) = m.a$, para cada $m \otimes a \in M \otimes A^0$, podemos escrever, para cada $x \in A$,

$$\phi\left(\sum_{i=1}^{n} \partial(x x_i) \otimes y_i\right) = \phi\left(\sum_{i=1}^{n} \partial(x_i) \otimes y_i x\right) \text{ , ou}$$

seja $\sum_{i=1}^{n} \partial(x).x_i y_i + \sum_{i=1}^{n} x.\partial(x_i).y_i = \sum_{i=1}^{n} \partial(x_i).y_i x$, para cada $x \in A$. Mas como $\sum_{i=1}^{n} \partial(x).x_i y_i = \partial(x)$, temos que

$$\partial(x) = \sum_{i=1}^{n} \partial(x_i).y_i x - \sum_{i=1}^{n} x.\partial(x_i).y_i \text{ , para}$$

cada $x \in A$. Portanto, pondo $m = \sum_{i=1}^{n} \partial(x_i).y_i$, resulta que ∂ é a R-derivação interior definida pelo elemento m . □

Dada uma R-álgebra A , dizemos que A é uma R-ÁLGEBRA SEPÁRAVEL (ou, simplesmente, que A é R-SEPARÁVEL) se alguma (e portanto todas) as condições equivalentes do teorema anterior é verificada.

Podemos observar que o elemento $e \in A^e$ dado em (iii) do mesmo teorema é um idempotente de A^e . De fato, $e^2 - e = (e - 1\otimes 1)e$ que é nulo, já que, $e - 1\otimes 1$ é um elemento de J , como é fácil verificar. Portanto, $e = e^2$, e é por isso que, quando a R-álgebra A é separável, dizemos que tal elemento e é um IDEMPOTENTE DE SEPARABILIDADE PARA A .

Apresentamos agora alguns exemplos de álgebras separáveis.

1. É óbvio que o próprio anel R é uma R-álgebra separável; mais geralmente, $R^{(n)} = R \oplus \ldots \oplus R$ é também uma R-álgebra separável, para qualquer inteiro positivo n . De fato, sabemos que os elementos $e_1 = (1,0,0,\ldots,0)$, $e_2 = (0,1,\ldots,0)$, $,\ldots,$ $e_n = (0,0,\ldots,1)$ de $R^{(n)}$ são idempotentes ortogonais e formam uma base do R-módulo $R^{(n)}$. Então, pondo $e = \sum_{j=1}^{n} e_j \otimes e_j$, temos, para cada $\alpha = \sum_{i=1}^{n} r_i.e_i \in R^{(n)}$,

$$(\alpha\otimes 1 - 1\otimes\alpha)e = \sum_{i,j=1}^{n} (r_i.e_i)e_j\otimes e_j - \sum_{i,j=1}^{n} e_j\otimes e_j(r_i.e_i)$$

$$= \sum_{j=1}^{n} (r_j.e_j \otimes e_j - e_j \otimes r_j.e_j) = 0$$

Por outro lado, $\mu(e) = \sum_{j=1}^{n} e_j = 1_{(R^n)}$.

2. Para mostrar que a R-álgebra $M_n(R)$ das matrizes de ordem $n \times n$ sobre R é separável, consideremos as matrizes canônicas E_{ij} para $i,j \in \{1,2,\ldots,n\}$, (i.e., $E_{ij} = (e_{rs})_{\substack{1 \leq r \leq n \\ 1 \leq s \leq n}}$, onde $e_{rs} = \delta_{ri}\delta_{sj}$), e definimos então

$e = \sum_{i=1}^{n} E_{ij} \otimes E_{ji}$, onde o índice j é fixo. Então $\mu(e) = \sum_{i=1}^{n} E_{ij}E_{ji} = \sum_{i=1}^{n} E_{ii} = I$. Portanto, resta-nos provar apenas que $Je = 0$. Para tal, é suficiente mostrarmos que $(E_{k\ell} \otimes I - I \otimes E_{k\ell})e = 0$, para k e ℓ percorrendo o conjunto $\{1,2,\ldots,n\}$, como é fácil verificar. Então

$$(E_{k\ell} \otimes I - I \otimes E_{k\ell})e = (E_{k\ell} \otimes I - I \otimes E_{k\ell})(\sum_{i=1}^{n} E_{ij} \otimes E_{ji}) =$$

$$= \sum_{i=1}^{n} (E_{k\ell}E_{ij} \otimes E_{ji} - E_{ij} \otimes E_{ji}E_{k\ell}) =$$

$$= E_{kj} \otimes E_{j\ell} - E_{kj} \otimes E_{j\ell} = 0 \text{ , o que completa}$$

a prova.

Observemos que, neste exemplo, fica claro que o idempotente de separabilidade de uma álgebra separável não é único necessariamente.

3. Seja G um grupo multiplicativo finito, de ordem n , tal que $n = n\,1_R$ é um elemento inversível em R .

Mostremos que, nestas condições, a R-álgebra de grupo $R[G]$ é separável sobre R. De fato, definindo $e = \frac{1}{n} \sum_{g \in G} g \otimes g^{-1}$, temos que $\mu(e) = \frac{1}{n} \sum_{g \in G} g\, g^{-1} = \frac{1}{n} \sum_{g \in G} 1 = \frac{1}{n}(n\,1) = 1_{R[G]}$. Além disso, para provarmos que $Je = 0$, é fácil verificar que é suficiente mostrarmos que $(h \otimes 1)e = (1 \otimes h)e$, para cada elemento h do grupo G. Então, para cada $h \in G$, fazendo a mudança de variável $\omega = hg$ no grupo G,

$$(h \otimes 1)e = \frac{1}{n} \sum_{g \in G} (hg \otimes g^{-1}) = \frac{1}{n} \sum_{\omega \in G} (\omega \otimes \omega^{-1}h) = (1 \otimes h)\frac{1}{n} \sum_{\omega \in G} (\omega \otimes \omega^{-1}) =$$

$= (1 \otimes h)e$, o que completa a prova.

Pode-se mostrar, reciprocamente, que, se $R[G]$ é uma R-álgebra separável, então n é um elemento inversível em R.

4. Seja W um sistema multiplicativo do anel R. Então já sabemos que o anel localizado $R_W = \{r/_\omega \mid r \in R \text{ e } \omega \in W\}$ é uma R-álgebra. Observemos agora que, para cada $r/_\omega \in R_W$,

$$r/_\omega \otimes \omega/_\omega - \omega/_\omega \otimes r/_\omega = (r\omega - \omega r).(1/_\omega \otimes 1/_\omega) = 0\,,$$

e então é óbvio que a unidade $\omega/_\omega \otimes \omega/_\omega$ da álgebra envolvente $(R_W)^e$ é um idempotente de separabilidade. Assim, o anel R_W é uma R-álgebra separável. Pode-se ainda mostrar que, neste caso, o homomorfismo contração é um isomorfismo, o que deixamos a cargo do leitor.

Finalmente, damos aqui um exemplo de uma álgebra

que não é separável. Vimos no capítulo I que se K é um corpo então o anel de polinômios $K[X]$ é uma K-álgebra. No entanto, $K[X]$ não é separável sobre K. De fato, sendo K um corpo, é óbvio que $K[X]$ é um K-módulo projetivo. Portanto, se $K[X]$ é uma álgebra separável sobre K, então $K[X]$ é um K-módulo finitamente gerado (ver Proposição 2.10), uma contradição.

§ 2. ALGUMAS PROPRIEDADES DAS ÁLGEBRAS SEPARÁVEIS

Nesta seção, apresentamos alguns resultados sobre as álgebras separáveis, que nos serão úteis ao longo deste trabalho.

Proposição 2.1: (Transitividade da Separabilidade)

Sejam S uma R-álgebra comutativa e separável, e A uma álgebra separável sobre S. Então A é também uma R-álgebra separável.

Prova:

Sejam $\sum_{i=1}^{n} a_i \otimes b_i \in A \otimes_S A^0$ e $\sum_{j=1}^{m} \alpha_j \otimes \beta_j \in S \otimes S^0$ idempotentes que satisfazem as condições de separabilidade de A sobre S e de S sobre R, respectivamente.

É fácil ver que a aplicação $\psi : A \times A^0 \to A \otimes A^0$ dada por $\psi(x,y) = \sum_{j=1}^{m} x\alpha_j \otimes \beta_j y$ está bem definida e é uma forma bilinear em relação à S-álgebra A. De fato, para cada

$s \in S$, $(x,y) \in A \times A^0$,

$$\psi(xs,y) = \sum_{j=1}^{m} xs\,\alpha_j \otimes \beta_j\, y = xs\Big(\sum_{j=1}^{m} \alpha_j \otimes \beta_j\Big)y = x\Big(\sum_{j=1}^{m} \alpha_j \otimes \beta_j\Big)sy =$$

$$= \sum_{j=1}^{m} x\,\alpha_j \otimes \beta_j\, sy = \psi(x,sy)$$

Portanto, pela propriedade universal do produto tensorial sobre S , vemos que a aplicação $\phi : A \otimes_S A^0 \to A \otimes A^0$, dada por $\phi(x \otimes y) = \sum_{j=1}^{m} x\,\alpha_j \otimes \beta_j\, y$ está bem definida. Além disso, tal aplicação é claramente um homomorfismo de A/R-módulos bilaterais.

Representando por μ o homomorfismo contração referente à R-álgebra A , e pondo $e = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \alpha_j \otimes \beta_j b_i$, temos:

$$\mu(e) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \alpha_j \beta_j b_i = \sum_{i=1}^{n} a_i \Big(\sum_{j=1}^{m} \alpha_j \beta_j\Big) b_i = 1 \ ,$$

e, para cada $a \in A$,

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a\,a_i\,\alpha_j \otimes \beta_j\, b_i = \phi\Big(\sum_{i=1}^{n} a\,a_i \otimes b_i\Big) = \phi\Big(\sum_{i=1}^{n} a_i \otimes b_i a\Big) =$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \alpha_j \otimes \beta_j\, b_i\, a \ , \text{ o que}$$

mostra que A é uma R-álgebra separável. □

Proposição 2.2:

Sejam S uma R-álgebra comutativa e A uma S-álgebra que é separável sobre R . Então A é uma S-álgebra separável.

Prova:

Seja $e = \sum_{i=1}^{n} a_i \otimes b_i \in A \otimes A^0$ um idempotente de separabilidade de A sobre R. Observemos que, da propriedade universal do produto tensorial sobre R e do fato de ser S uma R-álgebra, existe um homomorfismo de $A \otimes A^0$-módulos à esquerda $\alpha : A \otimes A^0 \to A \otimes_S A^0$, dada por $\alpha(a \otimes b) = a \otimes b \in A \otimes_S A^0$, para cada $a \otimes b \in A \otimes A^0$. Então, o elemento $e = \alpha(\sum_{i=1}^{n} a_i \otimes b_i)$ satisfaz a igualdade $\mu(e) = \sum_{i=1}^{n} a_i b_i = 1$ e, para cada $a \in A$,

$$(a \otimes 1)e = \alpha(\sum_{i=1}^{n} a a_i \otimes b_i) = \alpha(\sum_{i=1}^{n} a_i \otimes b_i a) = (1 \otimes a)e.$$

Logo, A é uma S-álgebra separável. □

O seguinte resultado é trivial:

Corolário 2.3:

Sejam A uma R-álgebra separável e S uma R-subálgebra do centro de A. Então A é uma S-álgebra separável.

Como caso particular do resultado acima, temos que toda R-álgebra separável é também uma álgebra separável sobre seu centro. Na verdade, é válido o teorema abaixo, cuja prova omitimos (ver Teorema 2.3 de [3])

Teorema 2.4:

Uma R-álgebra A é separável se e só se A é separável sobre seu centro $Z(A)$ e $Z(A)$ é separável sobre R.

Proposição 2.5:

Sejam A e B duas R-álgebras e $f : A \to B$ um epimorfismo de R-álgebras. Se A é R-separável então B é também separável sobre R .

Prova:

Se $e_A = \sum_{i=1}^{n} x_i \otimes y_i \in A^e$ é um idempotente de separabilidade da R-álgebra A , então o elemento

$e_B = \sum_{i=1}^{n} f(x_i) \otimes f(y_i) = (f \otimes f) e_A$ satisfaz $\sum_{i=1}^{n} f(x_i) f(y_i) =$

$= f(\sum_{i=1}^{n} x_i y_i) = 1$. Além disso, para cada $b \in B$, existe $a \in A$ tal que $f(a) = b$ e, portanto,

$$(1 \otimes b) e_B = (1 \otimes f(a)) (\sum_{i=1}^{n} f(x_i) \otimes f(y_i)) = \sum_{i=1}^{n} f(x_i) \otimes f(y_i) f(a) =$$

$$= (f \otimes f) (\sum_{i=1}^{n} x_i \otimes y_i a) = (f \otimes f) (\sum_{i=1}^{n} a x_i \otimes y_i) =$$

$$= \sum_{i=1}^{n} f(a) f(x_i) \otimes f(y_i) = (f(a) \otimes 1) e_B = (b \otimes 1) e_B \quad .$$

Logo, B é uma R-álgebra separável. □

Antes de provarmos a próxima propriedade, façamos algumas observações. Se R_1 e R_2 são anéis comutativos e A_1 é uma R_1-álgebra, então A_1 é também uma álgebra sobre $R_1 \oplus R_2$, se definimos a operação externa por $(r_1, r_2) . a_1 = r_1 . a_1$, para cada par $(r_1, r_2) \in R_1 \oplus R_2$ e para

cada $a_1 \in A_1$, como é fácil verificar. Analogamente, se A_2 , é uma R_2-álgebra, então, definindo uma operação externa por $(r_1,r_2).a_2 = r_2.a_2$, temos que A_2 é também uma álgebra sobre $R_1 \oplus R_2$. Portanto, podemos considerar a $R_1 \oplus R_2$-álgebra $A_1 \oplus A_2$.

É fácil verificar ainda, que a álgebra oposta $(A_1 \oplus A_2)^0$ é exatamente $A_1^0 \oplus A_2^0$. Então, pela distributividade do produto tensorial sobre $R_1 \oplus R_2$ em relação à soma direta, podemos escrever, pondo $R = R_1 \oplus R_2$,

$$(A_1 \oplus A_2) \otimes (A_1 \oplus A_2)^0 = (A_1 \oplus A_2) \otimes (A_1^0 \oplus A_2^0) \simeq A_1 \otimes (A_1^0 \oplus A_2^0) \oplus A_2 \otimes (A_1^0 \oplus A_2^0) \simeq$$

$$\simeq (A_1 \otimes A_1^0) \oplus (A_1 \otimes A_2^0) \oplus (A_2 \otimes A_1^0) \oplus (A_2 \otimes A_2^0)$$

Ainda, é fácil ver que existe um isomorfismo entre $A_1 \otimes A_1^0$ e $A_1 \otimes_{R_1} A_1^0 = A_1^e$ e que também $A_2 \otimes A_2^0$ é isomorfo a $A_2 \otimes_{R_2} A_2^0 = A_2^e$. Além disso, observemos que se $a_1 \otimes a_2$ é um elemento de $A_1 \otimes A_2^0$ então

$$a_1 \otimes a_2 = a_1.(1,0) \otimes a_2 = a_1 \otimes (1,0).a_2 = a_1 \otimes 0 = 0 \ ,$$

ou seja, $A_1 \otimes A_2^0 = 0$. Pela mesma razão, $A_1^0 \otimes A_2 = 0$. Portanto, podemos concluir que $(A_1 \oplus A_2)^e = (A_1 \oplus A_2) \otimes (A_1 \oplus A_2)^0 \simeq A_1^e \oplus A_2^e$, através da aplicação de $(A_1 \oplus A_2)^e$-módulos à esquerda $\rho : (A_1 \oplus A_2)^e \to A_1^e \oplus A_2^e$ dada por $\rho[(a_1,a_2) \otimes (a_1',a_2')] = ((a_1 \otimes a_1'),(a_2 \otimes a_2'))$ para cada elemento $(a_1,a_2) \otimes (a_1',a_2') \in (A_1 \oplus A_2)^e$, onde cada um dos tensores é considerado sobre $R = R_1 \oplus R_2$, R_1 e R_2 , respectivamente.

Estamos agora em condições de mostrar a seguinte

Proposição 2.6:

Sejam R_1 e R_2 anéis comutativos e A_1 e A_2 álgebras sobre R_1 e R_2, respectivamente. Então $A_1 \oplus A_2$ é uma R-álgebra separável se e só se A_1 e A_2 são separáveis sobre R_1 e R_2, respectivamente, onde $R = R_1 \oplus R_2$.

Prova:

Denotemos por μ_i o homomorfismo contração da R_i-álgebra A_i (i=1,2), e por μ o homomorfismo contração da $R_1 \oplus R_2$-álgebra $A_1 \oplus A_2$. Então, definindo a aplicação $\mu_1 \oplus \mu_2 : A_1^e \oplus A_2^e \to A_1 \oplus A_2$ por

$(\mu_1 \oplus \mu_2)(a_1 \otimes a_1', a_2 \otimes a_2') = (a_1 a_1', a_2 a_2')$, para cada par $(a_1 \otimes a_1', a_2 \otimes a_2') \in A_1^e \oplus A_2^e$, podemos observar que o seguinte diagrama de $(A_1 \oplus A_2)^e$-módulos à esquerda é comutativo:

$$\begin{array}{ccc} (A_1 \oplus A_2) \otimes (A_1 \oplus A_2)^0 & \xrightarrow{\rho} & (A_1 \otimes_{R_1} A_1^0) \oplus (A_2 \otimes_{R_2} A_2^0) \\ \Big\downarrow \mu & \swarrow \mu_1 + \mu_2 & \\ A_1 \oplus A_2 & & \end{array}$$

De fato, para cada $(a_1,a_2) \otimes (a_1',a_2') \in (A_1 \oplus A_2)^e$, $[(\mu_1 \oplus \mu_2) \circ \rho][(a_1,a_2) \otimes (a_1',a_2')] = (\mu_1 \oplus \mu_2)(a_1 \otimes a_1', a_2 \otimes a_2') =$

$$= (a_1a_1' , a_2a_2') = (a_1,a_2)(a_1' , a_2') =$$

$$= \mu[(a_1,a_2) \otimes (a_1' , a_2')] .$$

Suponhamos então que A_1 e A_2 são separáveis sobre R_1 e R_2, respectivamente. Então sabemos que existem homomorfismos $\psi_1 : A_1 \to A_1^e$ e $\psi_2 : A_2 \to A_2^e$ tais que $\mu_1\psi_1 = id_{A_1}$ e $\mu_2\psi_2 = id_{A_2}$. Portanto, a aplicação $\psi_1 \oplus \psi_2 : A_1 \oplus A_2 \to (A_1 \oplus A_2)^e$, dada por $(\psi_1 \oplus \psi_2)(a_1,a_2) = (\psi_1(a_1),\psi_2(a_2))$ para cada $(a_1,a_2) \in A_1 \oplus A_2$ verifica $\mu \circ \phi^{-1} \circ (\psi_1 \oplus \psi_2) = id_{A_1 \oplus A_2}$. Assim, pondo $\psi = \rho^{-1} \circ (\psi_1 \oplus \psi_2)$, temos que ψ é um homomorfismo de $(A_1 \oplus A_2)^e$-módulos à esquerda e $\mu\psi = id_{A_1 \oplus A_2}$. Ou seja, $A_1 \oplus A_2$ é uma álgebra separável sobre $R_1 \oplus R_2$.

Reciprocamente, se $A_1 \oplus A_2$ é separável sobre $R_1 \oplus R_2$, então sabemos que existe um homomorfismo $\psi : A_1 \oplus A_2 \to (A_1 \oplus A_2)^e$ tal que $\mu\psi = id_{A_1 \oplus A_2}$. Mostremos que, neste caso, A_1 é R_1-separável. Observemos que através da aplicação $i_1 : A_1 \to A_1 \oplus A_2$ dada por $i_1(a_1) = (a_1,0)$, para cada $a_1 \in A_1$, podemos considerar A_1 uma subálgebra de $A_1 \oplus A_2$. Além disso, se π_1 representa a projeção de $A_1^e \oplus A_2^e$ no primeiro somando A_1^e, então é fácil verificar que $\mu_1 \circ (\pi_1 \circ \rho \circ \psi \circ i_1) = id_{A_1}$. Como a composição $\pi_1 \circ \rho \circ \psi \circ i_1$

é um homomorfismo de A_1^e-módulos à esquerda, temos que A_1 é uma R_1-álgebra separável.

De maneira análoga, mostra-se que A_2 é separável sobre R_2 . □

Corolário 2.7:

Sejam A_1 e A_2 álgebras separáveis sobre R . Então $A_1 \oplus A_2$ é uma R-álgebra separável.

Prova:

Do resultado anterior temos que $A_1 \oplus A_2$ é separável sobre $R \oplus R$. Mas, pelo exemplo 1 de álgebras separáveis, $R \oplus R$ é uma R-álgebra separável. Logo, pela transitividade da separabilidade, temos que $A_1 \oplus A_2$ é uma álgebra separável sobre R . □

Se A é uma R-álgebra, então todo A-módulo M torna-se um R-módulo, se definimos a operação externa por $r.m = (r.1_A).m$, para cada $r \in R$, $m \in M$. Com referência a esta estrutura, mostramos a seguinte

Proposição 2.8:

Se A é uma R-álgebra separável então todo A-módulo M que é projetivo como R-módulo é também projetivo como A-módulo.

Prova:

Seja $0 \to L \to N \xrightarrow{\eta} M \to 0$ uma seqüência exata de A-módulos. Então, podemos considerá-la uma seqüência exata de R-módulos e sabemos que, como tal, esta seqüência cinde, já que M é um R-módulo projetivo. Logo, existe um homomorfismo de R-módulos $\psi : M \to N$ tal que $\eta\psi = id_M$. Queremos modificar convenientemente esta aplicação ψ a fim de que seja preservada esta propriedade, mas que a nova aplicação seja também um homomorfismo de A-módulos.

Para tal, observemos antes que, sendo A uma R-álgebra e M e N dois A-módulos à esquerda, então o conjunto $Hom_R(M,N)$ dos homomrofismos de R-módulos de M em N é um A^e-módulo à esquerda, cuja operação externa é dada por $[(a\otimes a').f](m) = a.f(a'.m)$, para cada $(a\otimes a') \in A^e$, $m \in M$ e para cada homomorfismo $f \in Hom_R(M,N)$.

Seja agora $e = \sum_{i=1}^{n} x_i \otimes y_i \in A^e$ um idempotente de separabilidade da R-álgebra A. Definimos $\psi' = e.\psi$, isto é, para todo $m \in M$, $\psi'(m) = (e.\psi)(m) = \sum_{i=1}^{n} x_i.\psi(y_i.m)$.

Sendo η um homomorfismo de A-módulos e como $\mu(e) = 1$, para cada $m \in M$, temos

$$(\eta\psi')(m) = \eta(\sum_{i=1}^{n} x_i.\psi(y_i.m)) = \sum_{i=1}^{n} x_i.\eta\psi(y_i.m) = (\sum_{i=1}^{n} x_i y_i).m = m .$$

Portanto, $\eta\psi = id_M$.

Logo, resta-nos apenas mostrar que ψ' é um A-homomorfismo. De fato, considerando que cada $a \in A$ satis

faz $(1\otimes a - a\otimes 1)e = 0$, podemos escrever:

$$(1\otimes a - a\otimes 1).\psi' = (1\otimes a - a\otimes 1).(e.\psi) = \left[(1\otimes a - a\otimes 1)e\right].\psi = 0 \ ,$$

e, portanto, para cada $m \in M$,

$$\left[(1\otimes a).\psi'\right](m) = \left[(a\otimes 1).\psi'\right](m) \ , \text{ ou ainda,}$$

$\psi'(a.m) = a.\psi'(m)$, para todo $m \in M$, o que completa a prova. □

Corolário 2.9:

Se A é uma R-álgebra separável que é projetiva como R-módulo então a álgebra envolvente A^e é um A-módulo projetivo.

Prova:

É óbvio que a R-álgebra oposta A^0 é também um R-módulo projetivo. Então, por I.2.4 , a álgebra envolvente A^e é um R-módulo projetivo. Logo, a proposição acima nos garante que A^e é um A-módulo projetivo. □

Utilizando este corolário, estamos em condições de mostrar o seguinte resultado sobre as álgebras separáveis que são projetivas como módulos sobre o anel base:

Proposição 2.10: (Villamayor e Zelinsky)

Seja A uma R-álgebra. Se A é separável sobre R e é um R-módulo projetivo, então A é um R-módulo finitamente gerado.

Prova:

Seja I um conjunto de índices e sejam $\{a_i\}_{i\in I}\subset A$ e $\{f_i\}_{i\in I}\subset \mathrm{Hom}_R(A,R)$ coordenadas projetivas do R-módulo A. É fácil ver que os subconjuntos $\{1\otimes a_i\}_{i\in I}\subset A^e$ e $\{(id\otimes f_i)\}_{i\in I}\subset \mathrm{Hom}_A(A^e,A)$ são coordenadas projetivas do A-módulo projetivo A^e. Além disso, sabemos que se tal conjunto de índices I puder ser escolhido finito, então A é um R-módulo finitamente gerado. De fato, vejamos que isto acontece.

Seja $e=\sum_{j=1}^{n} x_j\otimes y_j\in A^e$ um idempotente de separabilidade da R-álgebra separável A. Escolhemos I' o subconjunto formado pelos índices $i\in I$ tais que $f_i(y_j)\neq 0$, para algum $j\in\{1,2,\ldots,n\}$. Então é claro que I' é um conjunto finito, já que $f_r(y_j)$ é nulo, salvo um conjunto finito de índices $r\in I$. Além disso, para cada elemento $a\in A$ e para cada índice $i\in I$, $(id\otimes f_i)\left[(1\otimes a)e\right]=(id\otimes f_i)\left[(a\otimes 1)e\right]=$

$=\sum_{i=1}^{n} a x_j\otimes f_i(y_j)$, que é nulo sempre que $i\notin I'$.

Finalmente, para cada elemento a da R-álgebra A, podemos observar que

$$a=\mu\left[(1\otimes a)e\right]=\mu\{\sum_{i\in I}(id\otimes f_i)\left[(1\otimes a)e\right](1\otimes a_i)\}=$$

$$=\mu\Big(\sum_{i\in I'}\sum_{j=1}^{n} x_j\otimes f_i(y_j a)a_i\Big)=\sum_{i\in I'}\sum_{j=1}^{n} f_i(y_j a)x_j a_i.$$

Portanto, o R-módulo A é gerado pelos elementos $x_j a_i$, onde

i e j variam em conjuntos finitos; logo, A é um R-módulo finitamente gerado. □

Vamos agora dar uma caracterização da separabilidade que envolve o functor $(\ )^A$ definido no capítulo I. Utilizando este argumento, mostraremos ainda mais algumas propriedades das álgebras separáveis.

Proposição 2.11:

Uma R-álgebra A é separável se e só se o functor $(\ )^A$ é exato à direita.

Prova:

Basta-nos mostrar que se $M \xrightarrow{f} N \to 0$ é uma seqüência exata de A/R-módulos bilaterais então a seqüência de R-módulos $M^A \xrightarrow{f|} N^A \to 0$ é também exata, onde $f|$ representa a restrição de f ao R-submódulo M^A. Pela definição, A é R-separável se e só se o functor $\mathrm{Hom}_{A^e}(A,-)$ é exato. Então a proposição é conseqüência imediata de I.3.3. □

Seja A uma R-álgebra. Denotemos por $(0 : J)$ o anulador à direita em A^e do núcleo J, isto é,

$$(0 : J) = \{\sum_{i=1}^{n} a_i \otimes b_i \in A^e \mid J(\sum_{i=1}^{n} a_i \otimes b_i) = 0\} .$$

Então é válida a seguinte

Proposição 2.12:

Existe um isomorfismo de R-módulos entre

$(0 : J)$ e $\mathrm{Hom}_{A^e}(A, A^e)$. Além disso, se A é separável sobre R , então $\mu(0 : J) = Z(A)$, ($Z(A)$ denota o centro do anel A .)

Prova:

Observemos que um elemento $\sum_{i=1}^{n} a_i \otimes a_i'$ está no R-submódulo $(A^e)^A$ se e só se, para cada $a \in A$, $a.(\sum_{i=1}^{n} a_i \otimes a_i') = (\sum_{i=1}^{n} a_i \otimes a_i').a$, ou seja, para cada gerador $a \otimes 1 - 1 \otimes a \in J$, $(a \otimes 1 - 1 \otimes a)(\sum_{i=1}^{n} a_i \otimes a_i') = 0$. Assim, temos que $(A^e)^A = (0 : J)$, e, portanto, os R-módulos $(0 : J)$ e $\mathrm{Hom}_{A^e}(A, A^e)$ são isomorfos, por I.3.2.

Suponhamos agora que A é uma R-álgebra separável. Então o functor $(\ )^A$ é um functor exato. Logo, a seqüência $(A^e)^A \xrightarrow{\mu|} A^A \to 0$ é também exata. Mas como $(A^e)^A = (0 : J)$ e $A^A = Z(A)$, temos que $\mu|[(0 : J)] = Z(A)$, ou seja, $\mu(0 : J) = Z(A)$. □

Estamos agora em condições de mostrar mais algumas propriedades das álgebras separáveis.

Proposição 2.13:

Sejam S_1 e S_2 duas R-álgebras comutativas, e A_1 e A_2 álgebras separáveis sobre S_1 e S_2 , respectivamente. Se $A_1 \otimes A_2$ não é o anel nulo, então é uma álgebra separável sobre $S_1 \otimes S_2$.

Prova:

Suponhamos $A_1 \otimes A_2 \neq 0$. Então é fácil ver que este anel é um $S_1 \otimes S_2$-módulo, cujo produto externo é dado por distributividade e por $(s_1 \otimes s_2).(a_1 \otimes a_2) = s_1.a_1 \otimes s_2.a_2$, para todo $s_1 \otimes s_2 \in S_1 \otimes S_2$ e para todo $a_1 \otimes a_2 \in A_1 \otimes A_2$. Mais ainda, por serem A_1 e A_2 álgebras sobre S_1 e S_2 , respectivamente, também $A_1 \otimes A_2$ é uma $S_1 \otimes S_2$-álgebra.

Suponhamos que A_1 e A_2 são separáveis sobre S_1 e S_2 , respectivamente, e mostremos que $A_1 \otimes A_2$ é uma $S_1 \otimes S_2$-álgebra separável, provando que o functor $(\ )^{A_1 \otimes A_2}$ é exato à direita.

Seja então $M \xrightarrow{f} N \to 0$ uma seqüência exata de A/S-módulos bilaterais, onde $A = A_1 \otimes A_2$ e $S = S_1 \otimes S_2$. É fácil ver que, através das igualdades $a_1.m = (a_1 \otimes 1).m$ e $m.a_1 = m.(a_1 \otimes 1)$, para cada $a_1 \in A_1$, $m \in M$, temos induzidas em M estruturas de A_1-módulo à esquerda e à direita, respectivamente. Além disso, tais estruturas comutam, já que M é um A/S-módulo bilateral.

Para concluirmos que M é um A_1/S_1-módulo bilateral, resta-nos mostrar que as estruturas de S_1-módulos induzidas coincidem. Mas observemos que, para cada $s_1 \in S_1$, $m \in M$,

$s_1.m = (s_1.1).m = (s_1.1 \otimes 1).m = m.(s_1.1 \otimes 1) = m.s_1$. Portanto,

como podemos fazer o mesmo raciocínio para o A/S-módulo bilateral N, concluimos que M e N são A_1/S_1-módulos bilaterais. Como A_1 é S_1-álgebra separável, a seqüência de A_1/S_1-módulos bilaterais

$$M^{A_1} \xrightarrow{f|} N^{A_1} \to 0 \quad \text{é exata} .$$

De maneira análoga, podemos definir em M estruturas de A_2-módulos à direita e à esquerda através das igualdades $m.a_2 = m.(1 \otimes a_2)$ e $a_2.m = (1 \otimes a_2).m$, para cada $m \in M$, $a_2 \in A_2$, e podemos também mostrar que M é um A_2/S_2-módulo bilateral.

Observemos agora que as estruturas de módulo sobre A_1 e A_2 em M comutam, ou seja, para cada $a_1 \in A_1$, $a_2 \in A_2$, $m \in M$, $a_1.(a_2.m) = a_2.(a_1.m)$, como é fácil verificar. Utilizando este fato, podemos concluir que M^{A_1} é um A_2-submódulo à esquerda de M. De fato, para cada $m \in M^{A_1}$, $a_1 \in A_1$, $a_2 \in A_2$,

$$a_1.(a_2.m) = a_2.(a_1.m) = a_2.(m.a_1) = (1 \otimes a_2).[m(a_1 \otimes 1)] =$$

$$= [(1 \otimes a_2).m].(a_1 \otimes 1) = (a_2.m).a_1 \text{, ou seja, } a_2.m \in M^{A_1} .$$

Analogamente, M^{A_1} é um A_2-submódulo à direita de M. Ainda, como M é um A_2/S_2-módulo bilateral, é óbvio que o A_2-submódulo M^{A_1} também o é.

Portanto, como podemos fazer o mesmo raciocínio para o A_1/S_1-módulo bilateral N, concluimos que a seqüência $M^{A_1} \xrightarrow{f|} N^{A_1} \to 0$ é uma seqüência exata de A_2/S_2-módulos bilaterais. Logo, como A_2 é uma álgebra separável sobre S_2, temos que a seqüência $(M^{A_1})^{A_2} \xrightarrow{f|} (N^{A_1})^{A_2} \to 0$ é uma seqüência exata.

Mostremos, finalmente, que $(M^{A_1})^{A_2} = M^{A_1 \otimes A_2}$. De fato, se $m \in (M^{A_1})^{A_2}$ então, para todo elemento $a_1 \otimes a_2 \in A_1 \otimes A_2$,

$$(a_1 \otimes a_2).m = a_1.(a_2.m) = (m.a_2).a_1 = m.(a_1 \otimes a_2),$$

ou seja, $(M^{A_1})^{A_2} \subset M^{A_1 \otimes A_2}$. Reciprocamente, se $m \in M^{A_1 \otimes A_2}$, então, para cada $a_1 \in A_1$, $a_1.m = (a_1 \otimes 1).m = m.(a_1 \otimes 1) = m.a_1$, e, de maneira análoga, $a_2.m = m.a_2$, para cada $a_2 \in A_2$. Logo, $M^{A_1 \otimes A_2} \subset (M^{A_1})^{A_2}$.

Uma vez que o diagrama

$$\begin{array}{ccccc} (M^{A_1})^{A_2} & \xrightarrow{f|} & (N^{A_1})^{A_2} & \to & 0 \\ \downarrow & & \downarrow & & \\ M^{A_1 \otimes A_2} & \xrightarrow{f|} & N^{A_1 \otimes A_2} & & \end{array}$$

é comutativo, segue-se que a aplicação $f| : M^{A_1 \otimes A_2} \to N^{A_1 \otimes A_2}$ é sobrejetora, o que completa a prova. □

Corolário 2.14:

Sejam A uma R-álgebra separável e S uma álgebra comutativa sobre R . Então $A \otimes S$ é uma S-álgebra separável.

Prova:

Pondo no resultado anterior $A_1 = A$, $A_2 = S_2 = S$, e $S_1 = R$, conclui-se que $A \otimes S$ é uma álgebra separável sobre $R \otimes S \simeq S$.

Poderíamos agora nos perguntar sobre a validade de uma recíproca para a última proposição. Podemos provar a seguinte

Proposição 2.15:

Sejam S_1 e S_2 álgebras comutativas sobre R e A_1 e A_2 álgebras sobre S_1 e S_2 , respectivamente, tais que $A_1 \otimes A_2$ é uma $S_1 \otimes S_2$-álgebra separável. Se R é um R-somando direto do R-módulo A_2 , então A_1 é uma S_1-álgebra separável.

Prova:

Sejam M e N dois A_1/S_1-módulos bilaterais, e seja $f : M \to N$ um epimorfismo.

Observemos inicialmente que $M \otimes A_2$ é um $A_1 \otimes A_2/S_1 \otimes S_2$-módulo bilateral, como é fácil verificar. Analogamente, $N \otimes A_2$ é também um $A_1 \otimes A_2/S_1 \times S_2$-módulo bilateral

e a seqüência $M \otimes A_2 \xrightarrow{f \otimes id} N \otimes A_2 \to 0$ é uma seqüência exata de $A_1 \otimes A_2/S_1 \otimes S_2$-módulos bilaterais. Portanto, como $A_1 \otimes A_2$ é separável sobre $S_1 \otimes S_2$, a seqüência

$$(M \otimes A_2)^{A_1 \otimes A_2} \xrightarrow{f \otimes id|} (N \otimes A_2)^{A_1 \otimes A_2} \to 0 \quad \text{é}$$

também exata.

Por hipótese, $A_2 = R \oplus L$, para algum R-submódulo L de A_2. Então

$M \otimes A_2 = M \otimes (R \oplus L) \simeq (M \otimes R) \oplus (M \otimes L) \simeq M \oplus (M \otimes L)$, ou seja, M é um somando direto de $M \otimes A_2$ como A_1/S_1-módulo bilateral.

É fácil ver que $M \otimes A_2$ é também um A_1/S_1-módulo bilateral. Então considerando a projeção canônica $\pi_M : M \otimes A_2 \to M$ entre A_1/S_1-módulos bilaterais, temos que a imagem do $S_1 \otimes S_2$-submódulo $(M \otimes A_2)^{A_1 \otimes A_2}$ por este epimorfismo é exatamente M^{A_1}.

Fazendo o mesmo raciocínio para N, podemos considerar o seguinte diagrama comutativo:

$$\begin{array}{ccccc} (M \otimes A_2)^{A_1 \otimes A_2} & \xrightarrow{f \otimes id} & (N \otimes A_2)^{A_1 \otimes A_2} & \to & 0 \\ \downarrow{\scriptstyle \pi_M} & & \downarrow{\scriptstyle \pi_N} & & \\ M^{A_1} & \xrightarrow{f|} & N^{A_1} & & \end{array}$$

Portanto, a seqüência $M^{A_1} \xrightarrow{f|} N^{A_1} \to 0$ é exata, ou seja, A_1 é uma S_1-álgebra separável. □

Levando em conta a proposição acima, torna-se óbvio o seguinte

Corolário 2.16:

Sejam A_1 e A_2 duas R-álgebras tais que $A_1 \otimes A_2$ é uma R-álgebra separável. Se R é um somando direto de A_2 como R-módulo, então A_1 é separável sobre R .

O próximo resultado tenta estabelecer uma recíproca para 2.14:

Corolário 2.17:

Sejam S uma R-álgebra comutativa que contém R como R-somando direto e A uma R-álgebra tal que $A \otimes S$ é uma S-álgebra separável. Então A é separável sobre R .

Além disso, se $R.1_A \otimes S$ é o centro do anel $A \otimes S$, então $R.1_A$ é exatamente o centro de A .

Prova:

Para mostrar que A é R-separável, basta-nos aplicar a proposição anterior, pondo $A_1 = A$, $A_2 = S = S_2$ e $S_1 = R$.

Suponhamos então que o centro $Z(A \otimes S)$ é $1 \otimes S$. Logo, podemos escrever

$(A \otimes S)^{A \otimes S} = Z(A \otimes S) = R.1_A \otimes S$. Agora, por raciocínio análogo ao desenvolvido na última proposição, pode-

mos concluir que A é um somando direto de $A \otimes S$, já que S contém R como R-somando direto. Ainda, considerando a projeção canônica $\pi : A \otimes S \to A$, sabemos que o submódulo $(A \otimes S)^{A \otimes S}$ é projetado em $A^A = Z(A)$. Logo, $Z(A) = \pi\left[(A \otimes S)^{A \otimes S}\right] = \pi(R.1 \otimes S) = R.1_A$, o que completa a prova. □

Verifiquemos agora o que acontece quando consideramos quocientes de álgebras separáveis ou álgebras sobre quocientes do anel base R.

Proposição 2.18:

Sejam A uma R-álgebra separável e $\mathcal{A}$ um ideal do anel A. Então o quociente $A/_{\mathcal{A}}$ é também uma R-álgebra separável.

Prova:

É fácil ver que $A/_{\mathcal{A}}$ é uma R-álgebra, onde a operação externa de R-módulo é dada de maneira natural por $r.(a + \mathcal{A}) = r.a + \mathcal{A}$, para todo $a \in A$, $r \in R$. Então basta-nos considerar o epimorfismo de R-álgebras $\pi : A \to A/_{\mathcal{A}}$ e aplicar 2.5. □

Suponhamos agora que A é uma R-álgebra e I um ideal de R contido no anulador de A, i.e., $I.1_A = 0$. Então é claro que o quociente $R/_I$ é ainda um anel comutativo com unidade. Definindo de maneira natural uma operação

externa por $(r+I).a = r.a$, para toda classe $r+I \in R/_I$ e todo elemento $a \in A$, temos que A é um $R/_I$-módulo. Então é claro que A é uma $R/_I$-álgebra.

Ainda utilizando a propriedade universal do produto tensorial, é fácil mostrar que $A \otimes A^0$ é isomorfo ao A-módulo bilateral $A \otimes_{R/_I} A^0$.

Nestas condições, temos a seguinte

Proposição 2.19:

Sejam A uma R-álgebra e I um ideal de R contido no anulador $An_R(A)$ de A . Então A é uma R-álgebra separável se e só se A é separável sobre $R/_I$.

Prova:

É imediata, considerando 1.2, item (v). □

Proposição 2.20:

Sejam A uma R-álgebra separável e A um ideal de A . Então o quociente $A/_A$ é uma álgebra separável sobre $R.1_A/_{(R.1_A \cap A)}$, e o centro do anel $A/_A$ é $(Z(A)+A)/_A$.

Prova:

Já sabemos que o quociente $A/_A$ é uma R-álgebra separável. É fácil verificar que $R.1_A$ é um anel

comutativo com unidade e que $A/_A$ é uma $R.1_A$-álgebra. Ainda, $R.1_A \cap A$ é um ideal de $R.1_A$.

Logo, por 2.2, concluimos que $A/_A$ é uma R.1-álgebra separável e portanto, pela proposição anterior, $A/_A$ é uma álgebra separável sobre $R.1/_{(R.1 \cap A)}$.

Resta-nos então mostrar a igualdade $Z(A/_A) = (Z(A) + A)/_A$. Denotando por π a projeção canônica de A no anel quociente $A/_A$, temos que a seqüência $A \xrightarrow{\pi} A/_A \to 0$ é uma seqüência exata de A/R-módulos bilaterais. Então, como A é separável sobre R , a seqüência de R-submódulos $A^A \xrightarrow{\pi|} (A/_A)^A \to 0$ é também exata.

Observemos agora que uma classe $a + A$ é um elemento de $(A/_A)^A$ se e só se $ab + A = ba + A$, para todo $b \in A$, ou ainda, $(a + A)(b + A) = (b + A)(a + A)$. Portanto,

$$Z(A/_A) = (A/_A)^A = \pi(A^A) = \pi(Z(A)) = \pi(Z(A) + A) = \frac{Z(A) + A}{A} ,$$

o que completa a prova. □

Antes de finalizarmos esta seção, introduzimos um conceito que será bastante utilizado nos próximos capítulos.

Sejam A e B dois anéis comutativos e f,g dois homomorfismos de anéis de A em B . Dizemos que f e g são homomorfismos FORTEMENTE DISTINTOS se, para cada idem

potente não nulo $e \in B$, existe um elemento $a \in A$ tal que $f(a)e \neq g(a)e$. É óbvio que dois homomorfismos fortemente distintos são diferentes e que a recíproca é válida quando B não possui idempotentes próprios.

Proposição 2.21:

Sejam A uma R-álgebra comutativa e separável, e $f : A \to R$ um homomorfismo de R-álgebras. Então existe um único idempotente $\nu \in A$ tal que $f(\nu) = 1$ e $f(a).\nu = a\nu$, para cada $a \in A$. Além disso, se $f_1,\ldots,f_n$ são homomorfismos de R-álgebras de A em R dois a dois fortemente distintos, então os respectivos idempotentes $\nu_1,\ldots,\nu_n \in A$ são dois a dois ortogonais e $f_i(\nu_j) = \delta_{ij}$, para cada $i,j \in \{1,2,\ldots,n\}$. (δ_{ij} representa a função delta de Kronecker, i.e., $\delta_{ij} = 0$, se $i \neq j$ e $\delta_{ij} = 1_R$, se $i = j$).

Prova:

Seja $e = \sum_{j=1}^{m} x_j \otimes y_j \in A^e$ um idempotente de separabilidade de A sobre R. Definamos $\nu = \sum_{j=1}^{m} f(x_j).y_j \in A$, e mostremos que tal elemento é o idempotente procurado, em relação ao homomorfismo f. De fato, podemos observar que, sendo f um homomorfismo de R-álgebras, $f(\nu) = \sum_{j=1}^{m} f(x_j)f(y_j) = f(\sum_{j=1}^{m} x_jy_j) = 1$. Além disso, conside

rando o homomorfismo $f \otimes id_A$ de $A \otimes A$ em $R \otimes A \simeq A$ para cada $a \in A$.

$\sum_{j=1}^{m} f(x_j) \otimes a y_j = (f \otimes id_A)[(1 \otimes a)e] = (f \otimes id_A)[(a \otimes 1)e] =$

$= \sum_{j=1}^{m} f(a x_j) \otimes y_j$, donde segue-se que $\sum_{j=1}^{m} f(x_j).a y_j = \sum_{j=1}^{m} f(ax_j).y_j$

Portanto, $f(a).\nu = f(a) \sum_{j=1}^{m} f(x_j).y_j = \sum_{j=1}^{m} f(ax_j).y_j = \sum_{j=1}^{m} f(x_j).ay_j = a\nu$

Podemos observar ainda que, pondo $a = \nu$ na expressão acima, $\nu = f(\nu).\nu = \nu^2$. Ou seja, o elemento ν definido anteriormente é um idempotente.

Finalmente, se $\nu' \in A$ é um idempotente que também satisfaz $f(\nu') = 1$ e $f(a).\nu' = a\nu'$, para cada $a \in A$, então $\nu = f(\nu').\nu = \nu'\nu = \nu\nu' = f(\nu).\nu' = \nu'$, o que completa a primeira parte da prova.

Consideremos agora os homomorfismos $f_1,\ldots,f_n$ dados na hipótese, e sejam $\nu_1,\ldots,\nu_n \in A$ os idempotentes por eles determinados. É fácil verificar que, para cada $i,j \in \{1,2,\ldots,n\}$, $f_i(\nu_j)$ é um idempotente de R . Ainda, para cada $a \in A$,

$f_i(a) f_i(\nu_j) = f_i(a\nu_j) = f_i(f_j(a).\nu_j) = f_j(a) f_i(\nu_j)$. Portanto, como f_i e f_j são homomorfismos fortemente distintos, vem que $f_i(\nu_j) = 0$, se $i \neq j$. Assim, $f_i(\nu_j) = \delta_{ij}$, para cada $i,j \in \{1,2,\ldots,n\}$.

Além disso, como $\nu_i \nu_j = f_j(\nu_i).\nu_j = \delta_{ij}.\nu_j$, os idempotentes $\nu_1,\ldots,\nu_n$ são dois a dois ortogonais, o que completa a prova. □

§ 3 . ÁLGEBRAS SEPARÁVEIS SOBRE CORPOS

Nesta seção, mostramos a relação existente entre o conceito de álgebra separável sobre um anel comutativo com unidade e o de (corpo) extensão separável de um corpo, conceito este apresentado no Capítulo I. Mais precisamente, vamos mostrar que se S e R são corpos, então S é uma R-álgebra separável se e só se S é uma extensão finita e separável de R (no sentido apresentado no capítulo I).

Observemos que, da proposição 2.10, é claro que se R é um corpo e S é uma R-álgebra separável então S é um espaço vetorial de dimensão finita sobre R. Ainda, neste caso, é fácil ver que S é um R-módulo fiel e que o conjunto $R_0 = \{r.1_S \mid r \in R\}$ é um subconjunto do centro do anel S e um corpo isomorfo a R. Logo, podemos supor $R \subset S$.

Vemos então que a noção de R-álgebra separável só pode generalizar o conceito de extensão finita e separável de corpos. Por esta razão, nesta seção trabalharemos apenas com extensões finitas de corpos. Para evitar qualquer confusão, quando S e R forem corpos tais que S é uma extensão finita e separável de R (no sentido do capítulo I), diremos apenas que S é uma EXTENSÃO CLASSICAMENTE SEPARÁVEL DE R.

Apresentamos inicialmente o conceito de extensão primitiva de um corpo, a fim de mostrarmos uma propriedade que nos será útil sobre as extensões classicamen

te separáveis de um corpo K, para podermos, a seguir, abordar o problema principal desta seção.

Sejam K um corpo e E uma extensão de K. Um elemento $\alpha \in E$ é dito um ELEMENTO PRIMITIVO SOBRE K se $E = K(\alpha)$. Neste caso, o corpo E é denominado uma EXTENSÃO PRIMITIVA DE K. Queremos mostrar que toda extensão classicamente separável de um corpo K é na verdade uma extensão primitiva e separável de K. Para tal, precisamos antes fazer algumas observações.

Omitimos aqui a prova do resultado abaixo, mas ela pode ser encontrada em [10].

Lema 3.1:

Seja K um corpo e G um subgrupo finito do grupo multiplicativo $K - \{0\}$. Então G é um grupo cíclico.

Nos resultados que seguem, E e K denotam dois corpos (comutativos) quaisquer.

Proposição 3.2:

Seja E uma extensão finita de K. Então E é uma extensão primitiva de K se e só se existe um número finito de corpos intermediários.

Prova:

Suponhamos $n = [E : K]$. Se $E = K(\alpha)$, então $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ é um conjunto linearmente dependente e,

portanto, existe um polinômio $f(X) \in K[X]$ tal que $f(\alpha) = 0$. Então, se F é um corpo intermediário (i.e., $K \subset F \subset E$), temos que $E = K(\alpha) \subset F(\alpha) \subset E(\alpha) = E$, ou seja, $F(\alpha) = E$. Além disso, $f(X) \in F[X]$. Seja $g(X) \in F[X]$ um fator irredutível de $f(X)$ que tem α como raiz. Logo, é claro que α é um elemento algébrico sobre F cujo polinômio minimal é $g(X)$, e $[E : F] = [F(\alpha) : F] = \partial g$. Seja F' o corpo obtido de K pela adjunção de todos os coeficientes do polinômio $g(X)$. Então $K \subset F' \subset F$ e portanto $E = K(\alpha) \subset F'(\alpha) \subset F(\alpha) = E$.

Sendo F' um corpo intermediário entre K e E e sendo E de dimensão finita sobre K, temos que E é uma extensão finita de F'. Ainda, é fácil ver que $g(X)$ é um polinômio irredutível em $F'[X]$. Logo, $g(X)$ é também o polinômio minimal de α sobre F'. Mas então $[E : F'] = [F'(\alpha) : F'] = \partial g = [E : F] = [E : F'][F' : F]$, donde segue-se que $[F' : F] = 1$. Logo, $F' = F$, ou seja o corpo intermediário F está univocamente determinado pelo polinômio $g(X)$, que é um fator irredutível de $f(X)$ em $F[X]$. Como o número de tais fatores irredutíveis é finito, concluimos que existe um número finito de corpos intermediários.

Reciprocamente, suponhamos que existe um número finito de corpos intermediários entre E e K. Se K é um corpo finito, então é fácil ver que E é também finito, já que $[E : K] = n$. Assim, temos que $E - \{0\}$ é um grupo multiplicativo finito e, portanto, pelo lema anterior, $E - \{0\}$ é um grupo cíclico. Se α é um gerador de $E - \{0\}$, então é claro que $E = K(\alpha)$.

Suponhamos agora que K é um corpo infinito. Como, por hipótese, $[E : K] = n$, vemos que, se $\{\alpha_1,\ldots,\alpha_n\}$ é uma base para o espaço vetorial E sobre K, é claro que $E = K(\alpha_1,\ldots,\alpha_n)$. Mostremos que, neste caso, E é uma extensão primitiva de K.

De fato, se $\alpha,\beta \in E$, consideremos $\gamma = \alpha + a\beta$, onde $a \in K$ é um elemento a ser determinado, a fim de que seja satisfeita a condição $K(\alpha,\beta) = K(\gamma)$. Mas como $\gamma \in E$, é imediato que $K \subset K(\gamma) \subset E$ e portanto, variando o valor de $a \in K$, obtemos corpos intermediários; como tais corpos são em número finito existem $a_1, a_2 \in K$, com $a_1 \neq a_2$ e tais que se $\gamma_1 = \alpha + a_1\beta$ e $\gamma_2 = \alpha + a_2\beta$ então $K(\gamma_1) = K(\gamma_2)$, ou seja, $\gamma_1 - \gamma_2 = (a_1 - a_2)\beta \in K(\gamma_1)$. Então β e $\alpha = \gamma_1 - a_1\beta$ são elementos de $K(\gamma_1)$, ou seja, $K(\alpha,\beta) \subset K(\gamma_1)$. Assim, $K(\alpha,\beta) = K(\gamma_1)$.

Aplicando o Lema de Zorn, pode-se mostrar que existe um corpo intermediário da forma $K(\theta)$ que é maximal para a propriedade de ser um corpo intermediário entre E e K e uma extensão primitiva de K. Mostremos então que $E = K(\theta)$. De fato, se $\delta \in E - K(\theta)$, então é claro que $K(\theta,\delta)$ é um corpo intermediário entre E e K. Assim, pelo raciocínio feito no parágrafo anterior, sabemos que é possível encontrar $\gamma \in E$ tal que $K(\gamma) = K(\theta,\delta) \supset K(\theta)$. Mas pelo caráter maximal de $K(\theta)$, temos $K(\gamma) = K(\theta)$, ou seja, $\delta \in K(\theta)$, uma contradição. Logo, $E = K(\theta)$, ou seja, E é uma extensão primitiva de K. □

Estamos agora em condições de mostrar a seguinte propriedade das extensões finitas e separáveis de um corpo:

Teorema 3.3 (Teorema do Elemento Primitivo)

Seja E uma extensão finita de K da forma $E = K(\alpha_1,\ldots,\alpha_n)$, onde $\alpha_1,\ldots,\alpha_n$, são elementos separáveis sobre K. Então existe um elemento $\theta \in E$ que é primitivo sobre K, ou seja, $E = K(\theta)$.

Prova:

Sejam $f_1(X),\ldots,f_n(X) \in K[X]$ os polinômios minimais de $\alpha_1,\ldots,\alpha_n$, respectivamente, e sejam $f_1(X),\ldots,f_r(X)$ $(r \leq n)$ todos os polinômios minimais distintos. Então todas as raízes de $f_1(X),\ldots,f_r(X)$ são distintas. De fato, se α é raiz de $f_1(X)$ e $f_2(X)$ no fecho algébrico de K, então $f_1(X)$ e $f_2(X)$ são polinômios minimais de α em $K[X]$. Mas então $f_1(X) = f_2(X)$, uma contradição. Assim, o polinômio $p(X) = f_1(X)\ldots f_r(X)$ é um polinômio separável sobre K. Logo, se F é o corpo de decomposição de $p(X) \in K[X]$, temos que F é uma extensão de Galois do corpo K. Além disso, se G é o grupo de Galois de F sobre K, o Teorema Fundamental nos diz que existe uma correspondência biunívoca entre os corpos intermediários entre F e K e os subgrupos de

G . Mas como o grupo G é finito, concluimos que existe apenas um número finito de corpos intermediários entre F e K .

Observemos agora que, como $\alpha_1,\ldots,\alpha_n$ são raízes de $p(X)$, temos necessariamente $K \subset E = K(\alpha_1,\ldots,\alpha_n) \subset F$. Portanto, entre E e K existe também um número finito de corpos intermediários. Logo, pela proposição anterior, E é uma extensão primitiva de K . □

Voltemos agora a considerar R um corpo e S uma R-álgebra que é finitamente gerada como R-módulo. Vimos, no início desta seção, que neste caso S é um espaço vetorial de dimensão finita sobre R e que contém R . Mas então é claro que qualquer ideal de S é um R-subespaço vetorial de S . Ainda, como um espaço vetorial de dimensão finita satisfaz a condição da cadeia descendente (ccd) para subespaços, temos que S é um anel que satisfaz ccd . Portanto, é válido o seguinte

Lema 3.4:

Sejam R um corpo e S uma R-álgebra que é finitamente gerada como R-módulo. Então S é um anel que satisfaz ccd . Em particular, se S é uma R-álgebra classicamente separável, é também um anel que satisfaz ccd .

Finalmente, o próximo teorema estabelece o resultado central deste parágrafo, e relaciona a definição de separabilidade clássica e a de álgebra separável.

Teorema 3.5:

Sejam R e S corpos tais que S é um espaço vetorial de dimensão finita sobre R . Então são equivalentes:

(i) S é uma R-álgebra separável;

(ii) $S \otimes_R K$ é um anel semi-simples, para cada corpo K extensão de R ;

(iii) S é uma extensão de R classicamente separável (i.e., todo elemento de S é separável sobre R);

(iv) existe um elemento $s \in S$ tal que $S = R(s)$ e o polinômio minimal de s é separável sobre R .

Prova:

(i)$\Rightarrow$(ii):

Seja K um corpo extensão de R . Então é claro que K é uma R-álgebra comutativa e, portanto, $S \otimes_R K$ é uma K-álgebra separável. Dado um $S \otimes_R K$-módulo M , é claro que M é um K-módulo livre (e, portanto, projetivo). Logo, aplicando o resultado 2.8, vemos que M é projetivo sobre $S \otimes_R K$. Assim, $S \otimes_R K$ é um anel semi-simples.

(ii)$\Rightarrow$(iii):

É claro que S é uma extensão algébrica de R , já que S é um espaço vetorial de dimensão finita sobre R . Sejam α um elemento de S e $f(X) \in R[X]$ seu polinômio minimal. Então é suficiente mostrar que f(X) não possui raízes múltiplas no fecho algébrico de R .

Para tal consideremos a extensão $T = R(\alpha)$. Como $T \subset S$, é fácil ver que $T \otimes_R K \subset S \otimes_R K$. Além disso, como $S \otimes_R K$ é um anel semi-simples e comutativo, sabemos que não existem elementos nilpotentes em $S \otimes_R K$. Portanto, $T \otimes_R K$ é também um anel (comutativo) sem elementos nilpotentes. Logo, aplicando a recíproca de I.6.7, vemos que $T \otimes_R K$ é um anel semi-simples, para cada corpo extensão K de R . Observemos agora que, sendo $f(X) \in R[X]$ um polinômio irredutível e $\alpha \in S$ uma raiz de $f(X)$, temos que o corpo $R[X]/_{<f(X)>}$ é isomorfo a T , através da aplicação $g(X) + <f(X)> \longmapsto g(\alpha)$, para cada $g(X) \in R[X]$, como é fácil verificar. Assim, sabemos que $R[X]/_{<f(X)>} \otimes \Omega$ é um anel semi-simples, onde Ω denota o fecho algébrico de R .

Mas $R[X]/_{<f(X)>} \otimes \Omega \simeq \Omega[X]/_{<f(X)>}$, através da aplicação $(\sum_{i=0}^{n} r_i X^i + <f(X)>) \otimes \omega \longmapsto (\sum_{i=0}^{n} r_i . \omega X^i) + <f(X)>$, para cada $\sum_{i=0}^{n} r_i X^i \in R[X]$, como é fácil verificar. Assim, concluimos que $\Omega[X]/_{<f(X)>}$ é um anel comutativo semi-simples e, portanto, não contém elementos nilpotentes, conforme I.6.7.

Vejamos finalmente que $f(X)$ é um polinômio separável sobre R . Para tal, suponhamos que $\alpha = \alpha_1, \ldots, \alpha_s \in \Omega$ são todas as raízes disttintas de $f(X)$. Então é claro que

$f(X) = (X-\alpha_1)^{n_1}(X-\alpha_2)^{n_2} \ldots (X-\alpha_s)^{n_s}$, onde $n_i \geq 1$ $(i=1,2,\ldots,s)$. Observemos no entanto que, se $n_i > 1$, para algum $i \in \{1,2,\ldots,s\}$, então o polinômio $g(X) = (X-\alpha_1)^{n_1} \ldots (X-\alpha_i)^{n_i-1} \ldots (X-\alpha_s)^{n_s}$ é tal que $g(X) + \langle f(X)\rangle$ é não nulo em $\Omega[X]/_{\langle f(X)\rangle}$ e é um elemento nilpotente neste anel, uma contradição. Portanto, $f(X) = (X-\alpha_1) \ldots (X-\alpha_s) \in \Omega[X]$ não possui raízes múltiplas, o que completa a prova.

(iii) $\Longrightarrow$ (iv):

É uma aplicação direta de 3.3 .

(iv) $\Longrightarrow$ (i):

É fácil ver que $S \otimes S$ é um anel, onde todos os elementos da forma $x \otimes y$, com $x,y \in S - \{0\}$ são inversíveis: $(x \otimes y)^{-1} = x^{-1} \otimes y^{-1}$.

Vamos mostrar que $S \otimes S$ comtém um idempotente de separabilidade. Seja $f(X) \in R[X]$ o polinômio minimal de $s \in S$. Então, por hipótese, $f(X)$ é um polinômio separável sobre R (no sentido estabelecido no capítulo I). Então sabemos que $f(X) = (X-s)q(X)$, onde $q(X) \in S[X]$ e $q(s) \neq 0$, já que todas as raízes de f no corpo de decomposição de R são distintas.

Consideremos agora as aplicações $e_1 : S \to S \otimes S$ e $e_2 : S \to S \otimes S$ dadas, respectivamente, por

$$e_1(k) = k \otimes 1 \quad \text{e} \quad e_2(k) = 1 \otimes k \ , \text{ para cada } k \in S \ .$$

É fácil ver que e_1 e e_2 são R-homomorfismos. Agora, para cada polinômio $p(X) = \sum_{i=0}^{n} a_i X^i \in S[X]$, denotemos por $[e_i(p)](X)$, $(i=1,2)$, o polinômio de $(S \otimes S)[X]$ que resulta ao aplicarmos e_i a cada coeficiente de $p(X)$. Ou seja,

$$[e_1(p)](X) = \sum_{i=0}^{n} e_1(a_i) X^i = \sum_{i=0}^{n} (a_i \otimes 1) X^i \quad \text{e}$$

$[e_2(p)](X) = \sum_{i=0}^{n} (1 \otimes a_i) X^i$. Assim, como $f(X)$ tem coeficientes pertencentes a R , é fácil verificar $[e_1(f)](X) = [e_2(f)](X)$.

Além disso, se $p(X) = \sum_{i=0}^{n} a_i X^i \in S[X]$ então $[e_1(p)](e_1(s)) =$

$= \sum_{i=0}^{n} (a_i \otimes 1)(s \otimes 1)^i = \sum_{i=0}^{n} a_i s^i \otimes 1 = p(s) \otimes 1$. Em particular, como $q(s)$ é um elemento não nulo de S , vemos que $[e_1(q)](e_1(s))$ é um elemento inversível de $S \otimes S$.

Se $q(X) = \sum_{i=0}^{m} b_i X^i$, definimos

$$e = [e_2(q)](e_1(s)) . \{[e_1(q)](e_1(s))\}^{-1} = [\sum_{i=0}^{m} (s^i \otimes b_i)] [q(s) \otimes 1]^{-1} \in S \otimes S \ .$$

Mostremos que este elemento satisfaz a condição (iii) de 1.1. É fácil ver que se μ representa o homomorfismo contração da R-álgebra S , então $\mu(e) = 1$.

Observemos agora que, para cada $\alpha = \sum_{j=0}^{t} r_j s^j \in S$,

$(\alpha\otimes 1 - 1\otimes\alpha)e = (\sum_{j=0}^{t} r_j s^j \otimes 1 - 1\otimes \sum_{j=0}^{t} r_j s^j)e =$

$= \sum_{j=0}^{t} r_j \cdot [s^j\otimes 1 - 1\otimes s^j]e$. Então, como $s^j\otimes 1 = (s\otimes 1)^j$ e $1\otimes s^j = (1\otimes s)^j$, vem que é suficiente mostrarmos que $(s\otimes 1)e = (1\otimes s)e$, para concluirmos que $(\alpha\otimes 1 - 1\otimes\alpha)e = 0$, para cada $\alpha\in S$. Ou ainda, vemos que é suficiente provar que $(s\otimes 1 - 1\otimes s)[e_2(q)](e_1(s)) = 0$.

Observemos agora que, como $f(X) = (X-s)q(X)$, onde $q(X)\in S[X]$, podemos escrever $[e_2(f)](e_1(s)) = [e_1(s) - e_2(s)][e_2(q)](e_1(s))$. Ainda, como $[e_2(f)](X) = [e_1(f)](X)$, vem que

$[e_1(s) - e_2(s)][e_2(q)](e_1(s)) = [e_1(f)](e_1(s)) = f(s)\otimes 1 = 0$

e, portanto, $(s\otimes 1 - 1\otimes s)e = 0$.

Concluimos então que S é uma R-álgebra separável. □

CAPÍTULO III

SOBRE A TEORIA DE GALOIS DE ANÉIS

Em [3], M. Auslander e O. Goldman introduziram o conceito de extensão de Galois de um anel comutativo. No entanto, eles não apresentaram nenhum resultado que generalizasse o Teorema Fundamental (I.5.9). Tal generalização foi apresentada por S.U. Chase, D.K. Harrison e A. Rosenberg em [6]. Vamos mostrar aqui os resultados obtidos neste último trabalho citado.

Continuamos a supor que todo anel tem unidade e que $\otimes$ representa $\otimes_R$. Na última seção, supomos ainda que todos os anéis considerados são comutativos.

Dizemos que um anel S é um ANEL EXTENSÃO DE R se S é uma R-álgebra comutativa que é fiel como R-módulo. É fácil ver que, neste caso, o homomorfismo de anéis dado por $r \mapsto r.1_S$, para todo $r \in R$, é um homomorfismo injetor. Portanto, podemos identificar R com sua imagem $R.1_S$, e considerar R um subanel de S, (justificando assim o uso do termo extensão). A partir de agora então, sempre que nos referirmos a S como uma extensão de R estaremos supondo

para simplificar notações, que R é um subanel de S.

Em todo este capítulo, estudamos anéis extensões do anel R. Em particular, aquelas que satisfazem uma certa condição são chamadas extensões de Galois. Os resultados obtidos serão aplicados no próximo capítulo, quando estudaremos álgebras fortemente separáveis.

§ 1. EXTENSÕES DE GALOIS DE ANÉIS COMUTATIVOS

Generalizando o conceito estabelecido no capítulo I, se S é um anel e se H denota um grupo de automorfismos de S, então o conjunto de elementos de S que são deixados fixos por cada automorfismos de H é um subanel de S, como é fácil verificar. Tal subanel é denominado SUBANEL FIXO DE S POR H (ou, simplesmente, SUBANEL FIXO DE H, quando não há dúvidas quanto ao anel considerado), e é denotado por S^H. Então

$$S^H = \{x \in S \mid \sigma(x) = x \ , \ \forall \sigma \in H\}$$

Suponhamos agora que S é uma extensão de R. Observemos então que todo automorfismo de S que deixa R fixo é um R-automorfismo. Reciprocamente, se H é um grupo de R-automorfismos de S, então $R \subset S^H$.

No que segue, denotamos por S uma extensão de R, e G denota um grupo finito de automorfismos de S tal que $S^G = R$.

Dizemos que $D = D(S,G)$ é um PRODUTO CRUZADO DE S COM G se D é a R-álgebra definida da seguinte maneira: D é um S-módulo à esquerda livre, com geradores da forma u_σ, para cada $\sigma \in G$, i.e., $D = \bigoplus_{\sigma \in G} S.u_\sigma$ (observemos que a soma direta é finita, já que G é um grupo finito), onde a soma e o produto externo são definidos de maneira natural. Além disso, o produto interno é definido por distributividade e pela igualdade $(s.u_\sigma)(t.u_\zeta) = s\,\sigma(t).u_{\sigma\zeta}$, para cada $s,t \in S$, $\sigma,\zeta \in G$. O leitor pode verificar facilmente que D é realmente uma R-álgebra não necessariamente comutativa.

Podemos definir, de maneira natural, uma estrutura de S-módulo no conjunto $\mathrm{Hom}_R(S,S)$ dos R-homomorfismos de S em S. Além disso, com a composição de funções, $\mathrm{Hom}_R(S,S)$ é um anel. Logo, é fácil ver que $\mathrm{Hom}_R(S,S)$ é também uma R-álgebra (mas não necessariamente uma S-álgebra).

Relacionamos agora as R-álgebras D e $\mathrm{Hom}_R(S,S)$ no seguinte

Lema 1.1:

A aplicação $j : D \to \mathrm{Hom}_R(S,S)$, definida por $[j(\sum_{\sigma \in G} s.u_\sigma)](x) = \sum_{\sigma \in G} s\sigma(x)$, para cada $\sum_{\sigma \in G} s.u_\sigma \in D$, $x \in S$, é um homomorfismo de R-álgebras e de S-módulos.

Prova:

É fácil ver que j está bem definida e que é um homomorfismo de anéis. Ainda, para cada $s.u_\sigma \in D$, $x,s' \in S$,

$$[j(s's.u_\sigma)](x) = s's\sigma(x) = s'[j(s.u_\sigma)](x) = [s'.(j(s.u_\sigma))](x) .$$

Logo, j é um homomorfismo de R-álgebras e S-módulos. □

Denotemos por E o conjunto de todas as funções do grupo G no anel S , e consideremos em E as operações de adição e multiplicação de funções definidas de maneira natural. Definimos também um produto externo por $(s.f)(\sigma) = sf(\sigma)$, para cada $s \in S$, $f \in E$, $\sigma \in G$. Então é fácil verificar que E é um anel comutativo, cuja unidade é dada por $1_E(\sigma) = 1_S$, para todo $\sigma \in G$. Além disso, E é também uma S-álgebra, como é fácil provar.

Denotemos por v_σ os elementos de E dados por $v_\sigma(\zeta) = \delta_{\sigma\zeta}$, para cada $\sigma,\zeta \in G$. Podemos observar que:

i) $(v_\sigma)^2 = v_\sigma$, para cada $\sigma \in G$. Ou seja, v_σ é um elemento idempotente do anel E ;

ii) $v_\sigma v_\zeta = \delta_{\sigma\zeta}$, para cada $\sigma,\zeta \in G$. Ou seja, os elementos do conjunto $\{v_\sigma\}_{\sigma \in G}$ são dois a dois ortogonais;

iii) $\sum_{\sigma \in G} v_\sigma = 1_E$.

Concluimos então que $E = \bigoplus_{\sigma \in G} S.v_\sigma$, isto é,

E é gerado sobre S por idempotentes dois a dois ortogonais. Logo, podemos calcular o produto em E da seguinte maneira: para cada $\gamma,\sigma,\zeta \in G$, a_σ , $b_\zeta \in S$,

$[(a_\sigma.v_\sigma)(b_\zeta.v_\zeta)](\gamma) = (a_\sigma\delta_{\sigma\gamma})(b_\zeta\delta_{\zeta\gamma}) = a_\sigma b_\zeta \delta_{\sigma\zeta}$, ou seja,

$$(a_\sigma.v_\sigma)(b_\zeta.v_\zeta) = a_\sigma b_\zeta \delta_{\sigma\zeta}.v_\sigma \quad .$$

Relacionamos agora as S-álgebras $S \otimes S$ e E no seguinte lema, cuja prova deixamos a cargo do leitor.

Lema 1.2:

A aplicação linear $h : S \otimes S \to E$ dada por $[h(s \otimes t)](\sigma) = s\sigma(t)$, para cada $s \otimes t \in S \otimes S$, $\sigma \in G$, é um homomorfismo de S-álgebras.

Lembremos agora o conceito de operação de um grupo sobre um conjunto.

Sejam G um grupo e M um conjunto. Dizemos que G AGE EM M (ou que G OPERA EM M) se existe uma aplicação que associa a cada par $(\sigma,m) \in G \times M$ um elemento de M (denotado por $\sigma.m$) e que satisfaz as seguintes propriedades:

(i) para cada $\sigma,\zeta \in G$, $m \in M$, $\sigma.(\zeta.m) = (\sigma\zeta).m$;

(ii) $1_G.m = m$, para cada $m \in M$.

Desta maneira, é fácil verificar que se G age em M , então existe uma aplicação ψ de G no conjunto das aplicações de M em M (que denotamos por M^M), definida da

seguinte maneira: $[\psi(\sigma)](m) = \sigma.m$, para cada $\sigma \in G$, $m \in M$. Dizemos que G OPERA FIELMENTE EM M se esta aplicação ψ é injetora.

Ainda, se M é um grupo abeliano e G age em M , dizemos que M é um G-MÓDULO, se também é satisfeita a seguinte condição:

(iii) $\sigma.(m+m') = \sigma.m + \sigma.m'$, para cada $\sigma \in G$, $m, m' \in M$.

Consideremos novamente o anel $D = \bigoplus_{\sigma \in G} S.u_\sigma$, e seja M um D-módulo. Então é fácil ver que, através da igualdade $\sigma.m = u_\sigma.m$, para cada $\sigma \in G$, $m \in M$, M é um G-módulo. Por outro lado, M é também um S-módulo, cujo produto externo é dado por distributividade e pela relação $s.m = (s.u_{1_G}).m$, para cada $s \in S$, $m \in M$, como é fácil verificar; (logo, M é também um R-módulo). Além disso, para cada $s \in S$, $\sigma \in G$, $m \in M$, pode-se constatar que $s.(\sigma.m) = \sigma.(s.m)$. Também a recíproca é verdadeira, i.e., se M é um G-módulo e um S-módulo tal que $s.(\sigma.m) = \sigma.(s.m)$, para cada $s \in S$, $\sigma \in G$, $m \in M$, então M é um D-módulo, onde o produto externo é definido por distributividade e pela igualdade $(s.u_\sigma).m = s.(\sigma.m)$, para todo $s \in S$, $\sigma \in G$, $m \in M$, como é fácil verificar.

Seja M um D-módulo. Denotemos por M^G o subconjunto de M formado por todos os elementos de M que permanecem invariantes por G , i.e.:

$$M^G = \{m \in M \mid \forall \sigma \in G \ , \ \sigma.m = m\}$$

Então é fácil ver que M^G é um R-submódulo de M . Além disso, temos o seguinte

Lema 1.3:

Se M é um D-módulo, a aplicação linear $\omega : S \otimes M^G \to M$ dada por $\omega(s \otimes m) = s.m$, para cada $s \otimes m \in S \otimes M^G$, é um homomorfismo de S-módulos.

Prova:

Observemos que ω é induzida pelo produto externo do S-módulo M . De fato, a aplicação $\phi : S \times M^G \to M$ dada por $\phi(s,m) = s.m$, para cada $s \in S$, $m \in M^G$, é evidentemente uma forma bilinear sobre R . Logo, pela propriedade universal do produto tensorial, $\omega : S \otimes M^G \to M$ dada por $\omega(s \otimes m) = s.m$, para cada $s \otimes m \in S \otimes M^G$ está bem definida. O resto da prova é claro. □

Estamos agora em condições de mostrar o seguinte teorema que caracteriza as extensões de Galois de anéis comutativos. Utilizamos aqui o conceito de homomorfismos fortemente distintos, apresentado no final da seção 2 do capítulo II.

Teorema 1.4:

Sejam S um anel comutativo, G um grupo finito de automorfismos de S e $R = S^G$. Então as seguintes condições são equivalentes:

(a) S é uma R-álgebra separável e os elementos de G são dois a dois fortemente distintos;

(b) existem elementos $x_i, y_i \in S$ $(i=1,2,\ldots,n)$ tais que $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1\sigma}$, para cada $\sigma \in G$ (onde 1, na expressão $\delta_{1\sigma}$, é a identidade em S);

(c) S é um R-módulo finitamente gerado e projetivo, e a aplicação j (dada em 1.1) é um isomorfismo (de R-álgebras e S-módulos);

(d) se M é um D-módulo à esquerda, então a aplicação ω (dada em 1.3) é um isomorfismo de S-módulos;

(e) a aplicação h (dada em 1.2) é um isomorfismo de S-álgebras;

(f) para cada ideal maximal M de S e cada elemento $\sigma \neq 1_G$, de G, existe um elemento $s = s(M,\sigma)$ em S tal que $s - \sigma(s) \notin M$.

Prova:

a $\Longrightarrow$ b:

Para cada $\sigma \in G$, definimos uma aplicação linear $g_\sigma : S \otimes S \to S$ por $g_\sigma(s \otimes s') = [h(s \otimes s')](\sigma)$, para cada $s \otimes s' \in S \otimes S$ (onde $h : S \otimes S \to E$ é o homomorfismo considerado anteriormente). Portanto, é claro que g_σ está bem definida e é um homomrfismo de S-álgebras tal que $g_\sigma(s \otimes s')(\sigma) = s\sigma(s')$.

Ainda, como os elementos de G são por hipótese dois a dois fortemente distintos, para cada idempotente não nulo $e \in S$ e para cada par de elementos distintos

$\sigma,\zeta \in G$, existe um elemento $s \in S$ tal que $\sigma(s)e \neq \zeta(s)e$. Assim, $g_\sigma(1 \otimes s)e \neq g_\zeta(1 \otimes s)e$ e podemos concluir que os homomorfismos g_σ são também dois a dois fortemente distintos.

Observemos agora que, por II.2.14, $S \otimes S$ é uma S-álgebra separável e comutativa. Então, por II.2.21, para cada $\sigma,\zeta \in G$ existem idempotentes $e_\sigma, e_\zeta \in S \otimes S$ satisfazendo $g_\sigma(e_\zeta) = \delta_{\sigma\zeta}$, $e_\sigma e_\zeta = \delta_{\sigma\zeta}$ e $g_\sigma(s \otimes s').e_\sigma = (s \otimes s')e_\sigma$, para todo $s \otimes s' \in S \otimes S$, $\sigma,\zeta \in G$.

Se $e_1 = \sum_{i=1}^{n} x_i \otimes y_i \in S \otimes S$ então para cada $\sigma \in G$, $\delta_{1\sigma} = g_\sigma(e_1) = \sum_{i=1}^{n} x_i \sigma(y_i)$, o que completa a prova.

<u>b $\Longrightarrow$ c</u>:

Para mostrar que S é um R-módulo finitamente gerado e projetivo, consideremos a aplicação $t : S \to R$, dada por $t(s) = \sum_{\sigma \in G} \sigma(s)$, para cada $s \in S$. Observemos que, para cada $s \in S$, $t(s)$ é realmente um elemento de R . De fato, se $\zeta \in G$ então $\zeta(t(s)) = \sum_{\sigma \in G} \zeta\sigma(s) = \sum_{\rho \in G} \rho(s) = t(s)$ ou seja, $t(s) \in S^G = R$. É fácil ver ainda que t é homomorfismo de R-módulos.

Se existem $x_i, y_i \in S$ $(i=1,2,\ldots,n)$ tais que $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1\sigma}$, para cada $\sigma \in G$, definimos aplicações $f_i : S \to R$ por $f_i(s) = t(s\, y_i)$, para cada $s \in S$. Então é

claro que $f_i \in \mathrm{Hom}_R(S,R)$. Ainda, para cada $s \in S$,

$$\sum_{i=1}^{n} f_i(s)x_i = \sum_{i=1}^{n} t(s\,y_i)x_i = \sum_{\sigma \in G} \sum_{i=1}^{n} \sigma(s\,y_i)x_i =$$

$$= \sum_{\sigma \in G} \sigma(s) \sum_{i=1}^{n} \sigma(y_i)x_i = \sum_{\sigma \in G} \sigma(s)\delta_{1\sigma} = s \ .$$ Portanto, os

R-homomorfismos f_i e os elementos $x_i \in S$ $(i=1,2,\ldots,n)$

são coordenadas projetivas para o R-módulo S . Logo, S é um R-módulo finitamente gerado e projetivo.

Resta-nos mostrar que o homomorfismo de S-módulos e R-álgebras $j : D \to \mathrm{Hom}_R(S,S)$ é um isomorfismo.

De fato, dada uma aplicação $g \in \mathrm{Hom}_R(S,S)$, podemos escrever, para cada $x \in S$:

$$g(x) = g\Big(\sum_{i=1}^{n} f_i(x)x_i\Big) = \sum_{i=1}^{n} f_i(x)g(x_i) = \sum_{i=1}^{n} \sum_{\sigma \in G} \sigma(x\,y_i)g(x_i) =$$

$$= \sum_{\sigma \in G} \Big[\sum_{i=1}^{n} \sigma(y_i)g(x_i)\Big]\sigma(x) \ .$$

Então, pondo $s_\sigma = \sum_{i=1}^{n} \sigma(y_i)g(x_i) \in S$, para cada $\sigma \in G$, temos que $g(x) = \sum_{\sigma \in G} s_\sigma \sigma(x) = \big[j\big(\sum_{\sigma \in G} s_\sigma . u_\sigma\big)\big](x)$. Ou seja, $g = j\big(\sum_{\sigma \in G} s_\sigma . u_\sigma\big)$, donde concluimos que j é um epimorfismo.

Finalmente, suponhamos que $d = \sum_{\zeta \in G} s_\zeta . u_\zeta \in D$ é um elemento tal que $j(d) = 0$. Então, para cada $x \in S$, $0 = [j(d)](x) = \sum_{\zeta \in G} s_\zeta \zeta(x)$. Em particular, $[j(d)](x_i) = \sum_{\zeta \in G} s_\zeta \zeta(x_i) = 0$,

para $i=1,2,\ldots,n$. Portanto, é claro que

$$0 = \sum_{i=1}^{n} \sum_{\sigma \in G} \left[\sum_{\zeta \in G} s_\zeta \zeta(x_i)\sigma(y_i) \right].u_\sigma = \sum_{\sigma \in G} \sum_{\zeta \in G} s_\zeta \left[\sum_{i=1}^{n} \zeta(x_i)\sigma(y_i) \right].u_\sigma \ .$$

Mas $\sum_{i=1}^{n} \zeta(x_i)\sigma(y_i) = \zeta\left(\sum_{i=1}^{n} x_i \zeta^{-1}\sigma(y_i) \right) = \zeta(\delta_{1(\zeta^{-1}\sigma)}) = \zeta(\delta_{\sigma\zeta}) =$

$= \delta_{\sigma\zeta}$. Assim, podemos escrever

$0 = \sum_{\sigma \in G} \sum_{\zeta \in G} (s_\zeta \delta_{\sigma\zeta}).u_\sigma = \sum_{\sigma \in G} s_\sigma.u_\sigma = d$, o que mostra que j é também um monomorfismo.

<u>c $\Longrightarrow$ d</u>:

Seja M um D-módulo à esquerda. Para mostrar que, supondo (c), o homomorfismo de S-módulos $\omega : S \otimes M^G \to M$ é um isomorfismo, vamos definir uma aplicação inversa para ω . Antes, porém, façamos algumas observações que nos serão necessárias.

Sejam $f_i \in \mathrm{Hom}_R(S,R)$ e $x_i \in S$ $(i=1,2,\ldots,n)$ coordenadas projetivas do R-módulo S . Como R é um subanel de S , podemos considerar cada f_i um R-homomorfismo de S em S , i.e., $f_i \in \mathrm{Hom}_R(S,S)$, para cada $i \in \{1,2,\ldots,n\}$. Então, sendo j um isomorfismo de D sobre $\mathrm{Hom}_R(S,S)$, existem elementos $d_i \in D$ tais que $j(d_i) = f_i$ $(i=1,2,\ldots,n)$. Observemos então que, para cada $s \in S$,

$$[j(\sum_{i=1}^{n} x_i.d_i)](s) = \sum_{i=1}^{n} x_i [j(d_i)(s)] = \sum_{i=1}^{n} x_i f_i(s) = s \ , \text{ donde}$$

segue-se que $j(\sum_{i=1}^{n} x_i.d_i) = id_S$. Portanto, sendo j um isomorfismo, temos que

$$\sum_{i=1}^{n} x_i.d_i = 1_D .$$

Além disso, para cada $\sigma \in G$, $i \in \{1,2,\ldots,n\}$, $s \in S$,

$[j(u_\sigma d_i)](s) = [j(u_\sigma)j(d_i)](s) = [j(u_\sigma)](f_i(s)) = \sigma(f_i(s)) = f_i(s) = [j(d_i)](s)$. Portanto, $j(u_\sigma d_i) = j(d_i)$, ou ainda, $u_\sigma d_i = d_i$, já que j é um isomorfismo.

Considerando então a estrutura de G-módulo do D-módulo M , para cada $\sigma \in G$, $m \in M$, temos que $\sigma.(d_i.m) = u_\sigma.(d_i.m) = (u_\sigma d_i).m = d_i.m$. Portanto,

$d_i.m \in M^G$, para todo $i \in \{1,2,\ldots,n\}$

Conseqüentemente, a aplicação $\gamma : M \to S \otimes M^G$ dada por $\gamma(m) = \sum_{i=1}^{n} x_i \otimes d_i.m$, para cada $m \in M$, está bem definida e é aditiva. Então, para cada $m \in M$, temos que

$$(w\gamma)(m) = w(\sum_{i=1}^{n} x_i \otimes d_i.m) = \sum_{i=1}^{n} x_i.(d_i.m) = \sum_{i=1}^{n} (x_i.d_i).m = m ,$$

donde conclui-se que $w\gamma = id_M$.

Observemos agora que, se $d_i = \sum_{\sigma \in G} s_\sigma.u_\sigma$, então para cada $m \in M^G$, $s \in S$,

$$d_i.(s.m) = [d_i.(s.u_1)].m = \sum_{\sigma \in G} [s_\sigma \sigma(s)].m = [j(d_i)](s).m =$$

$= f_i(s).m$. Portanto, para cada $s \otimes m \in S \otimes M^G$, resulta que

$$(\gamma w)(s \otimes m) = \gamma(s.m) = \sum_{i=1}^{n} x_i \otimes d_i.(s.m) = \sum_{i=1}^{n} x_i \otimes f_i(s).m =$$

$$= (\sum_{i=1}^{n} x_i f_i(s)) \otimes m = s \otimes m \text{ . Ou seja, } \gamma w = id_{S \otimes M^G} \text{ , o que}$$

completa a prova.

<u>d $\Longrightarrow$ e</u>:

Para mostrar que o homomorfismo de S-álgebras $h : S \otimes S \to E$ é um isomorfismo, vamos representá-lo como uma composição de dois isomorfismos de S-álgebras.

Primeiramente é fácil ver que a S-álgebra $E = \bigoplus_{\sigma \in G} S.v_\sigma$ pode ser dotada de uma estrutura de G-módulo se definimos $(\sigma.g)(\zeta) = \sigma[g(\sigma^{-1}\zeta)]$, para cada $\sigma, \zeta \in G$, $g \in E$.

Portanto, podemos também definir sobre E uma estrutura de D-módulo, cujo produto externo é definido por distributividade e pela igualdade $(s.u_\sigma).g = s.(\sigma.g)$, para cada $s \in S$, $\sigma \in G$, $g \in E$, como é fácil verificar.

Assim, podemos obter um isomorfismo de S-mó<u></u>dulos $\omega : S \otimes E^G \to E$, dado por $\omega(s \otimes g) = s.g$, para cada $s \otimes g \in S \otimes E^G$.

Vejamos agora que os elementos de E^G são exatamente os G-homomorfismos de G em S . De fato, g é um elemento de E^G se e só se, para cada $\sigma \in G$, $g = \sigma.g$, i.e., para cada $\sigma, \zeta \in G$, $g(\zeta) = (\sigma.g)(\zeta) = \sigma[g(\sigma^{-1}\zeta)]$.

Logo, $g \in E^G$ se e só se $\sigma^{-1}.[g(\zeta)] = g(\sigma^{-1}\zeta)$, para cada $\sigma,\zeta \in G$, $g \in E$, ou, equivalentemente, g é um G-homomorfismo.

Para cada $s \in S$, $\sigma \in G$, coloquemos $[\theta(s)]\sigma = \sigma(s)$. Então $\theta(s)$ é um elemento de E, e, para cada $\sigma,\zeta \in G$,

$$[\theta(s)](\sigma\zeta) = (\sigma\zeta)(s) = \sigma[\zeta(s)] = \sigma[\theta(s)(\zeta)] = [\sigma\theta(s)](\zeta) .$$

Portanto, $\theta(s)$ é um G-homomorfismo e, consequentemente, $\theta(s) \in E^G$. Fica assim definida uma função $S \to E^G$ pela relação anterior.

É fácil ver que θ é um R-homomorfismo. Ainda, se $\psi : E^G \to S$ é a aplicação dada por $\psi(g) = g(1_G)$, para cada $g \in E^G$, então $(\theta\psi)(g) = \theta[g(1_G)]$ e, para cada $\sigma \in G$,

$$[\theta\psi(g)](\sigma) = \theta[g(1_G)](\sigma) = \sigma[g(1_G)] = (\sigma.g)(\sigma) = g(\sigma) ,$$

donde conclui-se que $\theta\psi = id_{E^G}$. Além disso, para cada $s \in S$, $(\psi\theta)(s) = \psi[\theta(s)] = [\theta(s)](1_G) = 1_G(s) = s$, i.e., $\psi\theta = id_S$. Logo, θ é um isomorfismo de R-módulos.

Então a aplicação $id_S \otimes S : S \otimes S \to S \otimes E^G$ é um isomorfismo de S-módulos. Além disso, sendo ω um isomorfismo de S-módulos, temos que a aplicação composta $\omega \circ (id_S \otimes \theta) : S \otimes S \to E$ é também um isomorfismo de S-módulos.

Mas então, para cada $s \otimes t \in S \otimes S$, $\sigma \in G$,

$\{[\omega \circ (id_S \otimes \theta)](s \otimes t)\}(\sigma) = [\omega(s \otimes \theta(t))](\sigma) = [s.\theta(t)](\sigma) =$

$= s\sigma(t) = [h(s \otimes t)](\sigma)$. Portanto, $\omega \circ (id_S \otimes \theta) = h$, o que completa a prova.

e $\Longrightarrow$ a

Mostremos inicialmente que S é um $S \otimes S$-módulo projetivo. Sendo $\{v_\sigma\}_{\sigma \in G}$ um conjunto ortogonal de geradores (idempotentes) da S-álgebra $E = \bigoplus_{\sigma \in G} S.v_\sigma$, é fácil ver que $E = \bigoplus_{\sigma \in G} E v_\sigma$, ou seja, $S.v_\sigma = E v_\sigma$, para cada $\sigma \in G$. Logo, $S.v_\sigma$ é um E-somando direto de E e, portanto, é um E-módulo projetivo.

Ainda, como por hipótese as S-álgebras E e $S \otimes S$ são isomorfas e como S é também isomorfo a $S.v_\sigma$, para cada $\sigma \in G$, podemos concluir que S é um $S \otimes S$-módulo projetivo.

Resta-nos então mostrar que os automorfismos de G são dois a dois fortemente distintos. Observemos antes que, como h é um isomorfismo, pondo

$h^{-1}(v_1) = \sum_{i=1}^{n} x_i \otimes y_i \in S \otimes S$, temos que, para cada $\sigma \in G$;

$$\delta_{1\sigma} = v_1(\sigma) = [h(h^{-1}(v_1))](\sigma) = h(\sum_{i=1}^{n} x_i \otimes y_i)(\sigma) = \sum_{i=1}^{n} x_i \sigma(y_i)$$

Suponhamos então que $e \in S$ é um idempotente não nulo de S , e que σ e ζ são dois elementos distintos de G . Se, para todo $s \in S$, $\sigma(s)e = \zeta(s)e$, em parti-

cular para cada $i \in \{1,2,\ldots,n\}$,

$[\sigma\zeta^{-1}(y_i)]e = [\zeta\zeta^{-1}(y_i)]e = y_i e$. Além disso,

pela observação feita acima, vem que $\delta_{1\sigma} e = \sum_{i=1}^{n} x_i \sigma(y_i) e$

e, consequentemente, $e = (\sum_{i=1}^{n} x_i y_i) e$.

Portanto, sendo σ e ζ distintos, temos

que $e = \sum_{i=1}^{n} x_i (y_i e) = [\sum_{i=1}^{n} x_i \sigma\zeta^{-1}(y_i)]e = \delta_{\sigma\zeta} e = 0$, uma contradição. Logo, σ e ζ são homomorfismos fortemente distintos.

b $\Longrightarrow$ f:

Sejam M um ideal maximal de S e σ um elemento de G tal que $\sigma \neq 1_G$. Suponhamos que para cada $s \in S$, $s - \sigma(s)$ é um elemento de M . Então, em particular, para cada $i \in \{1,2,\ldots,n\}$, $y_i - \sigma(y_i) \in M$ e portanto,

$\sum_{i=1}^{n} x_i [y_i - \sigma(y_i)]$ é também um elemento de M . Mas

$\sum_{i=1}^{n} x_i [y_i - \sigma(y_i)] = \sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{11} - \delta_{1\sigma} = 1$, o que contraria o caráter maximal do ideal M . Logo, existe um elemento $s \in S$ tal que $s - \sigma(s) \notin M$.

f $\Longrightarrow$ b:

Mostremos inicialmente que os elementos

$x_1,\ldots,x_n$, $y_1,\ldots,y_n \in S$ dados em (b) existem, para cada $\sigma \in G$ fixado. De fato, para cada $\sigma \in G$, $\sigma \neq 1_G$, consideramos o ideal I de S gerado por todos os elementos da forma $s - \sigma(s)$, com $s \in S$. Então, como para cada ideal maximal M de S existe $s' \in S$ tal que $s' - \sigma(s') \notin M$, temos que $I \not\subset M$, i.e., $I = S$. Então existem elementos $a_i, b_i \in S \ (i=1,2,\ldots,n_\sigma)$, tais que $1 = \sum_{i=1}^{n_\sigma} a_i [b_i - \sigma(b_i)] = \sum_{i=1}^{n_\sigma} a_i b_i - \sum_{i=1}^{n_\sigma} a_i \sigma(b_i)$.

Pondo $a_{n_\sigma+1} = - \sum_{i=1}^{n_\sigma} a_i \sigma(b_i)$ e $b_{n_\sigma+1} = 1$, é claro que

$$\sum_{i=1}^{n_\sigma+1} a_i b_i = 1 \quad \text{e} \quad \sum_{i=1}^{n_\sigma+1} a_i \sigma(b_i) = 0 \ , \text{ ou ainda,}$$

$\sum_{i=1}^{n_\sigma+1} a_i \sigma(b_i) = \delta_{1\sigma}$. Observemos, no entanto, que os elementos a_i e b_i $(i=1,2,\ldots,n_\sigma+1)$ são determinados em função do automorfismo σ fixado. Vamos utilizar este fato para mostrar a existência de elementos $x_i, y_i \in S$ que independem da escolha do automorfismo em G e que satisfazem a condição estabelecida em (b).

Por hipótese, G é um grupo finito. Sejam m a ordem de G e G' um subconjunto de G com k elementos. Vamos utilizar indução sobre k para mostrar que é possível encontar elementos de S que satisfazem a condição (b), para cada elemento de G' .

Se $k = 1$, já vimos, pela observação feita acima, que tais elementos existem. Podemos então supor, sem

perda de generalidade que G' é um subconjunto de G que contém o elemento 1_G. Suponhamos então $k < n$ e que existem elementos $x_i', y_i' \in S$, com $i \in \{1,2,\ldots,p\}$, tais que $\sum_{i=1}^{p} x_i' \sigma(y_i') = \delta_{1\sigma}$, para cada $\sigma \in G'$. Seja ζ um elemento de G não pertencente a G', e sejam $a_j, b_j \in S$, com $j=1,2,\ldots,m_\zeta$ elementos de S que satisfazem a igualdade $\sum_{j=1}^{m_\zeta} a_j \zeta(b_j) = \delta_{1\zeta}$.

Observemos então que

$$\sum_{i=1}^{\rho} \sum_{j=1}^{m_\zeta} a_j x_i' y_i' b_j = \sum_{j=1}^{m_\zeta} a_j \left(\sum_{i=1}^{p} x_i' y_i'\right) b_j = \sum_{j=1}^{m_\zeta} a_j b_j = 1 \quad \text{e,}$$

para cada $\sigma \in G'$, $\sigma \neq 1_G$,

$$\sum_{i=1}^{p} \sum_{j=1}^{m_\zeta} a_j x_i' \sigma(y_i' b_j) = \sum_{j=1}^{m_\zeta} a_j \left(\sum_{i=1}^{p} x_i' \sigma(y_i')\right) \sigma(b_j) = 0 .$$

Além disso, como $\zeta \neq 1_G$, $\sum_{i=1}^{p} \sum_{j=1}^{m_\zeta} a_j x_i' \zeta(y_i' b_j) = 0$. Logo, os elementos $x_{ji} = a_j x_i'$ e $y_{ji} = y_i' b_j$, com $i \in \{1,2,\ldots,p\}$ e $j \in \{1,2,\ldots,n_\zeta\}$ são tais que $\sum_{i=1}^{p} \sum_{j=1}^{m_\zeta} x_{ji} \sigma(y_{ji}) = \delta_{1\sigma}$, para cada $\sigma \in G' \cup \{\zeta\}$, o que completa a prova. □

Seja S uma extensão de R. Dizemos que S é uma EXTENSÃO DE GALOIS DE R ou EXTENSÃO GALOISIANA DE R,

se alguma das condições equivalentes do teorema anterior é satisfeita. Neste caso, um conjunto de elementos $x_i, y_i \in S$ $(i=1,2,\ldots,n)$ que satisfaz a condição (b) é denominado SISTEMA G-GALOIS DE COORDENADAS, enquanto que o grupo G dos R-automorfismos de S é chamado GRUPO DE GALOIS.

Façamos agora algumas observações a respeito do resultado anterior:

NOTA 1: Se S (e portanto R) é um corpo, é fácil ver que a condição (f) do resultado acima é verificada. Logo, neste caso, se $R = S^G$ para algum grupo finito G de automorfismos de S, então S é uma extensão galoisiana do corpo R, no sentido dado acima. Portanto, a condição (c) nos assegura que S é um R-módulo finitamente gerado, ou seja, S é um espaço vetorial de dimensão finita sobre R. Então a definição dada acima é uma generalização da definição usual para corpos.

NOTA 2: Da prova de $b \Longrightarrow c$ acima é fácil verificar que os elementos $x_i, y_i \in S$ dados em (b) e os R-homomorfismos $f_i : S \to R$ dados por $f_i(x) = t(x y_i)$, para cada $x \in S$ (onde $t : S \to R$ é o R-homomorfismo dado por $t(s) = \sum_{\sigma \in G} \sigma(s)$, para cada $s \in S$), formam um sistema de coordenadas projetivas para o R-módulo S. Além disso, mostremos aqui que esta aplicação t é exatamente a função traço $t_S : S \to R$ induzida pelo R-módulo finitamente gerado e projetivo S,

definida na seção 3 do capítulo I. De fato, para cada $x \in S$, sabemos que

$$t_S(x) = \sum_{i=1}^{n} f_i(x\, x_i) = \sum_{i=1}^{n} t(x\, x_i\, y_i) = t(x \sum_{i=1}^{n} x_i y_i) = t(x) \quad .$$

Portanto, concluimos que se S é uma extensão galoisiana de R então a função traço da R-álgebra S em R induzida pelo R-módulo finitamente gerado e projetivo S é dada por: $t(x) = \sum_{\sigma \in G} \sigma(x)$, para cada $x \in S$.

NOTA 3: Fica claro que, se S é uma extensão galoisiana de R então S é uma R-álgebra separável e um R-módulo finitamente gerado e projetivo.

NOTA 4: Se S é um anel sem idempotentes próprios que é uma extensão de Galois de R com grupo de Galois G, então os elementos de G são trivialmente dois a dois fortemente distintos. Neste caso, a condição (a) acima resume-se simplesmente a ser S uma R-álgebra separável. É claro que este é o caso se S é um corpo. Logo, se S não tem idempotentes próprios, S é uma extensão de Galois de R se e só se $S^G = R$ e S é R-sepáravel.

Com referência às extensões galoisianas de anéis, podemos mostrar a seguinte

Proposição 1.5:

Se S é uma extensão galoisiana de R com grupo de Galois G, então existe um elemento $c \in S$ tal

que $t(c) = 1_R$. Além disso, R é um R-somando direto de S .

Prova:

Sejam $x_1,\ldots,x_n,y_1,\ldots,y_n \in S$ um sistema G-galois de coordenadas. Então podemos escrever

$$\sum_{i=1}^{n} x_i\, t(y_i) = \sum_{i=1}^{n} x_i \sum_{\sigma \in G} \sigma(y_i) = \sum_{\sigma \in G} \sum_{i=1}^{n} x_i \sigma(y_i) = \sum_{\sigma \in G} \delta_{1\sigma} = 1_S .$$

Portanto, o ideal de S gerado pelo conjunto t(S) é S , (i.e., $S\,t(S) = S$) . Além disso, sabemos que S é um R-módulo finitamente gerado. Suponhamos então $S = R s_1 + \ldots + R s_m$, e mostremos que existe um elemento $r \in t(S)$ tal que $(1 - r)S = 0$. Isto implica $1 - r = 0$ e portanto, pondo $r = t(c)$, está completa a primeira parte da prova.

Definamos então $S_i = R s_i + R s_{i+1} + \ldots + R s_m$, para cada $i \in \{1,2,\ldots,m\}$ e $S_{m+1} = 0$, e, por indução, determinemos um elemento $z_i \in t(S)$ tal que $(1 - z_i)S \subset S_i$, para cada $i \in \{1,2,\ldots,m+1\}$.

Para i=1 é fácil ver que basta-nos tomar $z_1 = 0$, já que $S_1 = S$. Admitamos a seguir a existência de um elemento $z_i \in t(S)$ tal que $(1 - z_i)S \subset S_i$, para algum $i < m + 1$. Então, como $S\,t(S) = S$, podemos escrever $(1 - z_i)S \subset (1 - z_i)\, S\, t(S) \subset S_i\, t(S)$. Em particular, $(1 - z_i)s_i \in S_i\, t(S)$, ou seja, existem elementos $t_{ij} \in t(S)$,

$y_{ij} \in S_i$ $(j=1,2,\ldots,n_i)$ tais que $(1 - z_i)s_i = \sum_{j=1}^{n_i} y_{ij}t_{ij}$.

Além disso, como $S_i = Rs_i + Rs_{i+1} + \ldots + Rs_m$, temos que existem elementos $r_{ijk} \in R$ $(k=i,i+1,\ldots,m)$, tais que

$y_{ij} = \sum_{k=i}^{m} r_{ijk}s_k$, e então $(1 - z_i)s_i = \sum_{j=1}^{n_i}\sum_{k=i}^{m} r_{ijk}s_k t_{ij} =$

$= \sum_{k=i}^{m} (\sum_{j=1}^{n_i} t_{ij}r_{ijk})s_k = \sum_{k=i}^{m} z_{ik}s_k$, onde $z_{ik} = \sum_{j=1}^{n_i} t_{ij}r_{ijk}$,

para cada $k \in \{1,2,\ldots,m\}$. Portanto

$$(1 - z_i - z_{ii})s_i = \sum_{k=i+1}^{m} z_{ik}s_k \in S_{i+1} . \qquad (*)$$

Definimos agora z_{i+1} de modo a ser satisfeita a seguinte igualdade: $1 - z_{i+1} = (1 - z_i)(1 - z_i - z_{ii})$.

Então, considerando (*), temos:

$(1 - z_{i+1})S = (1 - z_i)S(1 - z_i - z_{ii}) \subset (1 - z_i - z_{ii})S_i \subset S_{i+1}$.

Resta-nos então mostrar que $z_{i+1} \in t(S)$. Para tal, bastanos observar que

$1 - z_{i+1} = (1 - z_i)(1 - z_i - z_{ii}) = 1 - 2z_i - z_{ii} + z_i^2 + z_i z_{ii}$ e

então $z_{i+1} = 2z_i + z_{ii} - z_i^2 - z_i z_{ii} \in t(S)$.

Então concluimos: $(1 - z_{m+1})S \subset S_{m+1} = 0$ ou seja $r = z_{m+1}$ satisfaz $(1 - r)S = 0$ e $r \in t(S)$.

Observemos agora que R é um R-módulo projetivo. Além disso, ficou provado acima que a seqüência de

R-módulos $S \xrightarrow{t} R \to 0$ é exata. Logo, tal seqüência cinde e R é um R-somando direto de S . □

Corolário 1.6:

Seja S uma extensão de Galois de R , com grupo de Galois G . Então:

(i) se T é uma R-álgebra comutativa então $T \otimes S$ é uma extensão de Galois de T com grupo de Galois G , onde G age linearmente em $T \otimes S$ via $\sigma.(t \otimes s) = t \otimes \sigma(s)$, para cada $t \in T$, $s \in S$, $\sigma \in G$;

(ii) o posto do R-módulo S é igual à ordem de G .

Prova:

(i) É fácil ver que G opera em $T \otimes S$. Além disso, sendo R um R-somando direto de S , é claro que $T \otimes S$ é uma T-álgebra.

Sejam $x_1, \ldots, x_n, y_1, \ldots, y_n \in S$ um sistema G-Galois de coordenadas; então os elementos $1 \otimes x_1, \ldots, 1 \otimes x_n$, $1 \otimes y_1, \ldots, 1 \otimes y_n \in T \otimes S$ são tais que, para cada $\sigma \in G$,

$$\sum_{i=1}^{n} (1 \otimes x_i)\sigma(1 \otimes y_i) = \sum_{i=1}^{n} (1 \otimes x_i)(1 \otimes \sigma(y_i)) = (1 \otimes \sum_{i=1}^{n} x_i \sigma(y_i)) =$$

$$= 1 \otimes \delta_{1\sigma} = \delta_{1\sigma} \quad .$$

Então, para completar a prova, resta-nos mostrar que $(T \otimes S)^G = T$.

Se t é um elemento de T, então $t = t \otimes 1$, e, para cada $\sigma \in G$, $\sigma(t \otimes 1) = t \otimes \sigma(1) = t \otimes 1 = t$. Logo, $T \subset (T \otimes S)^G$. Seja agora $u \in (T \otimes S)^G$, e seja $c \in S$ tal que $t(c) = 1$. Então $\sum_{\sigma \in G} \sigma(1 \otimes c) = \sum_{\sigma \in G} 1 \otimes \sigma(c) = 1 \otimes \sum_{\sigma \in G} \sigma(c) =$

$= 1 \otimes 1$. Assim, se $u(1 \otimes c) = \sum_{i=1}^{k} t_i \otimes s_i \in T \otimes S$, temos que

$$u = u(1 \otimes 1) = u\left[\sum_{\sigma \in G} \sigma(1 \otimes c)\right] = \sum_{\sigma \in G} \sigma[u(1 \otimes c)] = \sum_{\sigma \in G} \sigma\left(\sum_{i=1}^{n} t_i \otimes s_i\right) =$$

$$= \sum_{i=1}^{K} t_i \otimes \sum_{\sigma \in G} \sigma(s_i) = \sum_{i=1}^{K} t_i \otimes t(s_i) = \sum_{i=1}^{K} t_i t(s_i) \otimes 1 =$$

$$= \sum_{i=1}^{K} t_i t(s_i) \in T,$$ onde $t(s_i)$ denota a função traço aplicada a $s_i \in S$. Assim, $(T \otimes S)^G = T$.

(ii) É fácil ver que $\mathrm{Hom}_R(S,S)$ é um R-módulo finitamente gerado e projetivo. Além disso, as R-álgebras $\mathrm{Hom}_R(S,S)$ e D são isomorfas, conforme 1.4 (c).

Suponhamos primeiro que R é um anel local. Sabemos então que $\mathrm{Hom}_R(S,S)$ e S são R-módulos livres. Assim,

$[\mathrm{posto}_R\ S]^2 = \mathrm{posto}_R[\mathrm{Hom}_R(S,S)] = \mathrm{posto}_R\ D = m\ \mathrm{posto}_R\ S$, onde m é a ordem de G. Logo, $\mathrm{posto}_R\ S = m$.

Suponhamos agora que R é arbitrário e seja P um ideal primo de R. Então sabemos que R_P é uma R-álgebra comutativa, e G opera em $R_P \otimes S \simeq S_P$. Então, por (i),

temos que S_P é uma extensão de Galois de R_P, com grupo de Galois G. Logo, sendo R_P um anel local, já sabemos que $m = \text{POSTO}_{R_P}(S_P) = \text{POSTO}_{R_P}(R_P \otimes S)$. Ou seja, para qualquer ideal primo P de R, o P-posto do R-módulo S é m. Logo, concluimos que o posto do R-módulo S existe e é igual a m, a ordem do grupo G. □

§ 2 - TEOREMA FUNDAMENTAL DA TEORIA DE GALOIS PARA ANÉIS

Queremos agora provar o resultado que generaliza o Teorema Fundamental de Teoria de Galois para Corpos. No entanto, para que tal resultado seja válido também para anéis com idempotentes próprios, introduzimos a seguinte definição:

Seja S uma extensão de Galois de R com grupo de Galois G e seja T um subanel de S. Dizemos que T é G-FORTE se a restrição a T de dois quaisquer elementos de G são homomorfismos iguais ou fortemente distintos de T em S. É fácil ver que, se S não possui idempotentes próprios, então qualquer subanel de S é G-forte.

Teorema 2.1:

Seja S uma extensão de Galois de R com grupo de Galois G. Sejam H um subgrupo de G e

$T = S^H$. Então:

(i) S é uma extensão de Galois de T , com grupo de Galois H ;

(ii) T é uma R-álgebra separável, e G-forte;

(iii) H é o conjunto de todos os elementos de G que deixam T fixo, i.e., $H = \{\sigma \in G \mid \sigma_{|T} = id_T\}$.

Além disso, se H é um subgrupo normal de G , então T é uma extensão de Galois de R com grupo de Galois isomorfo a $G/_H$.

Prova:

Sejam $x_1,\ldots,x_n,y_1,\ldots,y_n \in S$ um sistema G-Galois de coordenadas. Então sabemos que, para cada $\sigma \in G$, $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1\sigma}$. Em particular, esta igualdade é verificada para todo $\sigma \in H$. Logo, S é uma extensão galoisiana de $S^H = T$, donde concluimos que (i) é verificada. Assim, como conseqüência de (i), S é um T-módulo finitamente gerado e projetivo. Se $a_1,\ldots,a_k \in S$ e $f_1,\ldots,f_k \in \mathrm{Hom}_T(S,T)$ são coordenadas projetivas do T-módulo S , então é fácil ver que os elementos $a_i \otimes a_j \in S$ e $f_i \otimes f_j \in \mathrm{Hom}_{T\otimes T}(S\otimes S , T\otimes T)$ são tais que $\sum_{i,j=1}^{k} (f_i \otimes f_j)(x\otimes y)(a_i \otimes a_j) = (x\otimes y)$, para cada $x\otimes y \in S\otimes S$. Logo, $S\otimes S$ é um $T\otimes T$-módulo projetivo.

Ainda, é claro que S é um $S \otimes S$-módulo projetivo e, portanto, é um $T \otimes T$-módulo projetivo. Então, sendo T um T-somando direto de S, temos que T é também um $T \otimes T$-somando direto de S e, portanto, T é um $T \otimes T$-módulo projetivo, ou seja, T é uma R-álgebra separável.

Antes de mostrarmos que T é G-forte, provamos parte de (iii).

Seja H' o subgrupo de G formado pelos automorfismos em G que deixam T fixo. Queremos mostrar que $H' = H$. É claro que $H' \supset H$, já que $T = S^H$. Portanto, $S^{H'} \subset S^H = T$, como é fácil verificar. Além disso, podemos observar que $S^{H'} = \{s \in S \mid \forall\, \zeta \in H',\ \zeta(s) = s\} \supset T$. Logo, $S^H = T = S^{H'}$, e então, por (i), S é também uma extensão de Galois de T com grupo de Galois H'. Sejam m e m' as ordens de H e H', respectivamente. Então, por 1.4 (e), os homomorfismos $h : S \otimes_T S \to E_H$ e $h' : S \otimes_T S \to E_{H'}$ são isomorfismos de S-álgebras. Além disso, E_H e $E_{H'}$ são S-módulos livres, gerados, respectivamente, por m e m' elementos. Logo, $E_H \simeq S \otimes_T S \simeq E_{H'}$ implica $m = m'$, ou seja, $H = H'$.

Para mostrar que T é G-forte, façamos, primeiro a seguinte observação. Como S é extensão galoisiana de T com grupo de Galois H, por 1.6, existe $c \in S$ tal que $\sum_{\zeta \in H} \zeta(c) = 1$. Por outro lado, sabe

mos que existem elementos $x_1,\ldots,x_n,y_1,\ldots,y_n \in S$ tais que, para cada $\sigma \in G$, $\sum_{i=1}^{n} x_i\sigma(y_i) = \delta_{1\sigma}$. Então, definindo $x_i' = \sum_{\rho \in H} \rho(x_i c)$ e $y_i' = \sum_{\zeta \in H} \zeta(y_i)$ $(i=1,2,\ldots,n)$, é claro que $x_i', y_i' \in S^H = T$. Além disso, se $\sigma \in H$, $\sum_{i=1}^{n} x_i'\sigma(y_i') =$

$= \sum_{\zeta,\rho \in H} \sum_{i=1}^{n} \rho(x_i c)\sigma\zeta(y_i) = \sum_{\zeta,\rho\in H} \rho(c) \sum_{i=1}^{n} \rho(x_i)\sigma\zeta(y_i) =$

$= \sum_{\rho \in H} \rho(c) = 1$. Ainda, se $\sigma \notin H$, de maneira análoga podemos mostrar que $\sum_{i=1}^{n} x_i'\sigma(y_i') = 0$, já que nunca ocorre $\rho = \sigma\zeta$, (pois do contrário teríamos $\sigma = \rho\zeta^{-1} \in H$, uma contradição). Logo, resumindo: $x_i', y_i' \in T$ $(i=1,2,\ldots,n)$ e são tais que, para cada $\sigma \in G$, $\sum_{i=1}^{n} x_i'\sigma(y_i') = \delta_{H\sigma}$, onde $\delta_{H\sigma} = 1$ se σ é um elemento de H e $\delta_{H\sigma} = 0$, caso contrário.

Suponhamos então que σ e ζ são dois elementos de G tais que $\zeta|_T \neq \sigma|_T$, e mostremos que tais homomorfismos de T em S são fortemente distintos. Seja $t' \in T$ tal que $\zeta(t') \neq \sigma(t')$. Então $t' \neq \zeta^{-1}\sigma(t')$, ou seja, $\zeta^{-1}\sigma \notin H$. Se $e \in S$ é um idempotente de S tal que, para cada $t \in T$, $\zeta(t)e = \sigma(t)e$, vejamos que, neste caso, $e = 0$. De fato, aplicando ζ^{-1} na igualdade anterior, temos $t\zeta^{-1}(e) = \zeta^{-1}\sigma(t)\zeta^{-1}(e)$, para cada $t \in T$.

Em particular, se $t = y_i'$, vem que $y_i'\zeta^{-1}(e) = \zeta^{-1}\sigma(y_i')\zeta^{-1}(e)$, e portanto,

$$\zeta^{-1}(e) = \sum_{i=1}^{n} x_i'y_i'\zeta^{-1}(e) = \left[\sum_{i=1}^{n} x_i'\zeta^{-1}\sigma(y_i')\right]\zeta^{-1}(e) = 0$$, já que

$\zeta^{-1}\sigma \notin H$. Logo, $e = 0$, o que mostra que T é G-forte.

Suponhamos agora que H é um subgrupo normal de G . Os automorfismos de S pertencentes a G induzem, através da restrição a T , automorfismos de T . De fato, para cada $\sigma \in G$, $t \in T$, $\zeta \in H$,

$\zeta(\sigma(t)) = (\sigma\sigma^{-1}\zeta\sigma)(t) = \sigma(t)$, já que $\sigma^{-1}\zeta\sigma \in H$, ou seja, $\sigma(t) \in S^H = T$. Portanto, $\sigma|_T$ é um automorfismo de T .

Consideremos agora o grupo quociente $G/_H$, e seja X uma classe de tal grupo, que contém os elementos $\sigma, \zeta \in G$. Então sabemos que $\sigma\zeta^{-1} \in H$, ou seja, $\sigma\zeta^{-1}(t) = t$, para cada $t \in T$, ou ainda, $\sigma(t) = \zeta(t)$. Desta observação podemos concluir que o grupo $G/_H$ pode ser considerado como um grupo de automorfismos de T da seguinte maneira: a cada classe X do grupo quociente $G/_H$, fazemos corresponder o automorfismo $\sigma_X = \sigma|_T$, onde σ é elemento arbitrário de G tal que $\sigma \in X$. Desta maneira, é fácil ver que o grupo $G/_H$ age fielmente em T .

Mostremos então que $T^{G/_H} = R$. É claro que $T^{G/_H} \supset R$, já que todo automorfismo σ_X é restrição de um elemento de G . Se $t \in T^{G/_H}$, para cada $\sigma \in G$, $t = \sigma_X(t) = \sigma(t)$,

ou seja, t é também um elemento de $S^G = R$. Logo, $T^{G/H} \subset R$.

Finalmente, considerando novamente os elementos $x_i', y_i' \in T$ tais que $\sum_{i=1}^{n} x_i' \sigma(y_i') = \delta_{H\sigma}$, para cada $\sigma \in G$, podemos observar que, se $\sigma_X = id_T$ (ou seja, $\sigma \in H$), então $\sum_{i=1}^{n} x_i' \sigma_X(y_i') = 1$ e, se $\sigma_X \neq id$, então $\sum_{i=1}^{n} x_i' \sigma_X(y_i') = 0$, o que completa a prova. □

Estabelecemos agora uma recíproca para o teorema acima.

Teorema 2.2:

Sejam S uma extensão de Galois de R com grupo de Galois G e T uma R-subálgebra separável de S que é G-forte como subanel de S . Se H é o subgrupo de G formado pelos elementos que deixam fixo T , então $T = S^H$.

Prova:

É claro que $S^H \supset T$. Resta-nos então mostrar que $S^H \subset T$. Façamos antes algumas observações.

Sabemos, por 1.6, que $S \otimes S$ é uma extensão de Galois de S com grupo de Galois G , onde G age em $S \otimes S$ da seguinte maneira: $\sigma.(s \otimes s') = s \otimes \sigma(s')$, para cada $s \otimes s' \in S \otimes S$. Mas, sendo S uma extensão de Galois de R ,

existe um isomorfismo de S-álgebras $h : S \otimes S \to E = \bigoplus_{\sigma \in G} S.v_\sigma$. Assim, E é uma extensão de Galois de S com grupo de Galois G , onde G opera em E através da igualdade $(\zeta.g)(\sigma) = g(\sigma\zeta)$, para cada $g \in E$, $\sigma, \zeta \in G$, como pode-se ver facilmente.

Como T é um subanel de S e como o functor $S \otimes \_$ é exato, é fácil ver que $S \otimes T$ é um subanel de $S \otimes S$. Além disso, sendo h um isomorfismo, podemos identificar $S \otimes T$ com sua imagem $h(S \otimes T)$.

Mostremos agora que E^H é um subconjunto de $h(S \otimes T)$. Antes, porém, consideremos o conjunto quociente $G/_H = \{\sigma_i H\}_{i=1}^r$. POdemos observar que g é um elemento de E^H se e só se $\zeta g = g$, para cada $\zeta \in H$, ou seja, $g(\sigma) = \zeta.g(\sigma) = g(\sigma\zeta)$, para cada $\sigma \in G$. Mas isto é equivalente ao fato de que cada elemento de E^H é constante sobre cada classe lateral de $G/_H$.

Reciprocamente se $g \in E$ é constante sobre cada classe lateral σH , com $\sigma \in G$, então, para cada $\zeta_1, \zeta_2 \in H$, sabemos que $g(\sigma\zeta_1) = g(\sigma\zeta_2)$. Em particular, se $\zeta_2 = 1_G$, observamos que $(\zeta_1.g)(\sigma) = (1_G.g)(\sigma) = g(\sigma)$, para cada $\zeta_1 \in H$, $\sigma \in G$, ou seja, $g \in E^H$. Concluimos, assim, que E^H é formado por todos os elementos de E que são constantes sobre cada classe lateral determinada pelo subgrupo H .

Agora, para cada $i \in \{1,2,\ldots,r\}$, definimos um homomorfismo de S-álgebras $f_i : E \to S$ por $f_i(g) = g(\sigma_i)$,

para cada $g \in E$. Como $h(S \otimes T)$ é uma S-subálgebra de $h(S \otimes S) = E$, podemos considerar as restrições de cada f_i à subálgebra $h(S \otimes T)$, que vamos continuar denotando por f_i $(i=1,2,\ldots,r)$.

Mostremos então que tais restrições são homomorfismos dois a dois fortemente distintos. Sejam $i,j \in \{1,2,\ldots,r\}$, com $i \neq j$, e seja $e \in S$ um idempotente de S . Sendo i e j distintos, as classes laterais $\sigma_i H$ e $\sigma_j H$ são também distintas, ou seja, $\sigma_i|_T \neq \sigma_j|_T$. Portanto, como T é G-forte, concluimos que estas restrições $\sigma_i|_T$ e $\sigma_j|_T$ são homomorfismos de T em S fortemente distintos. Assim, existe um elemento $t \in T$ tal que $\sigma_i(t)e \neq \sigma_j(t)e$. Logo, podemos escrever $f_i[h(1 \otimes t)]e =$

$= [h(1 \otimes t)](\sigma_i)e = \sigma_i(t)e \neq \sigma_j(t)e = [h(1 \otimes t)](\sigma_j)e = f_j[h(1 \otimes t)]e$.

Observemos agora que $S \otimes T$ é uma S-álgebra separável e, através da restrição do isomorfismo h a $S \otimes T$, concluimos que $h(S \otimes T)$ é também uma S-álgebra separável. Portanto, aplicando II.2.21 (com referência aos homomorfismos de S-álgebras $f_i : h(S \otimes T) \to S)$, podemos determinar únicos idempotentes $\omega_i \in h(S \otimes T)$ $(i=1,2,\ldots,r)$, tais que $f_i(\omega_j) = \delta_{ij}$, $\omega_i \omega_j = \delta_{ij}$ $(i,j \in \{1,2,\ldots,r\})$ e $f_i(x)\omega_i = x\omega_i$, para cada $x \in h(S \otimes T)$.

Vamos mostrar que este conjunto $\{\omega_1,\ldots,\omega_r\}$ constitui uma base para o S-módulo livre E^H . Para tal,

é suficiente mostrarmos que $\omega_i \in E^H$, para cada $i \in \{1,2,\ldots,r\}$ e $E^H \subset \sum_{i=1}^{r} S.\omega_i$.

Observemos, no entanto, que $h(S \otimes T) \subset E^H$. De fato, cada elemento de $h(S \otimes T)$ é constante sobre cada classe lateral, pois, para todo $\sigma \in G$, $\zeta \in H$, $s \otimes t \in S \otimes T$, $[h(s \otimes t)](\sigma\zeta) = s\sigma\zeta(t) = s\sigma(t) = h(s \otimes t)(\sigma)$. Logo, em particular, cada ω_i é um elemento de E^H $(i=1,2,\ldots,r)$.

Suponhamos agora que g é um elemento de E^H . Então, como $\omega_i(\sigma_j) = f_j(\omega_i) = \delta_{ij}$, para cada $j \in \{1,2,\ldots,r\}$ temos que $[\sum_{i=1}^{r} g(\sigma_i)\omega_i](\sigma_j) = \sum_{i=1}^{r} g(\sigma_i)\omega_i(\sigma_j) = g(\sigma_j)$. Além disso, como $\sum_{i=1}^{r} g(\sigma_i)\omega_i \in E^H$, tal elemento é constante sobre cada classe lateral. Como g também satisfaz esta propriedade, concluimos que $\sum_{i=1}^{r} g(\sigma_i)\omega_i = g$. Assim,

$$E^H = \sum_{i=1}^{r} S.\omega_i \subset h(S \otimes T) .$$

Portanto, aplicando o isomorfismo inverso h^{-1}, temos que $S \otimes T \supset h^{-1}(E^H) = h^{-1}([h(S \otimes S)]^H)$. Mas é fácil ver que $[h(S \otimes S)]^H = h(S \otimes S^H)$ e, portanto, $S \otimes T \supset h^{-1}[h(S \otimes S^H)] = S \otimes S^H$.

Aplicando na relação anterior o homomorfismo $t \otimes id_S \in \mathrm{Hom}_R(S \otimes S , S)$, vem que

$$S^H \simeq R \otimes S^H = (t \otimes id_S)(S \otimes S^H) \subset (t \otimes id_S)(S \otimes T) = R \otimes T \simeq T \text{ , ou}$$

seja, $S^H \subset T$, o que completa a prova. □

Com estes dois últimos resultados, podemos obter o teorema fundamental. Se S é uma extensão de Galois de R com grupo de Galois G , então podemos associar a cada R-subálgebra separável e G-forte T de S um subgrupo de G , a saber, $H_T = \{\sigma \in G \mid \sigma|_T = id_T\}$. Reciprocamente, se H é um subgrupo de G , podemos fazer corresponder a H uma R-subálgebra separável e G-forte T de S , isto é, $T = S^H$. Esta correspondência entre as R-subálgebras de S que são separáveis e G-fortes e os subgrupos do grupo de Galois G é chamada CORRESPONDÊNCIA DE GALOIS.

Resumindo, os dois últimos resultados, temos a seguinte generalização do Teorema Fundamental da Teoria de Galois para corpos.

Teorema 2.3:

Seja S uma extensão de Galois de R , com grupo de Galois G . Então:

(i) a correspondência de Galois é uma correspondência 1-1 entre as R-subálgebras separáveis e G-fortes de S e os subgrupos de G . Esta correspondência preserva a ação de G no seguinte sentido: se σ é um elemento de G e T uma R-subálgebra separável e G-forte de S , então $H_{\sigma(T)} = \sigma H_T \sigma^{-1}$.

(ii) um subgrupo H de G é normal em G se e só se o subanel S^H é tranformado sobre si mesmo por cada elemento de G . Neste caso, S^H é uma extensão de

Galois de R , com grupo de Galois $G/_H$.

Prova:

É fácil ver que a correspondência de Galois é biunívoca, pelos dois últimos teoremas. Vejamos então que esta correspondência preserva a ação de G .

Sejam $\sigma \in G$ e T uma R-subálgebra separável e G-forte de S . Então, através da restrição $\sigma|_T$, é claro que $\sigma(T)$ é também uma R-álgebra separável e G-forte. Observemos então que

$H_{\sigma(T)} = \{\zeta \in G \mid \zeta|_{\sigma(T)} = id_{\sigma(T)}\} = \{\zeta \in G \mid \forall t \in T \ , \ \sigma^{-1}\zeta\sigma(t) = t\}$,

e $\sigma H_T \sigma^{-1} = \{\sigma\rho\sigma^{-1} \mid \rho|_T = id_T\}$. Mas se $\gamma = \sigma\rho\sigma^{-1} \in \sigma H_T \sigma^{-1}$ então $\rho = \sigma^{-1}\gamma\sigma \in H_T$, ou seja, para cada $t \in T$,

$t = \rho(t) = (\sigma^{-1}\gamma\sigma)(t)$. Logo, $\gamma(\sigma(t)) = \sigma(t)$, para cada $t \in T$. Assim, $\sigma H_T \sigma^{-1} \subset H_{\sigma(T)}$. Ainda, é fácil ver que $H_{\sigma(t)} \subset \sigma H_T \sigma^{-1}$, e então (i) está provado.

Finalmente, seja $T = S^H$. Então H é um subgrupo normal de G se e só se $\sigma^{-1}H\sigma = H$, para todo $\sigma \in G$, ou equivalentemente, $H_{\sigma(T)} = H$, para cada $\sigma \in G$. Aplicando a correspondência biunívoca, a condição anterior equivale a $\sigma(T) = S^{H_{\sigma(T)}} = S^H = T$, o que completa a prova, por 2.1, parte (iii). □

CAPÍTULO IV

POLINÔMIOS SEPARÁVEIS

O principal objetivo deste capítulo é estudar as álgebras separáveis e comutativas sobre anéis comutativos. Em particular, introduzimos o conceito de polinômio separável sobre um anel comutativo. O principal resultado deste trabalho é precisamente o teorema 2.8 , que caracteriza tais polinômios.

O conteúdo deste capítulo se baseia nos trabalhos de Janusz [13], Elkins [8] e Nagahara [18] e [19] .

Continuamos aqui a supor que todos os anéis têm unidade e são comutativos. Além disso, $\otimes$ significa $\otimes_R$.

Na primeira seção deste capítulo apresentamos resultados e conceitos introdutórios para a segunda seção, onde então é abordado o problema essencial.

§ 1 . INTRODUÇÃO

Iniciamos introduzindo o conceito de álgebra

fortemente separável sobre um anel comutativo R . Uma R-álgebra A é dita FORTEMENTE SEPARÁVEL SOBRE R (ou, simplesmente, R-FORTEMENTE SEPARÁVEL) se A é R-separável e um R-módulo projetivo e finitamente gerado.

O teorema abaixo nos mostra a importância da função traço (definida em I.3) no estudo das álgebras fortemente separáveis.

Teorema 1.1:

Seja S uma R-álgebra que é finitamente gerada e projetiva como R-módulo. Então S é R-separável se e só se existem uma aplicação $t \in \mathrm{Hom}_R(S,R)$ e elementos $x_1,\ldots,x_n,y_1,\ldots,y_n \in S$ tais que

(i) $\sum_{j=1}^{n} x_j y_j = 1$

(ii) $\sum_{j=1}^{n} x_j . t(y_j x) = x$, para cada $x \in S$.

Neste caso, o homomorfismo t é a aplicação traço de S em R .

Prova:

Façamos inicialmente algumas observações. Sejam $a_1,\ldots,a_m \in S$ e $f_1,\ldots,f_m \in \mathrm{Hom}_R(S,R)$ coordenadas projetivas do R-módulo S e seja t a aplicação traço de S em R , isto é, $t(s) = \sum_{i=1}^{m} f_i(s\, a_i)$, para cada $s \in S$.

Observemos que dado um R-homomorfismo $f : S \to R$,

podemos considerar a aplicação $F = \psi_0 (id_S \otimes f)$, onde $\psi: S \otimes R \to S$ é o isomorfismo natural dado por $\psi(s \otimes r) = s.r$, para cada $s \otimes r \in S \otimes R$. Portanto, $F : S \otimes S \to S$ é dada por $F(s \otimes s') = s.f(s')$, para cada $s \otimes s' \in S \otimes S$, e é um S-homomorfismo à esquerda, como é fácil verificar.

É fácil ver ainda que $1 \otimes a_1, \ldots, 1 \otimes a_m \in S \otimes S$ e $F_1 = \psi_0 (1 \otimes f_1), \ldots, F_m = \psi_0 (1 \otimes f_m)$ são coordenadas projetivas para $S \otimes S$ como S-módulo à esquerda. Logo, $S \otimes S$ é um S-módulo finitamente gerado e projetivo. Ainda, se T denota o S-homomorfismo induzido pela função traço $t : S \to R$, temos:

$$T(s \otimes s') = s.t(s') = s. \sum_{i=1}^{m} f_i(s'a_i) = \sum_{i=1}^{m} s.f_i(s'a_i) .$$

Suponhamos agora que S é R-separável e seja $e = \sum_{j=1}^{n} x_j \otimes y_j \in S \otimes S$ um idempotente de separabilidade. Então $\sum_{j=1}^{n} x_j y_j = 1$. Além disso, para cada $s \in S$, $\sum_{j=1}^{n} s\, x_j \otimes y_j = \sum_{j=1}^{n} x_j \otimes y_j s$. Portanto, para cada $f \in \mathrm{Hom}_R(S,R)$,

$$\sum_{j=1}^{n} s\, x_j \otimes f(y_j) = (1 \otimes f)\Big[\sum_{j=1}^{n} s\, x_j \otimes y_j\Big] = (1 \otimes f)\Big[\sum_{j=1}^{n} x_j \otimes y_j s\Big] = \sum_{j=1}^{n} x_j \otimes f(y_j s) ,$$

ou ainda, aplicando o homomorfismo contração, $\sum_{j=1}^{n} s\, x_j . f(y_j) = \sum_{j=1}^{n} x_j . f(y_j s)$, para cada $s \in S$. Então, se $x \in S$, podemos escrever

$$T[(x\otimes 1)e] = T[\sum_{j=1}^{n} x\,x_j\otimes y_j] = \sum_{j=1}^{n} x\,x_j.t(y_j) = \sum_{i=1}^{m} x_i \sum_{j=1}^{n} x_j.f_i(y_j a_i) =$$

$$= \sum_{i=1}^{m} x \sum_{j=1}^{n} a_i x_j.f_i(y_j) = \sum_{j=1}^{n} x\,x_j \sum_{i=1}^{m} a_i.f_i(y_j) =$$

$$= x \sum_{j=1}^{n} x_j y_j = x\ .$$

Por outro lado,

$$T[(x\otimes 1)e] = T[(1\otimes x)e] = T[\sum_{j=1}^{m} x_j\otimes y_j x] = \sum_{j=1}^{n} x_j.t(y_j x)\ .$$

Portanto, para cada $x\in S$, $\sum_{j=1}^{n} x_j.t(y_j x) = x$.

Para mostrar a recíproca, suponhamos que existem uma aplicação $t\in \mathrm{Hom}_R(S,R)$ e elementos $x_1,\ldots,x_n,y_1,\ldots,y_n \in S$ que satisfazem as condições (i) e (ii) do enunciado, e mostremos que o elemento $e = \sum_{j=1}^{n} x_j\otimes y_j \in S\otimes S$ é um idempotente de separabilidade para a R-álgebra S . Para tal, é suficiente mostrar que para cada $x\in S$, $\sum_{j=1}^{n} x\,x_j\otimes y_j = \sum_{j=1}^{n} x_j\otimes y_j x$.

De fato, se $x\in S$ então

$$\sum_{j=1}^{n} x_j\otimes y_j x = \sum_{j=1}^{n} x_j\otimes [\sum_{i=1}^{n} x_i t(y_i y_j x)] = \sum_{j=1}^{n} \sum_{i=1}^{n} x_j.\, t(y_i y_j x)\otimes x_i =$$

$$= \sum_{i=1}^{n} [\sum_{j=1}^{n} x_j t(y_j y_i x)]\otimes x_i = \sum_{i=1}^{n} y_i x\otimes x_i = \sum_{i=1}^{n} x y_i\otimes x_i\ .$$

Então se $x = 1$, obtemos $e = \sum_{j=1}^{n} x_j\otimes y_j = \sum_{j=1}^{n} y_j\otimes x_j$, e podemos escrever $(1\otimes x)e = (x\otimes 1)e$, para cada $x\in S$. Portanto, S é uma R-álgebra separável.

Antes de mostrarmos que esta aplicação t é na verdade a aplicação traço do R-módulo S, observemos que cada aplicação $t(y_i -) : S \to R$ dada por $t(y_i -)(x) = t(y_i x)$ é um homomorfismo de R-módulos, para cada $i \in \{1,2,\ldots,n\}$, como é fácil verificar. Além disso, levando em conta (ii), é claro que os elementos $x_1,\ldots,x_n$ e $t(y_1 -),\ldots,t(y_n -) \in \mathrm{Hom}_R(S,R)$ são coordenadas projetivas para o R-módulo S. Então, se tr denota a aplicação traço do R-módulo S, temos, para cada $x \in S$,

$tr(x) = \sum_{i=1}^{n} t(y_i -)(x x_i) = t\left[\sum_{i=1}^{n} y_i x x_i\right] = t(x)$, o que completa a prova. □

Para obter uma conseqüência do teorema acima, façamos algumas observações. Se S é uma R-álgebra, então podemos definir em $\mathrm{Hom}_R(S,R)$ uma estrutura de S-módulo à direita, da seguinte maneira: $(f.s)(x) = f(sx)$, para cada $x,s \in S$ e $f \in \mathrm{Hom}_R(S,R)$, como é fácil verificar. Além disso, é claro que se S é um R-módulo finitamente gerado e projetivo e se $t \in \mathrm{Hom}_R(S,R)$ é a aplicação traço de tal R-módulo, então $t.S$ é um S-submódulo de $\mathrm{Hom}_R(S,R)$. Ainda, nestas condições, se $x_1,\ldots,x_n \in S$ e $f_1,\ldots,f_n \in \mathrm{Hom}_R(S,R)$ são coordenadas projetivas de S sobre R então é fácil ver que $\mathrm{Hom}_R(S,R)$ é um R-módulo finitamente gerado e projetivo, a saber, $f = \sum_{i=1}^{n} f(x_i) f_i$, para cada $f \in \mathrm{Hom}_R(S,R)$.

Corolário 1.2:

Seja S uma R-álgebra que é projetiva e finitamente gerada como R-módulo. Então S é R-separável se e só se a aplicação traço $t : S \to R$ é um gerador livre do S-módulo à direita $\mathrm{Hom}_R(S,R)$.

Prova:

Suponhamos que S é uma R-álgebra fortemente separável, e sejam $x_1,\ldots,x_n,y_1,\ldots,y_n \in S$ elementos que satisfazem as condições (i) e (ii) do teorema anterior. Então, para cada $x \in S$, $f \in \mathrm{Hom}_R(S,R)$,

$f(x) = f(\sum_{i=1}^{n} x_i.t(y_i x)) = \sum_{i=1}^{n} t(y_i x) f(x_i) = t(\sum_{i=1}^{n} f(x_i).y_i x)$. Assim, pondo $a_f = \sum_{i=1}^{n} f(x_i).y_i$, temos que $f = t(a_f -) = t.a_f$, donde t gera o S-módulo $\mathrm{Hom}_R(S,R)$. Ainda, se $t.a$ é o homomorfismo nulo de $\mathrm{Hom}_R(S,R)$ (para algum $a \in S$) , então $a = \sum_{i=1}^{n} x_i t(a y_i) = 0$, e podemos concluir que $\mathrm{Hom}_R(S,R)$ é um S-módulo livre, com base $\{t\}$.

Reciprocamente, suponhamos que t é um gerador livre do S-módulo $\mathrm{Hom}_R(S,R)$ e denotemos por $x_1,\ldots,x_m$ e $f_1,\ldots,f_m \in \mathrm{Hom}_R(S,R)$ as coordenadas projetivas do R-módulo S . Sejam $y_1,\ldots,y_m \in S$ elementos tais que $f_i = t.y_i$, para cada $i \in \{1,2,\ldots,m\}$. Então, para cada $s \in S$, podemos escrever (utilizando a definição de função traço):

$$[t(1 - \sum_{i=1}^{m} x_i y_i)](s) = t[(1 - \sum_{i=1}^{m} x_i y_i)s] = t(s) - t(\sum_{i=1}^{m} x_i y_i s) =$$

$$= \sum_{i=1}^{m} f_i(s\,x_i) - t(\sum_{i=1}^{m} x_i y_i s) =$$

$$= \sum_{i=1}^{m} (t.y_i)(s\,x_i) - t(\sum_{i=1}^{m} x_i y_i s) =$$

$$= t(\sum_{i=1}^{m} y_i s\,x_i) - t(\sum_{i=1}^{m} x_i y_i s) = 0 \ .$$

Portanto, como t é livre sobre S em $\mathrm{Hom}_R(S,R)$, vem que $1 = \sum_{i=1}^{m} x_i y_i$.

Além disso, para cada $s \in S$, $s = \sum_{i=1}^{m} f_i(s)\,x_i = \sum_{i=1}^{m} t(y_i s)\,x_i$. Logo, pelo teorema anterior, S é R-separável. □

Proposição 1.3:

Seja S uma R-álgebra que é finitamente gerada e projetiva como R-módulo. Então:

(i) S é R-separável se e só se S_M é uma álgebra separável sobre R_M , para cada ideal maximal M de R ;

(ii) S é R-separável se e só se $S/_{M.S}$ é uma álgebra separável sobre $R/_M$, para cada ideal maximal M de R .

Prova:

Mostremos inicialmente (i). Para tal, consideremos a aplicação traço $t \in \mathrm{Hom}_R(S,R)$ do R-módulo finitamente gerado e projetivo S , e a inclusão canônica $t.S \hookrightarrow \mathrm{Hom}_R(S,R)$,

que é um homomorfismo de S-módulos (e, portanto, de R-módulos). Então, como $-\otimes R_M$ é um funtor exato, para cada ideal maximal M de R (ver I.4.4), a seqüência $0 \to t.S\otimes R_M \hookrightarrow \mathrm{Hom}_R(S,R)\otimes R_M$ é uma seqüência exata de módulos sobre $S\otimes R_M \simeq S_M$, como é fácil verificar. Ainda, sendo S um R-módulo finitamente gerado e projetivo, é claro que S_M é também um módulo finitamente gerado e projetivo sobre R_M. Seja t_M a aplicação traço de tal R_M-módulo.

É fácil ver que os S_M-módulos à direita $\mathrm{Hom}_R(S,R)\otimes R_M$ e $\mathrm{Hom}_{R_M}(S_M,R_M)$ são isomorfos, e que o correspondente por este isomorfismo do S_M-submódulo $t.S\otimes R_M$ é $t_M.S_M$. Assim, vemos que a inclusão $t.S \hookrightarrow \mathrm{Hom}_R(S,R)$ é um epimosfismo se e só se a inclusão $t_M.S_M \hookrightarrow \mathrm{Hom}_{R_M}(S_M,R_M)$ de S_M-módulos é um epimorfismo, para todo M, donde t é um gerador do S-módulo $\mathrm{Hom}_R(S,R)$ se e só se t_M é um gerador do S_M-módulo $\mathrm{Hom}_{R_M}(S_M,R_M)$, para cada ideal maximal M de R.

Mostremos agora que t é livre se e só se t_M é livre, para cada ideal maximal M de R. Suponhamos então que $t_M.s/_m = 0$, para algum $s/_m \in S_M$, e que t é livre em $\mathrm{Hom}_R(S,R)$. Como $m/_m$ é a unidade de S_M, vemos que $t_M.s/_1 = 0$, ou, equivalentemente, $t.s/_1 = 0$. Assim, existe $y \notin M$ tal que $t.sy = 0$. Mas como t é livre, segue-se que

$sy = 0$, ou ainda, $s/_m = 0$. Reciprocamente, se t_M é livre, para cada ideal maximal M de R e se $t.s = 0$ para algum $s \in S$, então $t.s/_1 = t_M.s/_1 = 0$. Assim, como t_M é livre, $s/_1 = 0$. Logo, para cada ideal maximal M de R , existe um elemento $y \notin M$ tal que $s \cdot y = 0$, donde segue que $s = 0$, como é fácil verificar.

O resto da prova de (i) é agora evidente, se levarmos em conta o corolário anterior.

De maneira análoga, utilizando novamente a função traço do R-módulo S e aplicando os métodos usuais da álgebra comutativa, obtém-se (ii). □

§ 2 - POLINÔMIOS SEPARÁVEIS

Nesta seção apresentamos caracterizações de polinômios separáveis sobre anéis comutativos arbitrários, e algumas conseqüências que derivam de tais resultados.

Em toda esta seção, $R[X]$ denota o anel de polinômios na indeterminada X e com coeficientes no anel comutativo (com unidade) R. Além disso, $\langle f(X)\rangle$ denota o ideal gerado pelo polinômio $f(X) \in R[X]$, e $x = X + \langle f(X)\rangle$ denota a classe de X módulo $f(X)$.

Façamos inicialmente algumas considerações gerais.

Seja $f(X) = X^n + r_{n-1}X^{n-1} + \ldots + r_1X + r_0 \in R[X]$ um polinômio mônico. Então é fácil verificar que o anel quociente $\overline{R} = R[X]/_{\langle f(X)\rangle}$ é uma R-álgebra que é livre e finitamente gerado como R-módulo, com base $1, x, x^2, \ldots, x^{n-1}$, onde $x = X + \langle f(X)\rangle$ denota a classe de X em $\overline{R}$. Isto é, $R[X]/_{\langle f(X)\rangle} = R.1 \oplus R.x \oplus \oplus R.x^2 \oplus \ldots \oplus R.x^{n-1} = R[x]$, onde $x^n = -r_{n-1}x^{n-1} - \ldots - r_1x - r_0$, e onde a operação externa é definida distributivamente por $r.(r_ix^i) = (rr_i)x^i$, para cada $r, r_i \in R$, $i \in \{0,1,\ldots,n-1\}$.

Um polinômio $f(X) \in R[X]$ é dito um POLINÔMIO SEPARÁVEL (SOBRE R) se ele é mônico e $R[X]/_{\langle f(X)\rangle}$ é uma R-álgebra separável. Mais adiante nesta seção, ficará claro que esta definição de polinômio (mônico) separável sobre um anel comutativo com unidade é uma generalização da noção de polinômio (mônico) separável sobre um corpo.

Seja A uma R-álgebra. Então é claro que um

polinômio $f(X) = X^n + r_{n-1}X^{n-1} + \ldots + r_0 \in R[X]$ pode ser considerado um polinômio pertencente a $A[X]$ se o identificarmos com o polinômio $1_A X^n + (r_{n-1}.1_A)X^{n-1} + \ldots + (r_0.1_A) \in A[X]$. Esta observação será útil mais adiante.

Neste primeiro resultado que passamos a mostrar, utilizamos a seguinte notação: se A é uma R-álgebra, G um grupo de automorfismos de A e T uma R-subálgebra de A , então $G|_T$ denota o conjunto dos elementos de G restritos à R-subálgebra T (i.e., $G|_T = \{\sigma|_T \mid \sigma \in G\}$).

Lema 2.1:

Seja A um anel extensão de R tal que $A^G = R$, para algum grupo G de automorfismos de A . Seja $a \in A$ um elemento tal que o conjunto $\{\sigma(a) \mid \sigma \in G\}$ é finito e $\sigma(a) - a$ é inversível em A , para cada $\sigma \in G$ que satisfaz $\sigma(a) \neq a$. Se $a_1, \ldots, a_n$ são todos os elementos distintos de $\{\sigma(a) \mid \sigma \in G\}$ e se $f(X) = (X - a_1)\ldots(X - a_n)$ então:

(i) $\prod_{i \neq j} (a_i - a_j) \in U(R)$;

(ii) o anel $R[a_1, \ldots, a_n]$ é uma extensão de Galois de R , com grupo de Galois $G|_{R[a_1, \ldots, a_n]}$;

(iii) $f(X) \in R[X]$ e as R-álgebras $R[X]/_{<f(X)>}$ e $R[a_1]$ são isomorfas;

(iv) $f(X)$ é um polinômio separável sobre R .

Prova:

Suponhamos que $a = a_1$. Então, por hipótese, $a_i - a_1 \in U(A)$, para cada $i \in \{2,3,\ldots,n\}$. Ainda, para cada $j \in \{1,2,\ldots,n\}$, existe $\sigma \in G$ tal que $\sigma(a_1) = a_j$. Então, se $\sigma(a_i) = a_k$, temos que $\sigma(a_i - a_1) = a_k - a_j \in U(A)$, para cada $i,j \in \{1,2,\ldots,n\}$, com $i \neq 1$. É fácil concluir daqui que $a_i - a_j \in U(A)$, para cada $i,j \in \{1,2,\ldots,n\}$ com $i \neq j$. Portanto, $u = \prod_{i \neq j} (a_i - a_j) \in U(A)$. Mostremos agora que $U \in U(R)$. De fato, para cada $\sigma \in G$, $\sigma(u) = \prod_{i \neq j} [\sigma(a_i) - \sigma(a_j)] = u$, pois σ permuta os elementos a_i . Então $u \in A^G = R$, e $\sigma(u^{-1}) = [\sigma(u)]^{-1} = u^{-1}$, ou seja, u^{-1} é também um elemento de $A^G = R$. Logo, $u \in U(R)$, o que completa a prova de (i).

Seja $T = R[a_1,\ldots,a_n]$. Se $\sigma \in G$ e $g = \sum b_{i_1\ldots i_n} a_1^{i_1}\ldots a_n^{i_n}$ é um elemento de T então $\sigma(g) = \sum b_{i_1\ldots i_n} [\sigma(a_1)]^{i_1}\ldots[\sigma(a_n)]^{i_n}$. Como σ permuta os a_i , vemos que $\sigma(g) \in T$. Logo, o conjunto $G|_T$ dos automorfismos de A restritos a T é realmente um grupo de automorfismos de T . Ainda, é fácil ver que $G|_T$ é um grupo finito de ordem não superior a $n!$. Mostremos então que T é uma extensão de Galois de R com grupo de Galois $G' = G|_T$.

Inicialmente, se $g \in T^{G'}$, então, para cada $\sigma \in G$, $g = \sigma|_T(g) = \sigma(g)$, ou seja, $g \in A^G = R$. Logo, $T^{G'} = R$.

Ainda, por (i), sabemos que $u = \prod_{i \neq j} (a_i - a_j) \in U(R)$, e então $u^{-1}[\prod_{i \neq j} (a_i - \sigma(a_j))] = \delta_{1_G,\sigma}$. Por indução sobre n , é fácil constatar que esta relação implica existirem elementos $u_1,\ldots,u_m,v_1,\ldots,v_m \in T$ tais que $\delta_{1_G,\sigma} = u^{-1}[\prod_{i \neq j} (a_i - \sigma(a_j))] = \sum_{i=1}^{m} u_i \sigma(v_i)$. Portanto, por III.1.4, está completa a prova de (ii).

Para mostrar (iii), observemos inicialmente que o polinômio $f(X) = (X - a_1)\ldots(X - a_n)$ é realmente um elemento de $R[X]$. De fato, $f(X) = X^n - \alpha_{n-1}X^{n-1} + \ldots + (-1)^{n-1}\alpha_1 X + (-1)^n \alpha_0$, onde cada α_i é uma função simétrica elementar dos a_i , isto é, $\alpha_{n-i} = \sum_{j_1 < \ldots < j_i} a_{j_1}\ldots a_{j_i} \in R[a_1,\ldots,a_n]$, para cada $i \in \{1,2,\ldots,n\}$. Então, para cada $\sigma \in G$, $\sigma(\alpha_{n-i}) = \sum_{j_1 < \ldots < j_i} \sigma(a_{j_1})\ldots\sigma(a_{j_i}) = \alpha_{n-i}$. Portanto, $\alpha_i \in A^G = R$, para cada $i \in \{1,2,\ldots,n\}$, donde $f(x) \in R[X]$.

Seja $\gamma : R[X] \to R[a_1]$ a aplicação definida por $\gamma[g(X)] = g(a_1)$, para cada $g(X) \in R[X]$. Então é fácil ver que γ é um epimorfismo de R-álgebras e, portanto, induz um isomorfismo entre $R[X]/_{\text{Ker}\,\gamma}$ e $R[a_1]$. Mostremos que $\text{Ker}\,\gamma = \langle f(X) \rangle$. Se $h(X) = \sum_{i=0}^{m} b_i X^i \in \text{Ker}\,\gamma$ então $0 = \gamma(h(X)) = h(a_1)$ e, portanto, para cada $j \in \{1,2,\ldots,m\}$ e para cada $\sigma \in G$ tal que $\sigma(a_1) = a_j$, $0 = \sigma(h(a_1)) = \sum_{i=0}^{m} b_i [\sigma(a_1)]^i = \sum_{i=0}^{m} b_i a_j^{\,i} = h(a_j)$. Logo, a_j é raiz de $h(X)$, para cada $j \in \{1,2,\ldots,n\}$. Então

$h(X) = (X - a_1)q_1(X)$, para algum $q_1(X) \in A[X]$. Ainda, como $a_2 - a_1 \in U(A)$ e $h(a_2) = 0$, temos $q_2(a_2) = 0$. Ou seja, $h(X) = (X - a_1)(X - a_2)q_2(X)$, para algum $q_2(X) \in A[X]$. Continuando este raciocínio, chega-se a $h(X) = (X-a_1)(X-a_2)\ldots(X-a_n)q_n(X) = f(X)q_n(X)$, para algum $q_n(X) \in A[X]$. Ainda, como $h(X), f(X) \in R[X]$ e $f(X)$ é mônico, é fácil ver que $q_n(X) \in R[X]$. Logo, $h(X) \in \langle f(X) \rangle$. Como a inclusão contrária é evidente, a prova de (iii) fica completa.

Mostremos agora que $f(X)$ é um polinômio separável sobre R , i.e., que $R[X]/_{\langle f(X) \rangle} \simeq R[a_1]$ é uma R-álgebra separável. Consideremos novamente a R-álgebra $T = R[a_1,\ldots,a_n]$. Seja M um T-módulo livre à esquerda, de base $\{d_1,\ldots,d_n\}$, ou seja, $M = T.d_1 \oplus \ldots \oplus T.d_n$. Definimos em M uma estrutura de $R[a_1]$-módulo à direita induzida por $d_i.g(a_1) = g(a_i).d_i$, para cada $i \in \{1,2,\ldots,n\}$ e para cada $g(a_1) \in R[a_1]$. Seja $e = d_1 + \ldots + d_n \in M$. Vejamos que $M = T.e.R[a_1]$.

Observemos inicialmente que, para cada $i \in \{1,2,\ldots,n\}$, $e.a_1^i = \sum_{j=1}^{n} d_j.a_1^i = \sum_{j=1}^{n} a_j^i.d_j$, ou seja, na forma matricial,

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \vdots & & & \\ a_1^{n-1} & a_2^{n-1} & \ldots & a_n^{n-1} \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \\ \cdot \\ \cdot \\ \cdot \\ d_n \end{bmatrix} = \begin{bmatrix} e \\ e.a_1 \\ e.a_1^2 \\ \cdot \\ \cdot \\ e.a_1^{n-1} \end{bmatrix} \qquad (*)$$

Por outor lado, a matriz $A = \begin{bmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ \vdots & & & \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{bmatrix}$

é inversível. De fato, tal matriz é uma matriz de Vandermonde, cujo determinante vale $\pm \prod_{i<j} (a_i - a_j) \in T$. Além disso, este determinante é um fator de $\prod_{i\neq j} (a_i - a_j)$, que sabemos ser inversível em R . Então é fácil verificar que $\pm \prod_{i<j} (a_i - a_j) \in U(T)$. Assim, a matriz A é inversível em $M_{n\times n}(T)$, e podemos obter

$$\begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{bmatrix} = A^{-1} \begin{bmatrix} e \\ e.a_1 \\ \vdots \\ e.a_1^{n-1} \end{bmatrix}$$

. Logo, cada d_i $(i=1,2,\dots,n)$ pode ser escrito como combinação linear em T dos elementos $e, e.a_1, \dots, e.a_1^{n-1}$, donde segue que $d_i \in T.e.R[a_1]$, para cada $i \in \{1,2,\dots,n\}$. Assim, $M = T.e.R[a_1]$.

Consideremos agora a aplicação $\psi : T\otimes R[a_1] \to M$, dada por $\psi[\sum_{i=1}^{s} t_i \otimes g_i(a_1)] = \sum_{i=1}^{s} t_i.e.g_i(a_1)$, para cada $\sum_{i=1}^{s} t_i \otimes g_i(a_1) \in T\otimes R[a_1]$. É fácil ver que ψ está bem definida e é um homomorfismo de T-$R[a_1]$-bimódulos, e, pela observação feita acima, ψ é sobrejetora. Ainda, é fácil constatar que $\{1\otimes 1, 1\otimes a_1, \dots, 1\otimes a_1^{n-1}\}$ é uma base do T-módulo $T\otimes R[a_1]$. Além disso, o conjunto $\{e.a_1^i\}_{i=0}^{n-1}$ é uma base de M , pela relação (*). Então, como $\psi(1\otimes a_1^i) = 1.e.a_1^i = e.a_1^i$, para cada $i \in \{0,1,\dots,n-1\}$,

vemos que ψ leva base em base, ou seja, $M \simeq T \otimes R[a_1]$.

Portanto, $T \otimes R[a_1] \simeq T^{(n)}$ como T-módulos. É fácil ver ainda que tal isomorfismo é um isomorfismo de T-álgebras. Assim, $T \otimes R[a_1]$ é uma T-álgebra separável. Ainda, sendo T uma extensão de Galois de R , sabemos, por III.1.5, que R é um R-somando direto de T . Logo, aplicando II.2.17, concluimos que $R[a_1]$ é uma R-álgebra separável, o que completa a prova. □

Façamos agora algumas observações. Sejam $B = R[X_1,\ldots,X_n]$ o anel de polinômios a n indeterminadas e S o subanel dos polinômios simétricos de B . Então o polinômio $U = U(X_1,\ldots,X_n) = \prod_{i\neq j} (X_i - X_j)$ é um elemento de S e não é um divisor de zero em B , como é fácil ver. Consideremos então o sistema multiplicativo gerado por U em B , i.e., $\{U^j \mid j=0,1,2,\ldots,\}$ e as localizações $B_U = \{g(X_1,\ldots,X_n)/_{U^s} \mid$ $\mid g(X_1,\ldots,X_n) \in B$ e $s = 0,1,2,\ldots\}$ e S_U . Então $S \subset B \subset B_U$ e $S \subset S_U \subset B_U$, como é fácil verificar. Além disso, U é um elemento inversível do anel S_U .

Consideremos o grupo de permutações S_n . Então é claro que cada permutação $\sigma \in S_n$ pode ser estendida a um automorfismo de B (que vamos continuar denotando por σ), definido por $\sigma[f(X_1,\ldots,X_n)] = f(X_{\sigma(1)},\ldots,X_{\sigma(n)})$, para cada $f(X_1,\ldots,X_n) \in B$. Se levamos em conta a propriedade universal da localização (ver prop. 3.1 de [2]), este automorfismo po-

de estender-se a um automorfismo σ^* de B_U, da seguinte maneira:

$\sigma^*[f(X_1,\ldots,X_n)/_{U^s}] = \sigma[f(X_1,\ldots,X_n)]/_{U^s}$, para cada $f(X_1,\ldots,X_n)/_{U^s} \in B_U$, como é fácil verificar. Denotemos então por S_n^* o conjunto de todos os automorfismos $\sigma^* : B_U \to B_U$ onde $\sigma \in S_n$. É claro que S_n^* é um grupo finito de automorfismos de B_U. Ainda,

$$(B_U)^{S_n^*} = \{g(X_1,\ldots,X_n) \in B_U \mid g(X_{\sigma(1)},\ldots,X_{\sigma(n)}) = g(X_1,\ldots,X_n), \forall \sigma \in S_n\} = S_U .$$

No que segue, denotamos por $F(X)$ o polinômio de $S_U[X]$ definido por $F(X) = (X - X_1)\ldots(X - X_n)$.

Corolário 2.2:

O anel B_U é uma extensão de Galois de S_U com grupo de Galois S_n^*. Além disso, as S_U-álgebras $S_U[X]/_{<F(X)>}$ e $S_U[X_1]$ são isomorfas, e $F(X)$ é um polinômio separável sobre S_U.

Prova:

Vamos aplicar aqui o lema anterior com relação ao elemento $X_1 \in B_U$. Observemos que o conjunto $\{\sigma^*(X_1) \mid \sigma^* \in S_n^*\}$ é igual a $\{X_1,\ldots,X_n\}$. Além disso, se $\sigma^*(X_1) \neq X_1$, então o elemento $\sigma^*(X_1) - X_1 = X_j - X_1$, (para algum $j \in \{2,3,\ldots,n\}$), é

um inversível em B_U . De fato, $X_j - X_1$ é um fator de U , que é um inversível em B_U . Então é suficiente aplicarmos o lema anterior, levando em conta que $S_U[X_1,\ldots,X_n] = B_U$. □

Estamos agora em condições de provar a seguinte

Proposição 2.3:

Seja $f(X) \in R[X]$ um polinômio mônico. Se existe um anel extensão de R que contenha elementos $a_1,\ldots,a_n$ tais que $f(X) = (X - a_1)\ldots(X - a_n)$ e $\prod_{i\neq j} (a_i - a_j) \in U(R)$ então $f(X)$ é um polinômio separável sobre R .

Prova:

Sejam $X_1,\ldots,X_n,X$ indeterminadas independentes, e seja $U = \prod_{i\neq j} (X_i - X_j) \in B = R[X_1,\ldots,X_n]$. Consideremos a aplicação $\Phi : B_U[X] \to R[a_1,\ldots,a_n][X]$ dada por

$$\Phi\left\{\sum_{i=0}^{r} \left[g_i(X_1,\ldots,X_n)/U^{m_i} \right] X^i \right\} = \sum_{i=0}^{r} \left[g_i(a_1,\ldots,a_n) \cdot \prod_{j\neq k} (a_j - a_k)^{-m_i} \right] X^i$$

É fácil verificar que tal aplicação Φ está bem definida e é um homomorfismo de anéis. Ainda, $\Phi(S_U) = R$, onde S é o subanel dos polinômios simétricos de B . De fato, se $\alpha_{n-i}(X_1,\ldots,X_n)$ é a função simétrica elementar de grau i , então

$$\sum_{i=0}^{n} \alpha_{n-i}(a_1,\ldots,a_n) X^i = \prod_{i=0}^{n} (X - a_i) = f(X) \in R[X] \text{ , ou seja,}$$

$\alpha_i(a_1,\ldots,a_n)$ são os coeficientes de $f(X) \in R[X]$, e, portanto, são elementos de R . Assim, $\Phi[\alpha_i(X_1,\ldots,X_n)] = \alpha_i(a_1,\ldots,a_n) \in R$. Logo, $\Phi(S_U) = R$, conforme o Teorema Fundamental das Funções Simétricas (ver [28], pág. 79).

Consideremos novamente o polinômio $F(X) = (X - X_1)\ldots(X - X_n) \in S_U[X]$ que é separável sobre S_U , pelo corolário anterior. Além disso, $\Phi[F(X)S_U[X]] = f(X)R[X]$, (a imagem do ideal gerado por $F(X)$ em $S_U[X]$ pela restrição $\Phi|_{S_U[X]}$ é exatamente o ideal gerado por $f(X)$ em $R[X]$) . Assim, $\Phi|_{S_U[X]}$ induz um epimorfismo de anéis $\overline{\Phi} : S_U[X]/_{<F(X)>} \to R[X]/_{<f(X)>}$. Ainda, como $S_U[X]/_{<F(X)>}$ é uma álgebra (separável) sobre S_U e $\overline{\Phi}(S_U) = \Phi(S_U) = R$, é claro que $R[X]/_{<f(X)>}$ é uma R-álgebra separável, se levarmos em conta II.2.5(*). Assim, $f(X)$ é um polinômio separável sobre R . □

Antes de seguirmos adiante, necessitamos de um resultado sobre ideais comaximais. Lembramos que dois ideais M e N de um anel comutativo A são ditos IDEAIS COMAXIMAIS DE A se $M + N = A$.

Lema 2.4 (Teorema do Resto Chinês)

Se M e N são ideais comaximais de A então existe um isomorfismo de anéis e de A-módulos entre $A/_{(M \cap N)}$ e $A/_M \oplus A/_N$.

(*) A proposição II.2.5 pode ser generalizada no seguinte sentido: Seja A um anel extensão de R que é separável sobre R . Se $f : A \to B$ é um epimorfismo de anéis então B é uma álgebra separável sobre $f(R)$.

Prova:

É claro que a aplicação $\psi: A \to A/_M \oplus A/_N$ dada por $\psi(a) = (a+M, a+N)$, para cada $a \in A$, está bem definida, e é um homomorfismo de anéis e de A-módulos. Além disso, $\text{Ker}\,\psi = M \cap N$, como é fácil verificar. Logo, resta-nos apenas mostrar que ψ é sobrejetora.

Sejam $a, b \in A$. Então, como $M+N=A$, vem que $a = m_1 + n_1$ e $b = m_2 + n_2$, onde $m_1, m_2 \in M$ e $n_1, n_2 \in N$. Então $(a+M, b+N) = (n_1+M, m_2+N) = ((n_1+m_2)+M, (n_1+m_2)+N) = \psi(n_1+m_2)$, o que completa a prova. □

Este lema pode ser generalizado para o caso em que temos um número finito de ideais dois a dois comaximais. A prova desta generalização utiliza indução e uma generalização de I.4.10. Maiores detalhes podem ser encontrados em [5] (por exemplo, ver prop. 7, pág. A.I.102).

No que segue, se $f(X)$ é um polinômio com coeficientes sobre um corpo K, diremos que ele é um polinômio CLASSICAMENTE SEPARÁVEL se é separável no sentido estabelecido no Capítulo I. Além disso, denotaremos por $K[x]$ a K-álgebra $K[X]/_{<f(X)>}$, onde $x = X + <f(X)>$.

Lema 2.5:

Seja K um corpo, e seja $f(X) \in K[X]$ um polinômio mônico arbitrário. Então $f(X)$ é separável sobre K (i.e., $K[X]/_{<f(X)>}$ é K-separável) se e só se $f'(x)$ é um elemento inversível em $K[x]$ e $f(X)$ é um produto de poli-

nômios irredutíveis e distintos de $K[X]$.

Neste caso, cada um destes polinômios é também separável sobre K .

Prova:

Façamos inicialmente uma observação. Sendo $f(X) \in K[X]$ um polinômio mônico, existem polinômios mônicos e irredutíveis $g_1(X),\ldots,g_m(X) \in K[X]$, dois a dois distintos, e inteiros positivos $\ell_1,\ldots,\ell_m$ tais que $f(X) = g_1^{\ell_1}(X)\ldots g_m^{\ell_m}(X)$. Além disso, como cada $g_i(X)$ é por hipótese irredutível em $K[X]$, o ideal $\langle g_i(X)\rangle$ é maximal em $K[X]$. Então os ideais $\langle g_i(X)\rangle$ e $\langle g_j(X)\rangle$ são comaximais, sempre que $i \neq j$, como é fácil verificar. Portanto, pela generalização de I.4.10, $\langle g_i(X)\rangle^{\ell_i} = \langle g_i^{\ell_i}(X)\rangle$ e $\langle g_j(X)\rangle^{\ell_j} = \langle g_j^{\ell_j}(X)\rangle$ são também comaximais se $i \neq j$ e $\bigcap_{i=1}^{m} \langle g_i^{\ell_i}(X)\rangle = \langle g_1^{\ell_1}(X)\ldots g_m^{\ell_m}(X)\rangle$. Logo, pela generalização do Teorema do Resto Chinês,

$$K[X]/_{\langle f(X)\rangle} = K[X]/_{\langle g_1^{\ell_1}(X)\ldots g_m^{\ell_m}(X)\rangle} = K[X]/_{\bigcap_{i=1}^{m}\langle g_i^{\ell_i}(X)\rangle} \simeq$$

$$\simeq \bigoplus_{i=1}^{m} K[X]/_{\langle g_i^{\ell_i}(X)\rangle} \text{ , como } K\text{-álgebras, e tal isomorfismo (que}$$

vamos denotar por Γ) é dado por $\Gamma(g(X) + \langle f(X)\rangle) = (g(X) + \langle g_1^{\ell_1}(X)\rangle,\ldots,g(X) + \langle g_m^{\ell_m}(X)\rangle)$. Ainda, pondo $K[X]/_{\langle g_i^{\ell_i}(X)\rangle} =$

$= K[x_i] = K \oplus Kx_i \oplus Kx_i^2 \oplus \ldots \oplus Kx_i^{r_i - 1}$, onde $r_i = \partial g_i^{\ell_i}(X)$ e $x_i = X + \langle g_i^{\ell_i}(X)\rangle$, podemos escrever $K[x] \simeq K[x_1] \oplus \ldots \oplus K[x_m]$.

Suponhamos então que $f(X)$ é um polinômio separável, e mostremos que $\ell_i = 1$, para cada $i \in \{1,2,\ldots,m\}$. Sendo $f(X)$ separável sobre K , cada somando direto $K[x_i]$ é uma K-álgebra separável. Observemos então que, neste caso, $K[x_i]$ é um anel semi-simples. De fato, se M é um $K[x_i]$-módulo, então M é também um K-módulo, e, como K é um corpo, M é K-projetivo. Portanto, por II.2.8, M é projetivo sobre $K[x_i]$. Assim, por I.6.7, $K[x_i]$ não possui elementos nilpotentes, para cada $i \in \{1,2,\ldots,m\}$. Como $g_i^{\ell_i}(x_i) = 0$, concluimos que $\ell_i = 1$, necessariamente, para cada $i \in \{1,2,\ldots,m\}$ (se $\ell_i \geq 2$, $g_i(x_i) \neq 0$ é nilpotente). Ou seja, $f(X)$ é um produto de polinômios irredutíveis e distintos de $K[X]$.

Mostremos agora que $f'(x) \in U(K[x])$. Observemos que $f'(x) = g_1'(x)g_2(x)\ldots g_m(x) + g_1(x)g_2'(x)\ldots g_m(x) + \ldots + g_1(x)g_2(x)\ldots g_m'(x)$. Portanto, aplicando o isomorfismo Γ , temos que $\Gamma[f(x)] = (g_1'(x_1)g_2(x_1)\ldots g_m(x_1), g_1(x_2)g_2'(x_2)\ldots g_m(x_2), \ldots, g_1(x_m)g_2(x_m)\ldots g_m'(x_m))$. Observemos agora que $g_i(x_j) \in U(K[x_j])$, se $i \neq j$. De fato, $g_i(x_j) \neq 0$ em $K[x_j]$, pois caso contrário, $g_i(X)$ e $g_j(X)$ seriam ambos polinômios minimais de x_j em $K[x_j]$, donde segue que $g_i(X) = g_j(X)$, uma contradição. Assim $g_i(x_j) \neq 0$ e, como $K[x_j]$ é um corpo, $g_i(x_j) \in U(K[x_j])$.

Como $f'(x)$ é inversível em $K[x]$ se e só se cada i-ésima componente da m-upla $\Gamma[f(x)]$ é inversível em $K[x_i]$, temos que $f'(x) \in U(K[x])$ se e só se $g_i'(x_i) \in U(K[x_i])$,

para cada $i \in \{1,2,\ldots,m\}$. Por outro lado, se $g_i'(x_i) \notin U(K[x_i])$, então $g_i'(x_i) = 0$, donde segue que $g_i(X)$ e $g_i'(X)$ têm a raiz comum x_i em $K[x_i]$. Mostremos que este fato nos leva a uma contradição. Sendo $K[x_i]$ um corpo extensão de K , podemos aplicar II.3.5 e concluir que $g_i(X)$ é um polinômio classicamente separável sobre K , e, portanto, não possui raízes comuns com $g_i'(X)$, uma contradição. Logo, $f'(x) \in U(K[x])$.

Para mostrar a recíproca, suponhamos que $f(X) = g_1(X)\ldots g_m(X)$ é uma decomposição de $f(X)$ em polinômios irredutíveis e distintos de $K[X]$. Então pelas considerações feitas inicialmente, $K[x] \simeq \overset{m}{\underset{i=1}{\oplus}} K[x_i]$, onde cada $K[x_i]$ é um corpo, pois $\langle g_i(X)\rangle$ é um ideal maximal. Assim se $f'(x) \in K[x]$, vemos que $g_i'(x_i) \in U(K[x_i])$, para todo i .

Mostremos a seguir que $g_i(X)$ é um polinômio classicamente separável. De fato, se o corpo K tem característica zero, então por I.5.3, $g_i(X)$ é classicamente separável sobre K , por ser um polinômio irredutível em $K[X]$. Se K tem característica $p > 0$ e se $g_i(X) = h(X^p)$ para algum $h(X) \in K[X]$, então $g_i'(X) = 0$. Como $g_i'(x_i) \in U(K[x])$, chegamos a uma contradição. Então, novamente por I.5.3, vemos que $g_i(X)$ é classicamente separável sobre K , mesmo que K tenha característica $p \neq 0$. Assim, $K[x_i]$ é um corpo extensão de K tal que o polinômio minimal de x_i é classicamente separável sobre K . Logo, por II.3.5, $K[x_i]$

é uma K-álgebra separável, para cada $i \in \{1,2,\ldots,m\}$. Portanto, $K[x] \simeq \overset{m}{\underset{i=1}{\oplus}} K[x_i]$ é também K-separável, o que completa a prova. □

Da prova do lema acima, podemos obter as seguintes conclusões. Se K é um corpo e $f(X) \in K[X]$ é um polinômio mônico e separável sobre K então f(X) é um produto de polinômios irredutíveis, distintos e classicamente separáveis de $K[X]$. Ainda , como tais fatores geram ideais dois a dois comaximais de $K[X]$, é claro que não existem raízes comuns entre estes fatores, no fecho algébrico de K . Assim, f(X) é um polinômio classicamente separável sobre K . Reciprocamente, se f(X) não tem raízes múltiplas no fecho algébrico de K então é claro que f(X) é um produto de fatores irredutíveis e distintos de $K[X]$. Neste caso, pela prova anterior, $f'(x) \in U(K[x])$. De fato, se $f(X) = g_1(X)\ldots g_m(X)$ é a decomposição de f(X) como produto de fatores irredutíveis e distintos de $K[X]$, então $K[x] \simeq \overset{m}{\underset{i=1}{\oplus}} K[x_i]$, onde $x_i = X + \langle g_i(X) \rangle$ e $K[x_i]$ é um corpo extensão de K para cada $i \in \{1,2,\ldots,m\}$. Como cada $g_j(X)$ é o polinômio minimal de x_j em $K[X]$, tem-se que $g_i(x_j) \neq 0$ sempre que $i \neq j$, e, portanto, $g_i(x_j) \in U(K[x_j])$. Além disso, como cada $g_i(x)$ é um polinômio classicamente separável sobre K , tem-se que $g_i'(x_i) \neq 0$ em $K[x_i]$, ou seja, $g_i'(x_i) \in U(K[x_i])$. Assim, analisando a imagem de f'(x) pelo isomorfismo acima, vê-se que $f'(x) \in U(K[x])$. Logo, pelo lema anterior, f(X) é um polinô-

mio separável sobre K . Portanto, é válido o seguinte

Corolário 2.6:

Sejam K um corpo e $f(X) \in K[X]$ um polinômio mônico. Então $f(X)$ é separável sobre K se e só se $f(X)$ é classicamente separável sobre K .

Seja M um ideal maximal de R , e seja $f(X) \in R[X]$ um polinômio mônico de grau n . Denotemos por $\overline{f}(X)$ o polinômio obtido de $f(X)$ reduzindo seus coeficientes módulo M . Então, se $K = R/_M$, temos $\overline{f}(X) \in K[X]$. Observemos que as R-álgebras $R[X]/_{MR[X]+<f(X)>}$ e $R[x]/_{MR[x]}$ são isomorfas. De fato, pelos teoremas de passagem ao quociente,

$$R[x]/_{MR[x]} = \left[R[X]/_{<f(X)>}\right]/_{M\left[R[X]/<f(X)>\right]} = \left[R[X]/_{<f(X)>}\right]/_{\left[MR[x]+<f(X)>/_{<f(X)>}\right]} \simeq$$

$$\simeq R[X]/_{MR[X]+<f(X)>} \text{ . Além disso, as K-álgebras}$$

$K \otimes R[x] = R/_M \otimes R[x]$ e $R[x]/_{MR[x]}$ são também isomorfas, como é fácil verificar.

Com estas considerações, enunciamos agora um resultado cuja prova pode ser encontrada em [26] (ver Lemme 4, pág. 28), e que determina os ideais maximais de $R[x]$ quando R é um anel local.

Lema 2.6:

Se R é um anel local com ideal maximal M e

se $\overline{f}(X) = \prod_{i=1}^{r} \overline{h}_i^{s_i}(X)$, onde $\overline{h}_i(X)$ é um polinômio irredutível em $K[X] = R/_M[X]$, então os ideais de $R[x]$ dados por $M_i = \langle M, h_i(x) \rangle = MR[x] + h_i(x)R[x]$ são todos maximais, distintos dois a dois e são os únicos ideais maximais de $R[x]$. Além disso, o quociente $R[x]/_{M_i}$ é isomorfo ao corpo $K[X]/_{\langle \overline{h}_i(X) \rangle}$.

Com este resultado e com estas mesmas notações utilizadas, mostramos a seguinte

Proposição 2.7:

Se $f(X) \in R[X]$ é um polinômio separável, então $f'(X) \in U(R[x])$.

Prova:

Suponhamos inicialmente que R é um anel local, cujo ideal maximal é M . Neste caso o polinômio $\overline{f}(X) \in K[X]$ é separável sobre $K = R/_M$. De fato, sendo $R[x]$ uma R-álgebra separável, $K \otimes R[x]$ é uma K-álgebra separável. Mas

$$K[X]/_{\langle \overline{f}(X) \rangle} = R/_M[X]/_{f(X)R/_M[X]} = (R[X]/_{M[X]})/_{(fR[X]+M[X]/_{M[X]})} \simeq$$

$$\simeq R[X]/_{fR[X]+M[X]} \simeq R[x]/_{MR[x]} \simeq R/_M \otimes R[x] = K \otimes R[x] .$$

Assim, $K[X]/_{\langle \overline{f}(X) \rangle}$ é uma K-álgebra separável, ou, equivalentemente, $\overline{f}(X) \in K[X]$ é um polinômio separável sobre $K = R/_M$.

Portanto, por 2.5, $\overline{f}'(X + \langle \overline{f}(X) \rangle) \in U(K[X]/_{\langle \overline{f}(X) \rangle}) \simeq U(R[X]/_{\langle M, f(X) \rangle})$ e $\overline{f}(X) = \overline{g}_1(X) \ldots \overline{g}_m(X)$, onde os polinômios $\overline{g}_i(X) \in K[X]$ são todos irredutíveis e distintos dois a dois. Mostremos que isto implica $f'(x) \in U(R[x])$.

Pelo lema anterior, sabemos que os ideais de $R[x]$, $M_i = \langle M, g_i(x) \rangle$, são todos distintos e são os únicos ideais maximais de $R[x]$. Então, se $f'(x) \notin U(R[x])$, existe algum $i \in \{1,2,\ldots,m\}$ tal que $f'(x) \in M_i = \langle M, g_i(x) \rangle$, ou seja, $f'(X) \in \langle M, g_i(X) \rangle$ (ideal de $R[X]$) . Como

$f(X)R[X] \subset M[X] + f(X)R[X] \subset M[X] + g_i(X)R[X]$, podemos considerar os seguintes homomorfismos canônicos

$$R[X] \xrightarrow{\sigma_1} R[X]/_{\langle f(X) \rangle} \xrightarrow{\sigma_2} R[X]/_{\langle M, f(X) \rangle} \xrightarrow{\sigma_3} R[X]/_{\langle M, g_i(X) \rangle}$$

Então, se $\sigma = \sigma_3 \circ \sigma_2 \circ \sigma_1$, vemos que $f'(X) \in \text{Ker } \sigma$, já que $f'(X) \in \langle M, g_i(X) \rangle$. Por outro lado, $\sigma[f'(X)] = \sigma_3[\overline{f}'(x)]$, uma contradição (pois neste caso $\overline{f}'(x)$ não poderia ser um inversível em $R[X]/_{\langle M, f(X) \rangle} \simeq K[X]/_{\langle \overline{f}(X) \rangle}$) .

Logo, $f'(x) \in U(R[x])$, o que completa a prova deste primeiro caso.

Se R é um anel arbitrário, $f'(x)$ é inversível em $R[x]$ se e só se $f'_M(x) = f'(x)/_1$ é inversível em $(R[x])_M$, para cada ideal maximal M de R (ver NOTA a seguir). Podemos assim completar a prova facilmente. De fato, se $R[x]$ é R-separável então $R[x] \otimes R_M \simeq R_M[x] = R_M[X]/_{\langle f_M(X) \rangle}$

é separável sobre R_M . Logo, $f'(x)/_1$ é inversível em $(R[x])_M$, para cada ideal maximal M de R , donde $f(x)$ é inversível em $R[x]$. □

NOTA: Se A é uma extensão comutativa de R então um elemento $a \in A$ é inversível em A se e só se $a/_1$ é inversível em A_M , para cada ideal maximal M de R . De fato, se $a \in U(A)$, então $ab = 1$, para algum $b \in A$. Então $a/_1 \, b/_1 = ab/_1 = 1/_1$, donde segue que $a/_1 \in U(A_M)$, para cada ideal maximal M de R . Para mostrar a recíproca, observemos que o homomorfismo de R-módulos $f_a : A \to A$ daddo por $f_a(b) = ba$, para cada $b \in A$ é um epimorfismo se e só se $f_{a_M} : A_M \to A_M$ é um epimorfismo de R_M-módulos, para cada ideal maximal M de R . Então, se $a/_1 \in U(A_M)$, para cada ideal maximal M de R , é claro que f_{a_M} é um R_M-epimorfismo. Logo, existe $b \in A$ tal que $f_a(b) = 1$, ou seja, $a \in U(A)$.

Se A e A' são R-álgebras, dizemos que A é uma R-ÁLGEBRA HOMOMÓRFICA a A' se existe um epimorfismo de R-álgebras de A em A' .

Agora podemos provar o seguinte teorema, fundamental para nosso objetivo.

Teorema 2.8:

Seja $f(X) \in R[X]$ um polinômio mônico tal que $f'(x)$ é inversível em $R[X]/_{<f(X)>}$, onde $x = X + <f(X)>$ é

a classe de X módulo $f(X)$. Então existe uma extensão de Galois A de R com grupo de Galois $G \simeq S_n$ que contém elementos $a_1,\ldots,a_n$ tais que:

(i) $f(X) = (X - a_1)\ldots(X - a_n)$ e $\prod_{i\neq j} (a_i - a_j) \in U(R)$;

(ii) $A = R[a_1,\ldots,a_n]$ é um R-módulo livre de posto igual a $n!$;

(iii) se A' é um anel extensão de R que contém elementos $a_1^*,\ldots,a_n^*$ tais que $A' = R[a_1^*,\ldots,a_n^*]$ e $f(X) = (X - a_1^*)\ldots(X - a_n^*)$ então A é uma R-álgebra homomórfica a A' , através da aplicação $g(a_1,\ldots,a_n) \mapsto g(a_1^*,\ldots,a_n^*)$, para cada $g(a_1,\ldots,a_n) \in A$.

Além disso, o elemento de G correspondente a cada permutação $\sigma \in S_n$ é o automorfismo de A denotado por σ^* , onde $\sigma^*[g(a_1,\ldots,a_n)] = g(a_{\sigma(1)},\ldots,a_{\sigma(n)})$, para cada $g(a_1,\ldots,a_n) \in A$.

Prova:

Suponhamos inicialmente que $\partial f = 1$, ou seja, $f(X) = X + r$, para algum $r \in R$. Neste caso, tomamos $A = R$, que é uma extensão de Galois de R com grupo de Galois $G = \{id_R\}$. O restante é trivial.

Suponhamos agora que $\partial f > 1$. Seja X_1 uma indeterminada e seja $a_1 = X_1 + \langle f(X_1)\rangle$. Então é fácil ver

que as R-álgebras $R[X_1]/_{<f(X_1)>}$ e $R[a_1]$ são isomorfas e, portanto, os anéis de polinômios $R[X_1]/_{<f(X_1)>}[X]$ e $R[a_1][X]$ são também R-álgebras isomorfas. Então, como a_1 é raiz de $f(X)$ em $R[a_1]$, o polinômio $f(X) \in R[a_1][X]$ decompõe-se da seguinte maneira: $f(X) = (X - a_1)f_2(X)$, para algum polinômio mônico $f_2(X) \in R[a_1][X]$. Se $\partial f_2 > 1$, utilizamos o mesmo raciocínio acima. Seja X_2 uma indeterminada e seja $a_2 = X_2 + <f_2(X_2)>$ a classe de X_2 em $R[a_1][X_2]/_{<f_2(X_2)>}$. Então a_2 é raiz de $f_2(X)$ em $R[a_1][X_2]/_{<f_2(X_2)>} \simeq R[a_1][a_2] \simeq R[a_1,a_2]$ e, portanto, $f_2(X) = (X - a_2)f_3(X)$, para algum polinômio mônico $f_3(X) \in R[a_1,a_2][X]$ de grau maior ou igaul a 1. Assim, por indução, obtemos uma extensão $R[a_1,a_2,\ldots,a_{n-1}]$ do anel R no qual $f(X)$ decompõe-se na forma $f(X) = (X - a_1)\ldots(X - a_{n-1})f_n(X)$, onde $f_n(X)$ é um polinômio mônico pertencente a $R[a_1,\ldots,a_{n-1}][X]$, cujo grau é 1, i.e., $f_n(X) = X - a_n$, para algum $a_n \in R[a_1,\ldots,a_{n-1}]$. Logo, $A = R[a_1,\ldots,a_n] = R[a_1,\ldots,a_{n-1}]$ é uma extensão de R onde $f(X)$ decompõe-se num produto de fatores lineares.

Antes de completarmos a prova de (i), mostremos as outras partes deste teorema. Do raciocínio acima fica claro que A é um R-módulo livre. De fato, $R[a_1]$ é um R-módulo livre com base $\{1,a_1,a_1^2,\ldots,a_1^{n-1}\}$, onde $n = \partial f$. Ainda, $\partial f_2 = n - 1$, e, portanto, $R[a_1,a_2]$ é um $R[a_1]$-módulo livre

com base $\{1, a_2, a_2^2, \ldots, a_2^{n-2}\}$. Em geral, $R[a_1, \ldots, a_i]$ é um $R[a_1, \ldots, a_{i-1}]$-módulo livre com base $\{1, a_i, a_i^2, \ldots, a_i^{n-i}\}$, pois $\partial f_i = n - i + 1$, para cada $i \in \{1, 2, \ldots, n\}$. Logo, $A = R[a_1, \ldots, a_n]$ é um R-módulo livre cuja base possui $n(n-1)(n-2)\ldots 2.1 = n!$ elementos (de fato, tal base é do tipo $\{a_1^{i_1} a_2^{i_2} \ldots a_n^{i_n} \mid 0 \leqslant i_j \leqslant n-j \ , \forall\, j \in \{1, 2, \ldots, n\}\}$). Fica assim completa a prova de (ii).

Consideremos agora A' um anel extensão de R , que contém elementos $a_1^*, \ldots, a_n^*$ tais que $A' = R[a_1^*, \ldots, a_n^*]$ e $f(X) = (X - a_1^*)\ldots(X - a_n^*)$, e mostremos que vale (iii). Para tal, utilizamos indução sobre $n = \partial f$. Se $n = 1$, então $A = A' = R$, e nada há a provar. Suponhamos então que para algum $m < n$, $A_m = R[a_1, \ldots, a_m]$ é uma R-álgebra homomórfica a $A'_m = R[a_1^*, \ldots, a_m^*]$ através da aplicação ψ dada por $\psi[g(a_1, \ldots, a_m)] = g(a_1^*, \ldots, a_m^*)$ para cada $g(a_1, \ldots, a_m) \in A_m$. Então esta aplicação induz um epimorfismo de R-álgebras $\overline{\psi} : A_m[X] \to A'_m[a^*_{m+1}]$, dado por

$$\overline{\psi}\Big[\sum_{i=0}^{K} g_i(a_1, \ldots, a_m) X^i\Big] = \sum_{i=0}^{K} g_i(a_1^*, \ldots, a_m^*)(a^*_{m+1})^i \ ,$$

para cada $\sum_{i=0}^{K} g_i(a_1, \ldots, a_m) X^i \in A_m[X]$, como é fácil verificar. Como vimos acima, o polinômio $f(X)$ em $A_m[X]$ decompõe-se na forma $f(X) = (X - a_1)\ldots(X - a_m) f_{m+1}(X)$, onde $f_{m+1}(X) \in A_m[X]$. Então $\overline{\psi}[f(X)] = (X - a_1^*)\ldots(X - a_m^*)\,\overline{\psi}[f_{m+1}(X)]$. Por outro lado, como

$f(X) \in R[X]$, sabemos que $\bar{\psi}[f(X)] = f(X)$. Portanto, em $A'[X]$, obtemos $(X - a_1^*) \ldots (X - a_m^*)\, \bar{\psi}[f_{m+1}(X)] = (X - a_1^*) \ldots (X - a_n^*)$, ou seja, $\bar{\psi}[f_{m+1}(X)] = (X - a_{m+1}^*) \ldots (X - a_n^*)$. Assim, a_{m+1}^* é raiz de $\bar{\psi}[f_{m+1}(X)] = [\psi(f_{m+1})](x)$, donde $f_{m+1}(X) \in \operatorname{Ker} \psi$. Logo, temos um epimorfismo induzido de R-álgebras $\bar{\bar{\psi}} : A_m[X]/_{\langle f_{m+1}(X) \rangle} =$

$= A_{m+1} \to A_m'[a_{m+1}^*] = A_{m+1}'$ dado por $\bar{\bar{\psi}}[g(a_1, \ldots, a_{m+1})] = g(a_1^*, \ldots, a_{m+1}^*)$. Portanto, existe um epimorfismo de R-álgebras de $A = R[a_1, \ldots, a_n]$ em $A' = R[a_1^*, \ldots, a_n^*]$ nas condições de (iii).

Seja σ uma permutação de S_n . Definindo $a_i^* = a_{\sigma(i)}$, para cada $i \in \{1, 2, \ldots, n\}$, vemos que $R[a_1^*, \ldots, a_n^*] = A$ e que existe um epimorfismo $\sigma^* : R[a_1, \ldots, a_n] \to R[a_1^*, \ldots, a_n^*]$ dado por $\sigma^*[g(a_1, \ldots, a_n)] = g(a_1^*, \ldots, a_n^*)$, para cada $g(a_1, \ldots, a_n) \in A$. Ainda, como σ é uma bijeção, é fácil constatar que σ^* é um automorfismo da R-álgebra A .

Sabemos que $f(X) = (X - a_1) f_2(X)$, onde $f_2(X) \in R[a_1][X] \simeq R[X_1]/_{\langle f(X_1) \rangle}[X]$. Então $f'(X) = f_2(X) + (X - a_1) f_2'(X)$ e, portanto, $f'(a_1) = f_2(a_1) = (a_1 - a_2)(a_1 - a_3) \ldots (a_1 - a_n)$. Como por hipótese $f'(a_1) = f'(X_1 + \langle f(X_1) \rangle)$ é inversível em $R[X_1]/_{\langle f(X_1) \rangle} \simeq R[a_1]$, vem que $f'(a_1) = \prod_{j=2}^{n} (a_1 - a_j)$ é inversível em A . Portanto, $a_1 - a_j \in U(A)$, para cada $j \in \{2, 3, \ldots, n\}$. Ainda, dado $i \in \{1, 2, \ldots, n\}$ com $i \neq j$, escolhemos $\sigma_i \in S_n$ tal que $\sigma_i(1) = i$ e $\sigma_i(j) = j$. Então $a_i - a_j = \sigma_i^*(a_1 - a_j) \in U(A)$.

Logo, $\prod_{i\neq j} (a_i - a_j) \in U(A)$. Assim, $a_i \neq a_j$, sempre que $i \neq j$. Potanto, se G denota o conjunto de todos os automorfismos σ^* , i.e., $G = \{\sigma^* \mid \sigma \in S_n\}$, então é fácil verificar que G é isomorfo a S_n .

Seja $R' = A^G$. Então existe um inteiro $m \in \{1,2,\ldots,n-1\}$ tal que $R' \subset A_{n-m} \subseteq A$. Seja $r' \in R' \subset A_{n-m} = A_{n-m-1}[a_{n-m}]$. Então $r' = \sum_{j=0}^{m} b_j (a_{n-m})^j$, onde $b_j \in A_{n-m-1}$, para cada $j \in \{0,1,\ldots,m\}$. Seja t um inteiro tal que $n-m \leq t \leq n$ e seja σ^* um elemento de G tal que $\sigma^*(a_{n-m}) = a_t$ e $\sigma^*(a_i) = a_i$, para cada $i \in \{1,2,\ldots,n-m-1\}$. Então, como $b_j \in A_{n-m-1}$, é claro que $\sigma^*(b_j) = b_j$, para cada $j \in \{0,1,\ldots,m\}$. Assim, podemos escrever

$$\sum_{j=0}^{m} b_j (a_{n-m})^j = r' = \sigma^*(r') = \sum_{j=0}^{m} b_j [\sigma^*(a_{n-m})]^j = \sum_{j=0}^{m} b_j a_t^j =$$

$$= b_0 + \sum_{j=1}^{m} b_j a_t^j \text{ , donde } \sum_{j=1}^{m} b_j a_t^j + b_0 - r' = 0 \text{ , para cada inteiro } t \text{ que satisfaz a propriedade } n-m \leq t \leq n .$$

Considerando agora a matriz de Vandermonte de ordem $(m+1) \times (m+1)$

$$\begin{bmatrix} 1 & a_{n-m} & a_{n-m}^2 & \cdots & a_{n-m}^m \\ 1 & a_{n-m+1} & a_{n-m+1}^2 & \cdots & a_{n-m+1}^m \\ \vdots & & & & \\ 1 & a_n & a_n^2 & \cdots & a_n^m \end{bmatrix} ,$$

vemos que ela é inversível, pois seu determinante é

$\pm \sqrt{\prod_{n-m\leq i<j\leq n} (a_i - a_j)} \in U(A)$. Assim, o sistema

$$\begin{bmatrix} 1 & a_{n-m} & \cdots & a_{n-m}^m \\ 1 & a_{n-m+1} & \cdots & a_{n-m+1}^m \\ \vdots & & & \\ 1 & a_n & \cdots & a_n^m \end{bmatrix} \begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ X_{m+1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

admite unicamente a solução trivial. Portanto, $b_j = 0$, para cada $j \in \{1,2,\ldots,m\}$ e $b_0 - r' = 0$. Ou seja, $r' = b_0 \in A_{n-m-1}$. Logo, $R' = A^G \subset A_{n-m-1}$. Então, por indução, temos que $A^G = R' \subset A_0 = R$. Assim, podemos concluir que $A^G = R$, e, por 2.1, A é uma extensão de Galois de R com grupo de Galois G formado por todos os automorfismos de A da forma σ^* onde $\sigma \in S_n$, e $\sqrt{\prod_{i\neq j} (a_i - a_j)} \in U(R)$, ficando assim completa a prova. □

Estamos agora em condições de estabelecer o resultado principal deste trabalho. Ele resume os resultados anteriores e apresenta outras caracterizações para um polinômio separável.

Teorema 2.9:

Seja $f(X) \in R[X]$. Então as seguintes condições são equivalentes:

(a) f(X) é um polinômio separável sobre R ;

(b) f(X) é mônico e $f'(x) \in U(R[X]/_{<f(X)>})$;

(c) existe um anel extensão de R que contém

elementos $a_1,\ldots,a_n$ tais que $f(X) = (X - a_1)\ldots(X - a_n)$ e $\prod_{i\neq j} (a_i - a_j) \in U(R)$;

(d) existe uma extensão de Galois de R que contém elementos $a_1,\ldots,a_n$ tais que $f(X) = (X - a_1)\ldots(X - a_n)$ e $\prod_{i\neq j} (a_i - a_j) \in U(R)$;

(e) para cada ideal maximal M de R, a imagem de $f(X)$ é um polinômio separável sobre o anel local R_M ;

(f) para cada ideal maximal M de R, o polinômio obtido a partir de $f(X)$, reduzindo seus coeficientes módulo M, não tem raízes múltiplas no fecho algébrico de $R/_M$ (i.e., é um polinômio classicamente separável sobre $R/_M$) ;

(g) se t denota a aplicação traço do R-módulo livre $R[x] = R[X]/_{<f(X)>}$ então o determinante da matriz $(t(x^i x^j))$, com $0 \leq i,j < \partial f$, é um elemento inversível de R.

Prova:

As implicações (a)$\Rightarrow$(b), (b)$\Rightarrow$(d), (d)$\Rightarrow$(c) e (c)$\Rightarrow$(a) são conseqüências diretas de 2.3, 2.7 e 2.8, como é fácil verificar.

(a)$\Leftrightarrow$(e):

Como $R[X]/_{< f(X)>}$ é uma R-álgebra finitamente gerada e projetiva como R-módulo, podemos aplicar 1.4 . Então temos que $f(X)$ é um polinômio separável sobre R se e só se $R[X]/_{<f(X)>}$ é uma R-álgebra separável, ou, equivalentemente, $R_M \otimes R[X]/_{<f(X)>} \simeq R_M[X]/_{<f_M(X)>}$ é uma R_M-álgebra

separável, para cada ideal maximal M de R.

(a)$\Longleftrightarrow$(f):

Por 1.4, o quociente $R[x] = R[X]/_{<f(X)>}$ é R-separável se e só se $R/_M \otimes R[x] \simeq R[x]/_{MR[x]}$ é uma álgebra separável sobre $R/_M$, para cada ideal maximal M de R. Por outro lado, se $\overline{f}(X)$ denota o polinômio obtido a partir de $f(X)$ reduzindo seus coeficientes módulo M, temos que as $R/_M$-álgebras $R[x]/_{MR[x]}$ e $R/_M[X]/_{<\overline{f}(X)>}$ são isomorfas, conforme foi mostrado na prova de 2.7. Assim, $f(X)$ é um polinômio separável sobre R se e só se $\overline{f}(X)$ é separável sobre o corpo $R/_M$, i.e., $\overline{f}(X)$ é classicamente separável sobre $R/_M$.

(a)$\Longrightarrow$(g):

Sabemos que $R[X]/_{<f(X)>}$ é um R-módulo livre de base $\{1,x,\ldots,x^{n-1}\}$, onde $x = X + <f(X)>$ e $n = \partial f$. Então é claro que as projeções naturais $\pi_i : R[X]/_{<f(X)>} \to R$ formam, junto com a base $\{1,x,\ldots,x^{n-1}\}$, um sistema de coordenadas projetivas para $R[X]/_{<f(X)>}$. Portanto, a aplicação traço de tal R-módulo pode ser dada por $t(z) = \sum_{i=0}^{n-1} \pi_i(zx^i)$. Ainda, como $R[x] = R[X]/_{<f(X)>}$ é R-fortemente separável, por 1.2 esta aplicação traço é um gerador livre do $R[x]$-módulo à direita $\mathrm{Hom}_R(R[x],R)$. Em particular, para cada $i \in \{0,1,\ldots,n-1\}$ existe um elemento $z_i = \sum_{k=0}^{n-1} r_{ik}.x^k \in R[x]$ tal que $\pi_i = t(z_i -)$.

Portanto, para cada $i,j \in \{0,1,\ldots,n-1\}$, $\delta_{ij} = \pi_i(x^j) = t(z_i x^j) =$

$= \sum_{k=0}^{n-1} r_{ik} t(x^k x^j)$, donde resulta a seguinte equação matricial:

$(r_{ik})(t(x^k x^j)) = I_{n\times n}$, (onde $I_{n\times n}$ representa a matriz unidade de ordem $n \times n$). Portanto, o determinante da matriz $(t(x^k x^j))_{0\leqslant i,j<n}$ é um elemento inversível de R .

(g)$\Longrightarrow$(a)

Seguindo exatamente o caminho inverso da prova acima, vemos que $\pi_i = t(z_i -)$, para cada $i \in \{0,1,\ldots,n-1\}$, onde cada π_i representa a projeção canônica de $R[x] = R[X]/_{<f(X)>}$ no i-ésimo somando $R.x^i$. Ainda, se $f \in \mathrm{Hom}_R(R[x],R)$ é um R-homomorfismo arbitrário de $R[x]$ em R então, para cada $y = \sum_{i=0}^{n-1} r_i x^i \in R[x]$, temos que

$f(y) = \sum_{i=0}^{n-1} r_i f(x^i) = \sum_{i=0}^{n-1} \pi_i(y) f(x^i) = \sum_{i=0}^{n-1} f(x^i)\pi_i(y)$, donde

$f = \sum_{i=0}^{n-1} f(x^i)\pi_i = \sum_{i=0}^{n-1} t(f(x^i)z_i -)$. Portanto, a aplicação traço $t : R[x] \to R$ é gerador do $R[x]$-módulo à direita $\mathrm{Hom}_R(R[x],R)$. Para mostrar que t é um gerador livre, suponhamos que $t.a = 0$, para algum $a \in R[x]$. Então $t.a(z_i) = t(az_i) = 0$, para cada $i \in \{0,1,\ldots,n-1\}$. Logo, $\pi_i(a) = t(z_i a) = 0$, para cada i , e, portanto, $a = 0$. Assim, por 1.3, a prova está completa. □

O determinante da matriz $(t(x^i x^j))$ dada no

item (g) do teorema acima e denominado DISCRIMINANTE DE $f(X)$.

Vejamos agora algumas conseqüências dos resultados acima. Primeiramente, a seguinte nota é clara:

NOTA 1: Seja $f(X) \in R[X]$ um polinômio mônico. Se existe um anel A extensão de R que contém elementos $a_1,\ldots,a_n$ tais que $f(X) = (X - a_1)\ldots(X - a_n)$ e $U = \prod_{i\neq j} (a_i - a_j)$ é um não divisor de zero de A então $f(X)$ é um polinômio separável sobre R_U :

NOTA 2: Nas mesmas hipóteses do teorema 2.8, mostremos que $R[a_1,\ldots,a_n]$ é imagem homomórfica da R-álgebra fortemente separável $R[X_1]/_{<f(X_1)>} \otimes \ldots \otimes R[X_n]/_{<f(X_n)>}$. De fato, observemos inicialmente que existe um epimorfismo de R-álgebras $\Phi : R[X_1,\ldots,X_n] \to R[a_1,\ldots,a_n]$, dado por $\Phi[g(X_1,\ldots,X_n)] = g(a_1,\ldots,a_n)$, para cada $g(X_1,\ldots,X_n) \in R[X_1,\ldots,X_n]$, como é fácil verificar. Ainda, como $f(X_i) \in \operatorname{Ker}\Phi$, para cada $i \in \{1,2,\ldots,n\}$ (já que $f(a_i) = 0$) , podemos considerar o epimorfismo induzido de R-álgebras $\overline{\Phi} : R[X_1,\ldots,X_n]/_{<f(X_1),\ldots,f(X_n)>} \to R[a_1,\ldots,a_n]$. Mostremos agora que as R-álgebras $R[X_1,\ldots,X_n]/_{<f(X_1,\ldots,X_n)>}$ e $R[X_1]/_{<f(X_1)>} \otimes \ldots \otimes R[X_n]/_{<f(X_n)>}$ são isomorfas. De fato, é fácil ver que a aplicação

$\psi : R[X_1]/_{<f(X_1)>} \otimes \ldots \otimes R[X_n]/_{<f(X_n)>} \to R[X_1,\ldots,X_n]/_{<f(X_1),\ldots,f(X_n)>}$

dada por $\psi\{[p_1(X_1)+<f(X_1)>]\otimes\ldots\otimes[p_n(X_n)+<f(X_n)>]\} = p_1(X_1)\ldots p_n(X_n) +$

$+ <f(X_1),\ldots,f(X_n)>$ é um homomorfismo de R-álgebras que leva a base

$\{x_1^{i_1}\otimes\ldots\otimes x_n^{i_n}\}_{i_1,\ldots,i_n=0}^{\partial f-1}$ (onde $x_i = X_i + <f(X_i)>$) de

$R[X_1]/_{<f(X_1)>}\otimes\ldots\otimes R[X_n]/_{<f(X_n)>}$ na base

$\{X_1^{i_1}\ldots X_n^{i_n} + <f(X_1),\ldots,f(X_n)>\}_{i_1,\ldots,i_n=0}^{\partial f-1}$ de

$R[X_1,\ldots,X_n]/_{<f(X_1),\ldots,f(x_n)>}$. Assim, ψ é um isomorfismo entre tais R-álgebras. Ainda, como $f(X)\in R[X]$ é um polinômio separável, é claro que $R[X_1]/_{<f(X_1)>}\otimes\ldots\otimes R[X_n]/_{<f(X_n)>}$ é uma R-álgebra fortemente separável. Logo, $R[a_1,\ldots,a_n]$ é imagem, por $\overline{\Phi}$, de uma R-álgebra fortemente separável. Por II.2.5., segue que $R[a_1,\ldots,a_n]$ é também uma R-álgebra separável.

É fácil observar agora que o raciocínio acima pode ser feito para qualquer número m de raízes $a_1,\ldots,a_m$ de f(X) em A . Torna-se claro então o seguinte

Corolário 2.10:

Sejam $f(X)\in R[X]$ e A uma extensão de R que contém elementos $a_1,\ldots,a_n$ tais que $f(X) = (X-a_1)\ldots(X-a_n)$ e $\prod_{i\neq j}(a_i - a_j)\in U(R)$. Se $a_1^*,\ldots,a_m^*$ $(m<\infty)$ são raízes ar

bitrárias de $f(X)$ em A, então $R[a_1^*,\ldots,a_m^*]$ é imagem homomórfica de uma R-álgebra fortemente separável.

Os teoremas 2.8 e 2.9 têm como conseqüência o seguinte

Corolário 2.11:

Seja $f(X) \in R[X]$ um polinômio mônico. Então existe um anel extensão de R que contém elementos $a_1,\ldots,a_n$ tais que $f(X) = (X - a_1)\ldots(X - a_n)$. Neste caso, $f(X)$ é um polinômio separável sobre R se e só se $\prod_{i\neq j} (a_i - a_j) \in U(R)$.

Prova:

Como na demostração do teorema 2.8, tal extensão de R é $A = R[a_1,\ldots,a_n]$, onde $a_1 = X_1 + \langle f(X_1)\rangle \in R[X_1]/_{\langle f(X_1)\rangle}$ $a_2 = X_2 + \langle f_2(X_2)\rangle \in R[a_1][X_2]/_{\langle f_2(X_2)\rangle}$ é $f(X) = (X - a_1)f_2(X)$, para algum polinômio $f_2(X) \in R[a_1][X]$, etc. Além disso, pela equivalência (a)$\Longleftrightarrow$(c) do teorema 2.9, é fácil concluir esta prova. □

Corolário 2.12:

Sejam $r \in R$ e n um inteiro maior do que 1. Então o polinômio $X^n - r \in R[X]$ é separável sobre R se e só se $n.1_R$ e r são elementos inversíveis de R.

Prova:

Seja $f(X) = X^n - r$, e consideremos o quociente $R[x] \simeq R[X]/_{<f(X)>}$, onde $x = X + <f(X)>$. Então sabemos que x é raiz de $f(X) \in R[x][X]$ e, portanto, $x^n = r$. Além disso, $f'(X) = n X^{n-1}$. Assim, pelo teorema 2.9, $f(X) = X^n - r$ é um polinômio separável sobre R se e só se $nx^{n-1} \in U(R[x])$. Mostremos então que $nx^{n-1} \in U(R[x])$ se e só se $n.1_R \in U(R)$ e $r \in U(R)$.

Se $r \in U(R)$ e $n.1_R \in U(R)$, então $x \in U(R[x])$ (já que $x^n = r$), e é claro que $nx^{n-1} \in U(R[x])$. Reciprocamente, se $nx^{n-1} \in U(R[x])$ então $nx^{n-1}k(x) = 1$, para algum elemento $k(x) = \sum_{i=0}^{n-1} r_i x^i \in R[x]$. Ou seja: $1 = nx^{n-1} \sum_{i=0}^{n-1} r_i x^i =$

$= \sum_{i=0}^{n-1} nr_i x^{n+i-1} = nr_0 x^{n-1} + \sum_{i=1}^{n-1} nr_i r x^{i-1}$, donde vemos que $nr_1 r = 1$, já que $R[x]$ é um R-módulo livre. Assim, $r \in U(R)$ e $n.1_R \in U(R)$, o que completa a prova. □

Corolário 2.13:

Seja R uma álgebra sobre o corpo primo $GF(p)$, $(p \neq 0)$ e seja $f(X) = X^{pm} + r_{m-1}X^{p(m-1)} + \ldots + r_1 X^p + r_0 X^n + r \in R[X]$, onde $m \geqslant 1$ e $p > n$. Então

(i) se $n = 0$, $f(X)$ não é separável sobre R ;

(ii) se $n = 1$, $f(X)$ é separável sobre R se e só se $r_0 \in U(R)$;

(iii) se $n > 1$, $f(X)$ é separável sobre R se e só se r_0 e r são inversíveis em R .

Prova:

Se $n = 0$, então

$f'(X) = pmX^{pm-1} + p(m-1)r_{m-1}X^{p(m-1)} + \ldots + pr_1X^{p-1} = 0$, pois R é uma $GF(p)$-álgebra. Então $f'(x)$ não é um elemento inversível de $R[X]/_{<f(X)>}$, e, portanto $f(X)$ não é separável sobre R .

Se $n = 1$,

$f'(X) = pmX^{pm-1} + p(m-1)r_{m-1}X^{p(m-1)-1} + \ldots + pr_1X^{p-1} + r_0 = r_0$.

Então pelo teorema anterior, $f(X)$ é separável sobre R se e só se $r_0 \in U(R[x])$, onde $x = X + <f(X)>$. Mas é fácil ver que, como $R[x]$ é um R-módulo livre de posto finito, $r_0 \in U(R[x])$ se e só se $r_0 \in U(R)$. Assim, fica mostrado (ii).

Finalmente, se $n > 1$,

$f'(X) = pmX^{pm-1} + p(m-1)r_{m-1}X^{p(m-1)-1} + \ldots + pr_1X^{p-1} + nr_0X^{n-1} = nr_0X^{n-1}$

Então $f(X)$ é separável sobre R se e só se nr_0x^{n-1} é um elemento inversível em $R[x]$, ou, equivalentemente, se $n.1_R$, r_0 e x são inversíveis em $R[x]$. Como $1 < n < p$, $n.1_R$ é sempre inversível em R , e, portanto, também em $R[x]$. Além disso, $r_0 \in U(R[x])$ se e só se $r_0 \in U(R)$, como é fácil verificar. Mostremos, finalmente, que $x \in U(R[x])$ se e só se $r \in U(R)$. Suponhamos que $x \in U(R[x])$, e seja $x^{-1} = c_{pm-1}x^{pm-1} + \ldots + c_1x + c_0 \in R[x]$

Então $xx^{-1} = 1$ e considerando que $f(x) = 0$ e que $R[x]$ é um R-módulo livre de base $\{1, x, x^2, \ldots, x^{pm-1}\}$, é fácil obter $C_{pm-1}r + 1 = 0$. Assim, $r \in U(R)$. Reciprocamente, se $r \in U(R)$, então

$$x(x^{pm-1} + r_{m-1}x^{p(m-1)-1} + \ldots + r_1x^{p-1} + r_0x^{n-1}) = -r \in U(R) \subset U(R[x]),$$

donde $x \in U(R[x])$, o que completa a prova. □

Vejamos agora algumas conseqüências para anéis que não possuem idempotentes próprios:

Proposição 2.14:

Sejam A e R anéis sem idempotentes próprios, e seja $f(X) \in R[X]$ um polinômio separável e de grau n sobre R. Então $f(X)$ não possui mais do que n raizes em A. Além disso, se α, β são raízes distintas de $f(X)$ em A, então $\alpha - \beta \in U(A)$.

Prova:

Como A é uma R-álgebra comutativa e $f(X)$ é um polinômio separável sobre R, $A \otimes (R[X]/_{<f(X)>})$ é uma A-álgebra separável. Observemos que $A \otimes (R[X]/_{<f(X)>})$ é isomorfo à A-álgebra $A[X]/_{<f(X)>} = A[X]/_{f(X)A[X]}$. De fato, como $R[X]/_{<f(X)>} = R.1 \oplus R.x \oplus \ldots \oplus R.x^{n-1}$ como R-módulo, então é claro que a A-álgebra $A \otimes (R[X]/_{<f(X)>})$ é livre como A-módulo, com base $\{1 \otimes x^i\}_{i=0}^{n=1}$, ou seja,

$A \otimes (R[X]/_{<f(X)>}) = A.(1 \otimes 1) \oplus A(1 \otimes x) \oplus \ldots \oplus A.(1 \otimes x^{n-1})$. Ainda, é claro que a A-álgebra $A[X]/_{<f(X)>}$ é também um A-módulo livre, com base $\{1, \tilde{x}, \ldots, \tilde{x}^{n-1}\}$, onde $\tilde{x}$ representa a classe de X no quociente $A[X]/_{<f(X)>}$. Então existe um isomorfismo natural de A-módulos $\psi : A[X]/_{<f(X)>} \to A \otimes (R[X]/_{<f(X)>})$ dado por $\psi(\sum_{i=0}^{n-1} a_i \tilde{x}^i) = \sum_{i=0}^{n-1} a_i \otimes x^i$. Tal aplicação ψ é até um homomorfismo de anéis, como é fácil verificar. Portanto, as A-álgebras $A \otimes (R[X]/_{<f(X)>})$ e $A[X]/_{<f(X)>}$ são isomorfas, e então $A[X]/_{<f(X)>}$ é uma A-álgebra separável.

Sejam $\alpha_1, \ldots, \alpha_m$ raízes distintas de $f(X)$ em A . Para cada $i \in \{1,2,\ldots,m\}$, consideremos a aplicação $h_i : A[X] \to A$ dada por $h_i(\sum_{j=0}^{r} a_j X^j) = \sum_{j=0}^{r} a_j \alpha_i^j$, para cada $\sum_{j=0}^{r} a_j X^j \in A[X]$. É claro que cada h_i é um homomorfismo de A-álgebras. Além disso, $h_i[f(X)] = f(\alpha_i) = 0$, donde $F(X) \in \text{Ker } h_i$, para cada $i \in \{1,2,\ldots,m\}$. Assim, cada h_i induz um homomorfismo de A-álgebras $g_i : A[X]/_{<f(X)>} \to A$, dado por $g_i(k(\tilde{x})) = k(\alpha_i)$, para cada $k(\tilde{x}) \in A[X]/_{<f(X)>}$.

Observemos agora que se i,j são elementos distintos de $\{1,2,\ldots,m\}$ então os homomorfismos g_i e g_j são distintos. Assim, aplicando II.2.21 (notar que como R não possui idempotentes próprios g_i e g_j são homomorfismos fortemente distintos sempre que $i \neq j$), existem idempo-

tentes $e_i \in A[X]/_{<f(X)>}$, com $i \in \{1,2,\ldots,m\}$, dois a dois ortogonais tais que $g_i(e_j) = \delta_{ij}$, e $g_i[k(\tilde{x})].e_i = k(\tilde{x})e_i$, para cada $k(\tilde{x}) \in A[X]/_{<f(X)>}$. Então, como $\text{posto}_A(A[X]/_{<f(X)>}) = n$ e $\overset{m}{\underset{i=1}{\oplus}} (A[X]/_{<f(X)>}) \subset A[X]/_{<f(X)>}$, temos que $m \leq \text{posto}_A[\overset{m}{\underset{i=1}{\oplus}} (A[X]/_{<f(X)>})] \leq n$, o que completa a prova da primeira parte.

Sejam $\alpha, \beta \in A$ raízes distintas de $f(X)$ em A . Podemos supor que $\alpha = \alpha_i$ e $\beta = \alpha_j$, para $i \neq j$, e consideremos novamente os idempotentes ortogonais obtidos acima, $e_1,\ldots,e_m \in A[X]/_{<f(X)>}$. Então sabemos que $\tilde{x}e_i = g_i(\tilde{x})e_i = \alpha_i e_i$, para cada $i \in \{1,2,\ldots,m\}$, ou seja, $(\tilde{x} - \alpha_i)e_i = 0$. Assim, $<\tilde{x} - \alpha_i>$ é um ideal contido no anulador de e_i em $\overline{A} = A[X]/_{<f(X)>}$. Reciprocamente se $p(\tilde{x}) \in An_{\overline{A}}(e_i)$, então $p(\tilde{x})e_i = 0$, e portanto, aplicando o homomorfismo g_i , tem-se que $p(\alpha_i) = 0$, já que $g_i(e_i) = 1$. Assim, $p(\tilde{x}) \in <\tilde{x} - \alpha_i>$, e, portanto, $<\tilde{x} - \alpha_i> = An_{\overline{A}}(e_i)$, para cada $i \in \{1,2,\ldots,m\}$.

Mostremos agora que os ideais $<X - \alpha_i>$ e $<X - \alpha_j>$ de $A[X]$ são comaximais para $i \neq j$. Vejamos antes que $<\tilde{x} - \alpha_i>$ e $<\tilde{x} - \alpha_j>$ são ideais comaximais de $\overline{A}$. De fato, $(1 - e_i)e_i = 0$ e, portanto, $1 - e_i \in An_{\overline{A}}(e_i) = <\tilde{x} - \alpha_i>$. Assim, como $e_i \in An_{\overline{A}}(e_j)$, vem que $1 = (1 - e_i) + e_i \in <\tilde{x} - \alpha_i> + <\tilde{x} - \alpha_j>$, ou seja, $\overline{A} = <\tilde{x} - \alpha_i> + <\tilde{x} - \alpha_j>$. Então existem elementos $p(\tilde{x}), q(\tilde{x}) \in \overline{A}$ tais que $p(\tilde{x})(\tilde{x} - \alpha_i) + q(\tilde{x})(\tilde{x} - \alpha_j) = 1$, ou ainda,

$p(X)(X-\alpha_i) + q(X)(X-\alpha_j) - 1 \in \langle f(X) \rangle$. Logo, como α_i é raiz de $f(X)$ em A , $[p(X) - k(X)](X - \alpha_i) + q(X)(X - \alpha_j) = 1$, para algum polinômio $k(X) \in A[X]$. Assim, $\langle X - \alpha_i \rangle$ e $\langle X - \alpha_j \rangle$ são ideais comaximais de $A[X]$. Portanto, aplicando o homomorfismo h_i na expressão acima, vem que $q(\alpha_i)(\alpha_i - \alpha_j) = 1$, ou seja, $(\alpha_i - \alpha_j) \in U(A)$ e a prova está completa. □

Corolário 2.15:

Se R é um anel sem idempotentes próprios e se n é um inteiro maior do que 1 e tal que $n.1_R \in U(R)$ então R tem no máximo n raízes n-ésimas da unidade.

Prova:

Pondo $f(X) = X^n - 1 \in R[X]$, por 2.12, vemos que $f(X)$ é um polinômio separável sobre R . Então, fazendo $A = R$ em 2.14, segue que $f(X)$ não possui mais do que n raízes em R . □

Queremos agora, para finalizar, analisar qual é a relação existente entre os polinômios separáveis sobre R e as imagens homomórficas de $R[X]$ (i.e., imagens de $R[X]$ por um epimorfismo) , no caso de R não conter idempotentes próprios. Na demonstração, utilizamos um resultado de [13], cuja prova omitiremos por razões de espaço.

Corolário 2.16:

Suponhamos que R não possui idempotentes pró-

prios. Sejam T uma R-álgebra fortemente separável sem idempotentes próprios e α um elemento arbitrário de T. Então $R[\alpha]$ é uma R-subálgebra separável de T se e só se α é raiz de algum polinômio separável sobre R.

Prova:

É claro que se $f(X)$ é um polinômio separável sobre R tal que $f(\alpha) = 0$ então $R[\alpha]$ é também R-separável, pois é imagem homomórfica da R-álgebra separável $R[X]/_{<f(X)>}$.

Suponhamos agora que $R[\alpha]$ é uma R-álgebra separável. Sendo que T é uma R-álgebra fortemente separável, existe uma extensão de Galois T' de R, sem idempotentes próprios o que contém T (ver teor. 1.1 de [13]). Como $R[\alpha]$ é uma R-subálgebra de T, vemos que $R[\alpha]$ é também uma R-subálgebra de T'. Então podemos supor, sem perda de generalidade, que T é uma extensão de Galois de R.

Sejam G o grupo de Galois de T sobre R e H o subgrupo de G que deixa $R[\alpha]$ fixo. Então sabemos que $T^H = R[\alpha]$, por III.2.2.

Sejam $\sigma_1 = id_T, \sigma_2, \ldots, \sigma_r$ representantes de todas as r classes laterais à esquerda distintas de H em G, e seja $f(X) = \prod_{i=1}^{r} [X - \sigma_i(\alpha)]$. Podemos observar então que, para cada $\sigma \in G$, $\sigma[f(X)] = \prod_{i=1}^{r} [X - \sigma\sigma_i(\alpha)]$. Além disso, para cada $i \in \{1,2,\ldots,r\}$, existe um índice j e um elemento $\zeta_j \in H$ tais que $\sigma\sigma_i = \sigma_j\zeta_j$ e é claro que, se $i \neq j$, então

$\sigma\sigma_i$ e $\sigma\sigma_j$ são elementos de classes laterais distintas. Portanto, $\sigma[f(X)] = \prod_{j=1}^{r} [X - \sigma_j\zeta_j(\alpha)] = \prod_{j=1}^{r} [X - \sigma_j(\alpha)] = f(X)$, donde segue-se que cada $\sigma \in G$ deixa os coeficientes de $f(X)$ fixos. Assim, $f(X) \in T^G[X] = R[X]$. Ainda, como $\sigma_1 = id_T$, é claro que $f(\alpha) = 0$. Logo, resta-nos mostrar apenas que $f(X)$ é um polinômio separável sobre R.

Para tal, é suficiente mostrarmos que $\sigma_i(\alpha) - \sigma_j(\alpha) \in U(T)$, sempre que $i \neq j$. Suponhamos que existam $i,j \in \{1,2,\ldots,r\}$, com $i \neq j$ e tais que $\sigma_i(\alpha) - \sigma_j(\alpha) \notin U(T)$. Então, pondo $\sigma_i^{-1}\sigma_j = \sigma$, vem que $\alpha - \sigma(\alpha) = \sigma_i^{-1}[\sigma_i(\alpha) - \sigma_j(\alpha)] \notin U(T)$. Vamos chegar a uma contradição, mostrando que $\sigma \in H$.

Seja M um ideal maximal de T que contém o elemento $\alpha - \sigma(\alpha)$. Então, para cada inteiro positivo m,

$$\alpha^m - \sigma(\alpha^m) = (\alpha - \sigma(\alpha))[\alpha^{m-1} + \alpha^{m-2}\sigma(\alpha) + \alpha^{m-3}\sigma(\alpha^2) + \ldots + \sigma(\alpha^{m-1})] \in M .$$

Assim, para cada $\beta = \sum_{i=0}^{m} r_i\alpha^i \in R[\alpha]$, $\beta - \sigma(\beta) = \sum_{i=0}^{m} r_i(\alpha^i - \sigma(\alpha^i)) \in M$

Consideremos agora a função traço $t : T \to R$, que é dada por $t(x) = \sum_{\rho \in G} \rho(x)$, já que T é uma extensão de Galois de R. Além disso, por III.1.5, existe um elemento $c_0 \in T$ tal que $t(c_0) = 1$, e, por III.1.4., existem elementos $x_i, y_i \in T$ $(i=1,2,\ldots,n)$ tais que $\sum_{i=1}^{n} x_i\rho(y_i) = \delta_{1\rho}$, para cada $\rho \in G$. Definimos então

$$c = \sum_{i=1}^{r} \sigma_i(c_0)$$

$u_i = \sum_{\zeta \in H} \zeta(c\, x_i)$

$v_i = \sum_{\zeta \in H} \zeta(y_i)$, para cada $i \in \{1,2,\ldots,n\}$. Então, como H é um subgrupo de G , é claro que $\gamma(u_i) = u_i$ e $\gamma(v_i) = v_i$, para cada $\gamma \in H$, donde $u_i, v_i \in T^H = R[\alpha]$. Ainda, para cada $\gamma \in H$, $\sum_{i=1}^{n} u_i \gamma(v_i) = \sum_{i=1}^{n} u_i v_i =$

$$= \sum_{i=1}^{n} \Big[\sum_{\zeta \in H} \zeta(c\, x_i)\Big] \Big[\sum_{\eta \in H} \eta(y_i)\Big] = \sum_{\eta,\zeta \in H} \sum_{i=1}^{n} \zeta(c\, x_i)\, \eta(y_i) =$$

$$= \sum_{\eta,\zeta \in H} \zeta(c)\delta_{\zeta\eta} = \sum_{\zeta \in H} \zeta(c) = \sum_{\zeta \in H} \sum_{i=1}^{r} \zeta\sigma_i(c_0) = \sum_{\rho \in G} \rho(c_0) = 1 \ .$$

Por outro lado, se $\gamma \in G - H$, temos que $\gamma = \sigma_j \pi$, para algum $j \neq 1$ e $\pi \in H$, e então

$$\sum_{i=1}^{n} u_i \gamma(v_i) = \sum_{i=1}^{n} \Big[\sum_{\zeta \in H} \zeta(c\, x_i)\Big] \Big[\sum_{\eta \in H} \gamma\eta(y_i)\Big] = \sum_{\eta,\zeta \in H} \sum_{i=1}^{n} \zeta(c\, x_i)\, \gamma\eta(y_i) =$$

$$= \sum_{\eta,\zeta \in H} \zeta(c)\delta_{\zeta,\gamma\eta} = 0 \ , \text{ pois } \zeta \neq \gamma\eta \text{ , para } \zeta,\eta \in H \ .$$

Logo, $\sum_{i=1}^{n} u_i \gamma(v_i) = \delta_{H\gamma}$, onde $\delta_{H\gamma} = 1$, se $\gamma \in H$, e $\delta_{H\gamma} = 0$, se $\gamma \notin H$. Portanto, se $\sigma \notin H$, então

$1 = \sum_{i=1}^{n} u_i v_i - \sum_{i=1}^{n} u_i \sigma(v_i) = \sum_{i=1}^{n} u_i (v_i - \sigma(v_i)) \in M$, uma contradição. Concluimos que $\sigma \in H$, o que completa a prova. □

NOTA FINAL: Nos últimos anos, várias pesquisas têm sido realizadas abordando o estudo de separabilidade sobre anéis não

necessariamente comutativos. Em particular, problemas semelhantes aos assuntos abordados neste capítulo têm sido estudados para o caso dos chamados "Skew Polynomial Rings"(ver [4]). Rsultados correspondentes relacionados com a separabilidade, neste caso, podem ser encontrados em [9], [11], [14], [16] [17], [20], [21], [22] e [23].

RESUMO

Define-se álgebra separável sobre um anel comutativo com unidade e mostra-se que este conceito generaliza o conceito de separabilidade envolvido na teoria de corpos. Faz-se um estudo detalhado sobre as extensões separáveis que são quocientes de anéis de polinômios. Em particular, obtem-se diversas caracterizações de polinômios separáveis.

ABSTRACT

A separable algebra over a commutative ring is defined and it is shown that this concept generalizes the one involved in Field Theory. A detailed study of the separable extensions which are quotients of polynomial rings is presented here. In particular, one obtains several characterizations for separable polynomials.

REFERÊNCIAS

[1] ARTIN,E. Galois theory. 2ed. London, University of Notre Dame Press |c1971| 82p.

[2] ATIYAH, M.F. and MACDONALD, I.G. Introduction to commutative algebra. Reading, Addison-Wesley |c1969| 128p.

[3] AUSLANDER, M. and GOLDMAN, O. "The Brauer group of a commutative ring" Trans. Amer. Math. Soc., Providence, Rhode Island, 97:367-409, 1960.

[4] BAUMVOL, G.K. Isomorfismos de anéis de polinômios. Porto Alegre, Instituto de Matemática da UFRGS, 1979. 130p. [Dissertação de Mestrado].

[5] BOURBAKI, N. "Algèbre". In: __. Éléments de Mathématique. Paris , Hermann,1970. v.1 cap.1-3 p.1-258.

[6] CHASE, S., HARRISON, D.K. and ROSENBERG, A. "Galois theory and cohomology of commutative rings" Mem. Amer.Math. Soc., Providence, Rhode Island, 52:15-33, 1965.

[7] DEMEYER, F. and INGRAHAM, E. "Separable algebras over commutative rings" Lecture Notes in Mathematics,New York, 181:1-114, 1971.

[8] ELKINS, B.L. "Characterization of separable ideals" Pacific J. Math., Berkeley, California, 34:45-49, 1970.

[9] FERRERO, M.A. and KISHIMOTO, K. "Separable polynomials over skew polynomial rings of derivation type" (datilog.).

[10] HERSTEIN, I. N. Topics in Algebra. New York, Blaisdell, 1964. 342p.

[11] IKEHATA, S. "A note on separable polynomials in skew polynomial rings" Math. J. Okayama University, Okayama, 22:59-60, 1980.

[12] IKEHATA, S. "On separable polynomials and Frobenius polynomials in skew polinomial rings" Math. J. Okayama Univ., Okayama, 22:115-129, 1980.

[13] JANUSZ, G. J. "Separable algebras over commutative rings" Trans. Amer. Math. Soc., Providence, Rhode Island, 122: 461-79, 1966.

[14] KISHIMOTO, K. "On abelian extensions of rings II" Math. J. Okayama Univ., Okayama, 15:57-70, 1971.

[15] MILLIES, F. C. P. Anéis e módulos. São Paulo, Instituto de Matemática e Estatística da Universidade de São Paulo, 1972. 199p.

[16] MIYASHITA, Y. "On a skew polynomial ring" J. Math. Soc. Japan, Tokyo, 31:317-30, 1979.

[17] NAGAHARA, T. "A note on separable polynomials in skew polynomial rings of automorphism type" Math. J. Okayama Univ.,Okayama, 22:73-76, 1980.

[18] NAGAHARA, T. "Characterization of separable polynomials over a commutative ring" Proc. Japan Acad., 46:1011-15, 1970.

[19] NAGAHARA, T. "On separable polynomials over a commutative ring" Math. J. Okayama Univ., Okayama, 14(2):175-81, dec., 1970.

[20] NAGAHARA, T. "On separable polynomials of degree 2 in skew polynomial rings" Math. J. Okayama Univ., Okayama, 19:65-95, 1976.

[21] NAGAHARA, T. "On separable polynomials of degree 2 in skew polynomial rings II" Math. J. Okayama Univ., Okayama, 21:166-77, 1979.

[22] NAGAHARA, T. "On separable polynomials of degree 2 in skew polynomial rings III" Math. J. Okayama Univ., Okayama, 22:61-64, 1980.

[23] NAGAHARA, T. "Supplements to the previous paper 'On separable polynomials of degree 2 in skew polynomial rings'" Math. J. Okayama Univ., Okayama, 19:159-161, 1977.

[24] NORTHCOTT, D.G. A first course of homological algebra. London, Cambridge University, 1973. 206p.

[25] RIBENBOIM, P. Rings and modules. New York, Interscience, 1969. 162p.

[26] SERRE, J.P. Corps locaux. Paris, Hermann, 1962. 243p.

[27] STEWART, I. Galois theory. London, Chapman and Hall, 1973. 226p.

[28] WAERDEN, B. L. V. D. Algebra. 4ed. Berlin, Springer, 1959. 264p.