Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Programa de Pós-Graduação em Matemática

Érica Isabel dos Santos [†]

Álgebras de Azumaya e o produto cruzado por uma ação parcial torcida

Campina Grande - PB

2024

[†]Este trabalho contou com apoio financeiro da Capes.

Érica Isabel dos Santos

Álgebras de Azumaya e o produto cruzado por uma ação parcial torcida

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática da Universidade Federal de Campina Grande, pertencente à linha de pesquisa Álgebra e área de concentração Matemática como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Prof. Dra. Josefa Itailma da Rocha

Campina Grande - PB

2024

S237p Santos, Érica Isabel dos.

Álgebras de Azumaya e o produto cruzado por uma ação parcial torcida / Érica Isabel dos Santos. – Campina Grande, 2024.

122 f. : il.

Dissertação (Mestrado em Matemática) – Universidade Federal de Campina Grande, Centro de Ciências e Tecnologia, 2024.

"Orientação: Profa. Dra. Josefa Itailma da Rocha".

Referências.

1. Álgebras de Azumaya. 2. Produto Cruzado Parcial. 3. Teoria de Galois. 4. Ação Parcial Torcida. 5. H-separabilidade. I. Rocha, Josefa Itailma da. II. Título.

CDU 512(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

Álgebras de Azumaya e o produto cruzado por uma ação parcial torcida

por

Érica Isabel dos Santos

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada em: 15 de março de 2024

Prof. Dr. Mikhailo Dokuchaev - USP

Prof. Dr. Héctor Edonis Pinedo Tapia - Universidad Industrial de Santander

---

Prof. Dra. Josefa Itailma da Rocha - UFCG

Orientador

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Programa de Pós-Graduação em Matemática

Março - 2024

Agradecimentos

Inicialmente, agradeço a Deus por me dá força e coragem para enfrentar os obstáculos da vida e me permitir vivenciar este momento.

Aos meus pais, Cristina e Edival, e a minha irmã Maria Emília, que sempre me incentivaram a lutar pelos meus sonhos e estão comigo em todos os momentos. Aos meus primos Yasmim e João Henrique, que me proporcionam muitos momentos de alegria. A minha madrinha Lucivânia, aquela que sempre me impulsiona a seguir em frente e é um exemplo de determinação. Enfim, agradeço a todos os meus familiares.

Aos professores do curso de Matemática da UFCG (campus Cajazeiras), onde fiz a minha graduação, em especial, a Tonires Mélo e a Francielia Limeira, por tantas contribuições e por sempre me encorajarem em fazer uma pós-graduação.

A minha orientadora Josefa Itailma, pela orientação, dedicação e paciência durante este tempo de mestrado, onde a mesma contribuiu diretamente para a minha pesquisa e se tornou uma referência, assim como uma amiga que levarei para o resto da vida.

Aos professores da banca examinadora que contribuíram para a melhoria do nosso trabalho.

Aos amigos de graduação e pós-graduação, que se fizeram presentes em tantos momentos de estudos e boas conversas.

A CAPES pelo apoio financeiro.

Dedicatória

Aos meus pais, Edival Severiano
e Isabel Cristina.

Resumo

Um anel é chamado Azumaya se é uma extensão separável de seu centro. Neste trabalho, estudamos condições para que o produto cruzado parcial de um grupo finito G por uma ação parcial torcida α seja Azumaya. Os critérios abordados são obtidos por meio dos conceitos de H-separabilidade, separabilidade e extensões de Galois parcial. Trazemos o estudo detalhado das álgebras separáveis, em particular, das álgebras de Azumaya, e das extensões H-separáveis, buscando compreender as principais caracterizações desses conceitos e estabelecer relações entre eles.

Palavras-chave: Álgebras de Azumaya; Produto cruzado parcial; Teoria de Galois; Ação parcial torcida; H-separabilidade.

Abstract

A ring is called Azumaya if it is a separable extension of its center. In this work, we study conditions for the partial crossed product of a finite group G by a twisted partial action α to be Azumaya. The results are obtained through the concepts of H-separability, separability, and partial Galois extensions. We introduce a detailed study of separable algebras, in particular, Azumaya algebras, and H-separable extensions, to understand the main characterizations of these concepts and establish relationships between them.

Azumaya algebras; Partial crossed product; Galois theory; Twisted partial action; H-separability.

Sumário

Introdução

A teoria das álgebras separáveis sobre anéis comutativos tem forte ligação com todas as áreas da álgebra, incluindo a teoria algébrica dos números, a teoria dos anéis, a álgebra comutativa e a geometria algébrica. A partir disso, nos dedicamos ao estudo das álgebras separáveis e, em particular, das álgebras que são centrais separáveis, ou, álgebras de Azumaya, como também são chamadas. Em todo nosso estudo, consideraremos álgebras associativas sobre anéis comutativos.

Em 1960, M. Auslander e O. Goldman no artigo [3] apresentaram os fundamentos da teoria geral das álgebras separáveis sobre anéis comutativos arbitrários, teoria esta que generaliza a teoria clássica das álgebras centrais simples sobre corpos e o grupo de Brauer de um corpo. O artigo [3] se tornou a referência principal para a construção do material de F. DeMeyer e E. Ingraham [9], uma das referências primordiais para a elaboração do nosso trabalho. Das várias condições equivalentes da separabilidade na teoria clássica das álgebras separáveis sobre um corpo, existe aquela que é a mais adequada para generalização, segundo os autores. Dizemos que uma álgebra A sobre um anel comutativo R é separável se A for um módulo projetivo sobre sua álgebra envolvente $A^e = A \otimes_R A$. Ademais, dizemos que A é central se A é um R-módulo fiel e $R \cdot 1$ coincide com o centro de A. Ao lidar com álgebras fiéis, identificamos R com $R \cdot 1$ e, portanto, consideramos R como um subanel do centro de A. Uma R-álgebra A é uma álgebra de Azumaya se A é central e separável.

Muitas características importantes das álgebras separáveis serão estudadas, com ênfase para aquelas que são preservadas da teoria clássica. É mostrado que o produto tensorial de duas álgebras separáveis é ainda uma álgebra separável. A separabilidade é transitiva, ou seja, se A é separável sobre S e S é separável sobre R, então A é separável

sobre R. Além disso, uma álgebra A é separável sobre R se, e somente se, A é separável sobre seu centro $C(A)$ e $C(A)$ é separável sobre R ([9, Teorema 3.8]). Este fato mostra que o estudo da separabilidade pode ser dividido em dois casos: álgebras comutativas e álgebras centrais. O caso envolvendo as álgebras comutativas foi estudado com maior destaque por M. Auslander e D. A. Buchsbaum em [2]. Já em [3], os autores se dedicaram as álgebras que são centrais.

Em 1951, o matemático japonês Gorô Azumaya antecipou alguns dos resultados que tratam das propriedades formais das álgebras separáveis e do grupo de Brauer em [4]. No entanto, a definição dada por Azumaya de uma álgebra maximalmente central é uma versão local do que M. Auslander e O. Goldman chamam de álgebra central separável. Sendo assim, muitos dos resultados apresentados pelos autores acima citados podem ser deduzidos dos resultados de Azumaya.

O conceito de ações parciais surgiu na teoria de álgebra dos operadores. R. Exel em [13] introduziu a noção de uma ação parcial torcida de um grupo localmente compacto em uma C^*-álgebra e o produto cruzado correspondente a essa ação e provou também a associatividade desse produto cruzado parcial. Os estudos de R. Exel inspiraram outros trabalhos em torno do conceito de ações parciais. Em 2005, é iniciado por M. Dokuchaev e R. Exel o estudo das ações parciais em um contexto puramente algébrico. Utilizando a álgebra dos multiplicadores, M. Dokuchaev e R. Exel em [10] generalizam um resultado de Exel (1997) relacionado a associatividade do produto cruzado obtido no contexto de C^*-álgebras. Nesse caso, os autores apresentam condições para que o produto cruzado correspondente a uma ação parcial de um grupo em uma álgebra seja associativo. Já em 2008, M. Dokuchaev, R. Exel e J. Simón em [12] introduziram a noção de ações parciais torcidas de grupos em anéis abstratos e produtos cruzados correspondentes, mostrando também a associatividade desse produto cruzado.

No ano de 2007, M. Dokuchaev, A. Paques e M. Ferrero generalizam em [11] a teoria de Galois de Chase, Harrison e Rosenberg [8]. Com [11], os autores definem extensões parciais de Galois e provam um teorema que traz condições equivalentes para que tenhamos uma extensão de Galois parcial ([11, Teorema 4.1]). Além disso, definem a aplicação traço parcial e o subanel dos invariantes, sendo este último utilizado com frequência nos resultados principais.

O objetivo principal deste trabalho é investigar condições necessárias e suficientes

para que o produto cruzado parcial $S = R \rtimes_{\alpha,\omega} G$ por uma ação parcial torcida α de um grupo finito G em um anel R seja Azumaya, de acordo com [21]. Para isso, são necessários os conceitos de H-separabilidade, separabilidade e extensões de Galois parciais.

A noção de H-separabilidade foi introduzida na literatura por Hirata [16] e isso proporcionou uma nova visão para o estudo das extensões separáveis. Dada uma extensão de anéis $R \subseteq S$, dizemos que S é H-separável sobre R se $S \otimes_R S$ é isomorfo a um somando direto de uma soma direta finita de cópias de S como um S-bimódulo. Também podemos caracterizar as extensões de anéis H-separáveis por meio de um sistema de coordenadas, chamado de sistema H-separável [26].

Este trabalho está dividido em 4 capítulos. No primeiro Capítulo, apresentamos os conceitos básicos que serão utilizados em todo o trabalho, como o conceito de módulo, sequência exata, tipos especiais de módulos (projetivo, finitamente gerado, fiel, gerador, progerador), entre outros.

No Capítulo 2, trazemos o estudo das álgebras separáveis e suas respectivas propriedades, enfatizando que determinadas propriedades da teoria clássica são preservadas quando estamos trabalhando com este tipo de álgebra. As álgebras centrais separáveis (ou álgebras de Azumaya) ganham notoriedade neste capítulo. Para qualquer R-álgebra A temos que A pode ser considerada como um A^e-módulo à esquerda através do produto $(a \otimes b) \cdot x = axb$, para $a, x \in A$ e $b \in A^o$. Esta estrutura induz um homomorfismo de R-álgebras $\varphi : A^e \to Hom_R(A, A)$. Podemos caracterizar as álgebras de Azumaya a partir do homomorfismo φ e dos módulos progeradores ([9, Teorema 3.4]). Ainda neste capítulo, apresentamos a noção de H-separabilidade e suas principais caracterizações. Os resultados principais desse capítulo mostram que extensões H-separáveis são separáveis [16] e que todo anel que é Azumaya é H-separável sobre seu centro [24].

No Capítulo 3 nos dedicamos a estudar as ações parciais e a Teoria de Galois parcial para anéis comutativos. Como um dos exemplos fundamentais deste capítulo, trazemos a construção de uma ação parcial através de uma ação global dada. Baseando-se em [12], expomos a definição de ação parcial torcida de um grupo em uma álgebra (associativa e não necessariamente unitária) sobre um anel comutativo e unitário. É provado que o produto cruzado parcial correspondente é associativo. Por fim, apresentamos a definição e o resultado que caracteriza a extensão de Galois parcial.

No Capítulo 4, apresentamos os resultados de A. Paques e A. Sant'Ana [21] que

expressam condições para que o produto cruzado parcial por uma ação parcial torcida seja Azumaya. Os autores estendem os principais resultados de Alfaro e Szeto [1] e Carvalho [7] para o contexto de ações parciais torcidas, em termos de H-separabilidade, separabilidade e extensões parciais de Galois ([21, Teorema 2.4, Proposições 3.1, 3.2, 3.3 e 3.4]).

Capítulo 1

Preliminares

Neste capítulo, apresentamos os conceitos fundamentais utilizados durante toda a construção do trabalho, trazendo como referências principais [9] e [23]. Quando utilizamos o termo ideal, estamos nos referindo a ideais bilaterais, salvo indicação contrária. O estudo de módulos, que tem aplicações em diferentes áreas, está fortemente associado a ideia de espaços vetoriais. Apresentamos também alguns tipos especiais de módulos, como os livres, projetivos, finitamente gerados, geradores e progeradores. Os conceitos de sequência exata e sequência cinde são amplamente abordados. Como pré-requisitos para a leitura deste capítulo, estabelecemos os conceitos de grupo, anel e espaço vetorial.

1.1 Módulos

Definição 1.1 *Seja R um anel com unidade. Dizemos que um conjunto não vazio M é um módulo à esquerda sobre R, ou um R-módulo à esquerda, se M é um grupo abeliano com relação a uma operação que denotaremos por $+$, e está definida uma lei de composição externa que a cada par $(a, m) \in R \times M$ associa um elemento $a \cdot m \in M$, que satisfaz as seguintes condições:*

(i) $a_1 \cdot (a_2 \cdot m) = (a_1 a_2) \cdot m$,

(ii) $a_1 \cdot (m_1 + m_2) = a_1 \cdot m_1 + a_1 \cdot m_2$,

(iii) $(a_1 + a_2) \cdot m = a_1 \cdot m + a_2 \cdot m$,

(iv) $1 \cdot m = m$,

para todo $a_1, a_2 \in R$ e $m_1, m_2 \in M$.

De forma análoga, pode-se definir a noção de R-módulo à direita, considerando a multiplicação à direita por elementos do anel.

Exemplo 1.2 *(i) Todo espaço vetorial V sobre um corpo K é um K-módulo.*

(ii) Seja I um ideal á esquerda de um anel R. Então, I admite uma estrutura de R-módulo com a soma induzida pela soma de R e a multiplicação por escalares definida pela multiplicação de R, ou seja,

$$a \cdot x = ax,$$

para todo $a \in R$ e $x \in I$. Em particular, todo anel R pode ser considerado como um módulo sobre si mesmo, onde tomamos $R = I$.

(iii) Seja G um grupo abeliano. Indicaremos por $End(G)$ o conjunto de todos os endomorfismos de G. Pode-se definir em G uma estrutura de $End(G)$-módulo associando a cada par $(f, x) \in End(G) \times G$ o elemento $f \cdot x = f(x) \in G$.

Mais exemplos podem ser vistos em [23]. Essa diversidade de exemplos mostra as possíveis aplicações da teoria de módulos em outras áreas.

Definição 1.3 *Seja M um R-módulo. Um subconjunto $N \subset M$ diz-se um R-submódulo de M, ou simplesmente, um submódulo se:*

(i) N é um subgrupo aditivo de M.

(ii) N é fechado á multiplicação por escalares, isto é, para todo $a \in R$ e todo $n \in N$, tem-se que, $a \cdot n \in N$.

Exemplo 1.4 *(i) Seja V um espaço vetorial sobre um corpo K. Um subconjunto $S \subset V$ é um submódulo se, e somente se, S é um subespaço de V.*

(ii) Seja R um anel. Os R-submódulos de ${}_RR$ são seus ideais à esquerda.

(iii) Sejam N_1 e N_2 submódulos de um R-módulo M. O conjunto

$$N_1 + N_2 = \{n_1 + n_2 \mid n_1 \in N_1 \, e \, n_2 \in N_2\}$$

também é um submódulo de M, chamado submódulo soma de N_1 e N_2.

(iv) Seja M um R-módulo e $\{N_i\}_{i \in I}$ uma família de submódulos de M. Então $\bigcap_{i \in I} N_i$ também é um submódulo de M.

(v) Seja S um subconjunto de um R-módulo M, o conjunto

$$(S) = \left\{ \sum_i^n a_i s_i \mid n \in \mathbb{N}, a_i \in R, s_i \in S \right\}$$

é um submódulo de M chamado submódulo gerado por S.

Se $S = \{m\}$, com $m \in M$, o submódulo $(S) = (m)$ diz-se o módulo cíclico gerado por m.

Proposição 1.5 (Lei modular) *Sejam L, M e N submódulos de um módulo tal que $L \subseteq N$. Então,*

$$L + (M \cap N) = (L + M) \cap N.$$

Demonstração. Seja $z \in L + (M \cap N)$, então existem $x \in L$ e $y \in M \cap N$ tais que $z = x+y$. Como $x \in L$ e $L \subseteq N$, temos que $z = x+y \in N$. Além disso, $z = x+y \in L+M$, ou seja, $z \in (L + M) \cap N$, provando que $L + (M \cap N) \subseteq (L + M) \cap N$. Para a inclusão contrária, seja $z \in (L + M) \cap N$. Como $z \in L + M$, existem $x \in L$ e $y \in M$ tais que $z = x + y$. Observe que:

$$y = z - x \in N,$$

pois $z \in N$, $x \in L \subseteq N$ e N é um submódulo. Daí, $z = x + y \in L + (M \cap N)$. Portanto, vale a igualdade. ∎

Definição 1.6 *Um R-módulo M diz-se simples se $M \neq (0)$ e os únicos submódulos de M são (0) e o próprio M.*

Definição 1.7 *Sejam R um anel e M um R-módulo. O conjunto*

$$Anl_R(M) = \{a \in R \mid a \cdot m = 0, \forall m \in M\}$$

diz-se o anulador do módulo M. De forma análoga define-se anulador de um subconjunto de M. Um R-módulo M é dito fiel se $Anl_R(M) = \{0\}$.

Seja agora M um R-módulo e N um submódulo de M. Considerando apenas a estrutura de grupo abeliano de M podemos construir o módulo quociente $M/N = \{m+N \mid m \in M\}$ cuja estrutura de grupo abeliano é dada por

$$(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N$$

e a multiplicação por escalares de R é definida por

$$a \cdot (m + N) = (a \cdot m) + N.$$

A definição independe do representante. De fato, sejam $m_1+N = m_2+N$ em M/N, então $m_1 - m_2 \in N$. Como N é um submódulo de M, temos que

$$a \cdot (m_1 - m_2) = a \cdot m_1 - a \cdot m_2 \in N,$$

para todo $a \in A$. Assim, $(a \cdot m_1) + N = (a \cdot m_2) + N$ em M/N. Portanto, $a \cdot (m_1 + N) = a \cdot (m_2 + N)$.

Nessas condições, obtemos uma estrutura de A-módulo em M/N.

Definição 1.8 *Sejam M e N dois R-módulos. Uma aplicação $f : M \to N$ diz-se um homomorfismo de R-módulos, ou um R-homomorfismo, se para todos $m_1, m_2 \in M$ e todo $a \in R$ se verifica:*

(i) $f(m_1 + m_2) = f(m_1) + f(m_2)$,

(ii) $f(a \cdot m_1) = a \cdot f(m_1)$.

Dado um homomorfismo de R-módulos $f : M \to N$ chama-se imagem de f e núcleo (ou kernel) de f respectivamente os conjuntos:

$$Im(f) = \{n \in N \mid n = f(m), \text{ para algum } m \in M\},$$

$$ker(f) = \{m \in m \mid f(m) = 0\}.$$

É fácil ver que $Im(f)$ e $ker(f)$ são submódulos de N e M, respectivamente.

Exemplo 1.9 *(i) Homomorfismo inclusão: Seja N um submódulo de um R-módulo M. A aplicação $f : N \to M$ definida por $f(n) = n$, para todo $n \in N$, é um homomorfismo de R-módulos. Em particular, se $N = M$, temos o homomorfismo identidade sobre o R-módulo M, que iremos denotar por I_M.*

(ii) Homomorfismo canônico: Seja N um submódulo de um R-módulo M. A aplicação $\pi : M \to M/N$ definida por $f(m) = m+N$, para todo $m \in M$, é um homomorfismo de R-módulos. Além disso, temos que π é sobrejetor e $ker(\pi) = N$.

Definição 1.10 *Um homomorfismo de R-módulos $f : M \to N$ é dito um*

(a) Epimorfismo se f for sobrejetor;

(b) Monomorfismo se f for injetor.

Claramente, um R-homomorfismo $f : M \to N$ é um R-epimorfismo se, e somente se, $Im(f) = N$. Da mesma forma, f é um R-monomorfismo se, e somente se, $ker(f) = \{0\}$.

Na próxima proposição, são apresentadas propriedades elementares dos R-homomorfismos.

Proposição 1.11 *(i) Sejam* $M \xrightarrow{f} M' \xrightarrow{g} M''$ *R-homomorfismos. Então* $g \circ f : M \to M''$ *é um R-homomorfismo.*

(ii) Se $M \xrightarrow{f} M' \xrightarrow{g} M'' \xrightarrow{h} M'''$ *são R-homomorfismos, então*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

(iii) Sejam $M \xrightarrow{f_1} M' \xrightarrow{g} M''$ *e* $M \xrightarrow{f_2} M' \xrightarrow{g} M''$ *homomorfismos de R-módulos, então*

$$g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2.$$

Em condições análogas vale:

$$(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f.$$

(iv) Dado um R-homomorfismo $f : M \to N$*, então:*

$$I_N \circ f = f \quad e \quad f \circ I_M = f.$$

(v) Dados R-homomorfismos $M \xrightarrow{f} M' \xrightarrow{g} M$ *tais que* $g \circ f = I_M$*, então* f *é um monomorfismo e* g *é um epimorfismo.*

Demonstração. A demonstração dos itens $(i) - (iv)$ é imediata. Vamos demonstrar apenas (v). Para isso, sejam $x_1, x_2 \in M$ tais que $f(x_1) = f(x_2)$. Então, $g \circ f(x_1) = g \circ f(x_2)$, ou seja, $I_M(x_1) = I_M(x_2)$ e daí $x_1 = x_2$, provando que f é monomorfismo.

Agora, seja $x \in M$. Temos $I_M(x) = x$ e $g \circ f(x) = x$. Tomando $y = f(x) \in M'$, segue que $g(y) = x$ e portanto g é um epimorfismo. ■

Definição 1.12 *Um R-homomorfismo* $f : M \to N$ *diz-se um R-isomorfismo se existe um R-homomorfismo* $g : N \to M$ *tal que*

$$g \circ f = I_M \quad e \quad f \circ g = I_N.$$

Neste caso, dizemos que M *e* N *são isomorfos e denotaremos por* $M \simeq N$*.*

Proposição 1.13 *Um R-homomorfismo* $f : M \to N$ *é um isomorfismo se, e somente se,* f *é simultaneamente, monomorfismo e epimorfismo.*

Demonstração. [23, Proposição 2.1.3]. ■

Teorema 1.14 (Teorema do Homomorfismo para módulos) *Sejam* M *e* N *R-módulos,* $f : M \to N$ *um R-homomorfismo,* $\pi : M \to M/ker(f)$ *a projeção canônica ao quociente e* $i : Im(f) \to N$ *a inclusão. Existe uma única função*

$$f^* : M/ker(f) \to Im(f)$$

tal que:

(i) $f = i \circ f^* \circ \pi$.

(ii) f^* *é um isomorfismo.*

A relação entre as funções do enunciado pode-se visualizar no diagrama abaixo:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ M/\ker(f) & \xrightarrow[f^*]{} & Im(f) \end{array}$$

Demonstração. [23, Teorema 2.1.1]. ∎

Corolário 1.15 *Se* $f : M \to N$ *é um* R*-epimorfismo, então* $M/ker(f) \simeq N$.

1.2 Sequências exatas

Definição 1.16 *Sejam* F, G *e* H *três* R*-módulos e* $f : F \to G$, $g : G \to H$ R*-homomorfismos. Diz-se que o diagrama:*

$$F \xrightarrow{f} G \xrightarrow{g} H$$

é uma sequência exata em G *se* $Im(f) = ker(g)$.

Observação 1.17 *No contexto acima, a condição* $Im(f) \subset ker(g)$ *é equivalente a* $g \circ f = 0$.

Definição 1.18 *Seja* $\{\ldots, M_{i-1}, M_i, M_{i+1}, \ldots\}$ *uma família, eventualmente infinita, de* R*-módulos e* $\{\ldots, f_i : M_i \to M_{i+1}, \ldots\}$ *uma família de* R*-homomorfismos. Diz-se que o diagrama:*

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$$

é uma sequência exata se é exata em $M_i, \forall i \in I$, *isto é, se* $Im(f_{i-1}) = ker(f_i), \forall i \in I$.

Exemplo 1.19 *(i) A sequência* $0 \longrightarrow E \xrightarrow{f} G$ *é exata se, e somente se,* f *é um* R*-monomorfismo.*

(ii) A sequência $0 \xrightarrow{f} E \longrightarrow G$ *é exata se, e somente se,* f *é um* R*-epimorfismo.*

(iii) A sequência $0 \longrightarrow E \xrightarrow{f} F \longrightarrow 0$ *é exata se, e somente se,* f *é um isomorfismo.*

(iv) A sequência $0 \longrightarrow M \longrightarrow 0$ *é exata se, e somente se,* $M = 0$.

(v) Em geral, se E *é um submódulo de um* R*-módulo* F *e indicamos por* $i : E \to F$ *a inclusão e por* $\pi : F \to F/E$ *a projeção canônica, então a sequência*

$$0 \longrightarrow E \xrightarrow{i} F \xrightarrow{\pi} F/E \to 0$$

é exata.

1.3 Somas e produtos diretos

Dados dois R-módulos M e N, pode-se obter um novo R-módulo considerando o conjunto de todos os pares ordenados da forma (m, n) onde $m \in M$ e $n \in N$, e definindo:

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

$$a(m, n) = (am, an).$$

Seja $\{M_i\}_{i \in I}$ uma família de R-módulos e $M = \prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i\}$ o produto cartesiano dos membros da família. Em M pode-se introduzir uma estrutura de R-módulo definindo as operações por:

$$(m_i)_{i \in I} + (m'_i)_{i \in I} = (m_i + m'_i)_{i \in I},$$

$$a(m_i)_{i \in I} = (am_i)_{i \in I}.$$

O R-módulo construído acima diz-se o produto cartesiano ou direto da família $\{M_i\}_{i \in I}$.

Agora, sejam $\{M_i\}_{i \in I}$ uma família de R-módulos e $M = \prod_{i \in I} M_i$. Uma família $(m_i)_{i \in I} \in M$ diz-se uma família *quase-nula* se $m_i = 0$ exceto para um número finito de índices. No conjunto das famílias quase nulas de M pode-se introduzir uma estrutura de R-módulo, por restrição de operações de M (já que a soma de famílias quase nula é quase nula e produto de uma família quase nula por um escalar também é quase nula).

Definição 1.20 *Seja $\{M_i\}_{i \in I}$ uma família de R-módulos. O conjunto das famílias quase nulas de $M = \prod_{i \in I} M_i$, com a estrutura de R-módulo definida pela restrição das operações de M, chama-se soma direta externa da família e se indica pelo símbolo $\dot{\bigoplus_{i \in I}} M_i$.*

Quando $I = \{1, 2, \ldots, n\}$, a soma e o produto direto da família $\{M_i\}_{i \in I}$ coincidem.

A noção de soma direta interna está fortemente associada a ideia vista em espaços vetoriais. Um R-módulo M é soma direta interna de uma família $\{M_i\}_{i \in I}$ de submódulos se todo elemento de M se escreve, de uma única forma, como soma de elementos dos submódulos M_i. Podemos caracterizar a noção de soma direta interna de outra forma, como em [23].

Proposição 1.21 *Seja $\{M_i\}_{i \in I}$ uma família de submódulos de um R-módulo M. As seguintes afirmações são equivalentes:*

(i) Todo elemento $m \in M$ se escreve de um único modo na forma $m = \sum_{i \in I} m_i$, onde $m_i \in M_i \, \forall i \in I$ e a família $(m_i)_{i \in I}$ é quase nula.

(ii) $M = \sum_{i\in I} M_i$ *e, se* $\sum_{i\in I} m_i = 0$ *com* $m_i \in M_i$*, tem-se* $m_i = 0, \forall i \in I$.

(iii) $M = \sum_{i\in I} M_i$ *e* $M_j \cap \sum_{i\neq j} M_i = (0), \forall j \in I$.

Demonstração. [23, Proposição 2.4.1]. ∎

Definição 1.22 *Um R-módulo M diz-se soma direta interna de uma família* $\{M_i\}_{i\in I}$ *de submódulos se estiver verificando alguma (e portanto todas) das condições equivalentes da proposição acima.*

Para indicar que M é a soma direta interna dos submódulos $\{M_i\}_{i\in I}$ usaremos o símbolo

$$M = \bigoplus_{i\in I} M_i$$

e se, $I = \{1, 2, \ldots, n\}$ escreveremos

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n.$$

As proposições 2.4.2 e 2.4.3 de [23] mostram que existe uma correspondência entre somas diretas externas e internas. Por causa disso, é frequente não distingui-las e usar indistintamente o símbolo $\oplus$ para ambas.

Definição 1.23 *Seja N um submódulo de um R-módulo M. Diz-se que um submódulo* $N_1 \subset M$ *é um suplementar de N se* $M = N \oplus N_1$*. Um submódulo, que admite um suplementar, diz-se um somando direto de M.*

Definição 1.24 *Seja M um R-módulo. Um R-homomorfismo* $p : M \to M$ *diz-se um projetor se* $p^2 = p$ *(onde* $p^2 = p \circ p$*).*

O próximo resultado é bastante útil quando queremos mostrar que um certo submódulo é um somando direto.

Lema 1.25 *Seja N um submódulo de um R-módulo M. Então N é um somando direto de M se, e somente se, existir um endomorfismo* $f : M \to M$ *tal que* $f \circ f = f$ *e* $Im(f) = N$.

Demonstração. Suponha que N é um somando direto de M. Então, $M = N \oplus N'$, para algum N' submódulo de M. Consideremos $f : M = N \oplus N' \to N$ dada por $f(n+n') = n$, onde $n \in N$ e $n' \in N'$. Claramente f é um homomorfismo com $Im(f) = N$. Agora, seja $m \in M$, com $m = n + n'$, para $n \in N$ e $n' \in N'$. Veja que:

$$f(f(m)) = f(f(n + n')) = f(n) = f(n + n') = f(m).$$

Logo, $f^2 = f$.

Reciprocamente, suponha que existe um endomorfismo $f : M \to M$ tal que $f \circ f = f$ e $Im(f) = N$. Temos que $M = ker(f) \oplus Im(f)$, pois:
(i) $M = ker(f) + Im(f)$. De fato, inicialmente, observe que para todo $m \in M$, tem-se que $m - f(m) \in ker(f)$, uma vez que

$$f(m - f(m)) = f(m) - f(f(m)) = f(m) - f(m) = 0.$$

Além disso, podemos ver todo elemento $m \in M$ como

$$m = (m - f(m)) + f(m) \in ker(f) + Im(f).$$

(ii) $ker(f) \cap Im(f) = \{0\}$. Seja $m \in Im(f) \cap ker(f)$, então existe $m' \in M$ tal que $f(m') = m$. Sendo $f(m) = 0$, veja que:

$$f(f(m')) = f(m) \Rightarrow f(m') = 0 \Rightarrow m = 0.$$

Portanto, $M = ker(f) \oplus Im(f)$. Como $Im(f) = N$, temos o resultado desejado.

■

Agora, estudaremos uma relação entre somas diretas e sequências exatas.

Definição 1.26 *Diz-se que uma sequência exata de R-módulos*

$$0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$$

cinde se $E' = Im(f) = ker(g)$ é um somando direto de F.

O resultado a seguir se destaca como um dos mais importantes dessa seção, pois apresenta uma caracterização de quando uma determinada sequência exata cinde.

Proposição 1.27 *Dada uma sequência exata de R-módulos*

$$0 \longrightarrow E \xrightarrow{f} F \xrightarrow{g} G \longrightarrow 0$$

as seguintes afirmações são equivalentes:

(i) A sequência cinde;

(ii) Existe um R-homomorfismo $\psi : F \to E$ tal que $\psi \circ f = I_E$;

(iii) Existe um R-homomorfismo $\phi : G \to F$ tal que $g \circ \phi = I_G$;

Nestas condições, $F \simeq E \oplus G$.

Demonstração.

$(i) \Rightarrow (ii)$ Denotando $E' = Im(f)$, já que a sequência cinde, deve existir um submódulo E'' de F tal que $F = E' \oplus E''$. Podemos definir ψ da seguinte forma: dado $x \in F$, escreva $x = x' + x''$, com $x' \in E'$ e $x'' \in E''$. Como f é injetora (sequência exata), existe um único $y \in E$ tal que $f(y) = x'$. Definimos então $\psi(x) = \psi(f(y) + x'') = y$. É imediato verificar que ψ é um R-homomorfismo. Dado $y \in E$, temos que $f(y) \in E'$ e se escreve da forma $f(y) = f(y) + 0$. Assim,

$$\psi(f(y)) = \psi(f(y) + 0) = y$$

e portanto $\psi \circ f = I_E$.

$(ii) \Rightarrow (i)$ Vamos mostrar que $F = Im(f) \oplus ker(\psi)$. De fato, dado $x \in F$ considere $y = f \circ \psi(x) \in F$ e tome $z = x - y \in F$. Então $x = y + z$ com $y \in Im(f)$. Vamos mostrar que $z \in ker(\psi)$. Observe que:

$$\psi(z) = \psi(x) - \psi(y) = \psi(x) - \psi \circ f \circ \psi(x) = \psi(x) - I_E(\psi(x)) = \psi(x) - \psi(x) = 0.$$

Logo, $F = Im(f) + ker(\psi)$. Agora, seja $y \in Im(f) \cap ker(\psi)$. Então existe $x \in E$ tal que $f(x) = y$. Assim,

$$0 = \psi(y) = \psi(f(x)) = I_E(x) = x$$

e portanto $y = f(x) = 0$.

$(i) \Rightarrow (iii)$ Escrevendo novamente $F = E' \oplus E''$, onde $E' = ker(g)$, definimos $\phi : G \to F$ por: dado $y \in G$, como g é sobrejetora, existe $x \in F$ tal que $g(x) = y$. Escreva $x = x' + x''$, onde $x' \in E' = ker(g)$ e $x'' \in E''$, assim

$$y = g(x) = g(x') + g(x'') = 0 + g(x'') = g(x'').$$

Defina então $\phi(y) = x''$. Daí, $g \circ \phi = I_G$.

$(iii) \Rightarrow (i)$ Nessas condições, conseguimos mostrar que $F = ker(g) \oplus Im(\phi)$, utilizando um raciocínio análogo ao que fizemos anteriormente.

Como $\psi \circ f = I_E$ e $g \circ \phi = I_G$, pela Proposição 1.11 (v), f e ϕ são injetoras. Pelo Teorema 1.14, temos que

$$E \simeq \frac{E}{ker(f)} \simeq Im(f) \quad \text{e} \quad G \simeq \frac{G}{ker(\phi)} \simeq Im(\phi).$$

Logo, $E \simeq Im(f) = ker(g)$ e $G \simeq Im(\phi)$. Sendo $F = ker(g) \oplus Im(\phi)$, segue que

$$F \simeq E \oplus G.$$

■

Observação 1.28 *Considere a sequência exata de R-módulos $0 \longrightarrow E \xrightarrow{f} F$. Pela proposição acima, se existir um R-homomorfismo $g : F \to E$ tal que $g \circ f = I_E$, então a sequência cinde. Além disso, temos que $F = Im(f) \oplus ker(g)$.*

1.4 Módulos progeradores

Vamos considerar anéis associativos que possuem unidade 1. Além disso, assumiremos que os subanéis contêm a unidade do anel superior e que um homomorfismo de anéis de R para S leva a identidade de R à unidade de S. Quando nos referirmos a módulos estamos falando de módulos à esquerda.

Dado um anel R, denotaremos por $R^{(I)}$ o conjunto de todas as famílias quase-nulas $(\lambda_i)_{i\in I}$ onde $\lambda_i \in R, \forall i \in I$. Note que $R^{(I)}$ é uma soma direta $\oplus_{i\in I} R_i$ onde cada somando é igual a R.

Definição 1.29 *Seja $\{x_i\}_{i\in I}$ uma família de elementos de um R-módulo M. Diz-se que um elemento $x \in M$ é uma combinação linear dos elementos da família, se existe $(\lambda_i)_{i\in I} \in R^{(I)}$ tal que*

$$x = \sum_{i\in I} \lambda_i x_i.$$

A soma acima está bem definida, pois só um número finito de parcelas é diferente de zero.

Dado um subconjunto S de M, vimos pelo Exemplo 1.4 (v) que o submódulo gerado por S é, precisamente, o conjunto de todas as combinações lineares de elementos de S.

Definição 1.30 *Uma família $\{x_i\}_{i\in I}$ de elementos de um R-módulo M diz-se linearmente independente ou livre se para toda $(\lambda_i)_{i\in I} \in R^{(I)}$ tem-se que:*

$$\sum_i \lambda_i x_i = 0 \, implica \, \lambda_i = 0 \, para \; todo \, i \in I.$$

Definição 1.31 *Uma família $\{x_i\}_{i\in I}$ de elementos de um R-módulo M diz-se uma base de M se é uma família linearmente independente e gera M.*

Definição 1.32 *Um R-módulo M diz-se livre se ele contém uma base.*

Exemplo 1.33 *(i) Todo espaço vetorial sobre um corpo K é um K-módulo livre.*

(ii) Se R é um anel com unidade, o R-módulo ${}_RR$ é livre e o conjunto $\{1\}$ é uma base.

(iii) Dado um anel R consideremos a soma direta $R^{(I)}$. Indicaremos por e_k o elemento $e_k = (x_i)_{i\in I}$ onde $x_k = 1$ e $x_i = 0$ se $i \neq k$. A família $\{e_k\}_{k\in I}$ é uma base de $R^{(I)}$, chamada sua base canônica.

Definição 1.34 *Dizemos que um R-módulo M é finitamente gerado se existe uma família $\{x_1, \ldots, x_n\}$ de elementos de M tal que todo outro $x \in M$ é da forma $x = \sum_{i=1}^{n} \lambda_i x_i$ com $\lambda_i \in R, 1 \leq i \leq n$.*

A proposição seguinte mostra que para definirmos um homomorfismo de R-módulos $f : M \to N$, sendo M livre, é suficiente definirmos em uma base.

Proposição 1.35 *Sejam M e N R-módulos. Suponhamos M livre e seja $X = \{x_i\}_{i\in I}$ uma base de M. Dada uma função $f : X \to N$ sempre é possível estender f a um R-homomorfismo $\overline{f} : M \to N$. Tal homomorfismo é único.*

Demonstração. Seja

$$\begin{array}{rccc} f: & X & \to & N \\ & x_i & \mapsto & f(x_i) \end{array}.$$

Como X é base de M, então todo elemento de M se escreve de forma única como $m = \sum_i \lambda_i x_i$, com $(\lambda_i)_{i\in I} \in R^{(I)}$. Defina $\overline{f}$ da seguinte forma

$$\begin{array}{rccc} \overline{f}: & M & \to & N \\ & m & \mapsto & \sum_i \lambda_i f(x_i) \end{array}.$$

É imediato verificar que $\overline{f}$ é um R-homomorfismo. Dado $x_i \in X$, temos que $x_i = 1x_i$. Agora, veja que:

$$\overline{f}(x_i) = \overline{f}(1x_i) = 1f(x_i) = f(x_i).$$

Logo, $\overline{f} = f$. Mostraremos agora a unicidade de $\overline{f}$. Seja $g : M \to N$ um R-homomorfismo tal que $g(x_i) = f(x_i)$, para todo $x_i \in X$. Considere $m = \sum_i \lambda_i x_i \in M$. Aplicando g em M, temos:

$$\begin{aligned} g(m) &= g\left(\sum_i \lambda_i x_i\right) = \sum_i \lambda_i g(x_i) \\ &= \sum_i \lambda_i f(x_i) = \overline{f}\left(\sum_i \lambda_i x_i\right) \\ &= \overline{f}(m). \end{aligned}$$

Portanto, $\overline{f}$ é única e temos o resultado. ∎

Como consequência da proposição acima, temos que se M é um R-módulo livre com base $X = \{x_i\}_{i \in I}$, então M é isomorfo a $R^{(I)}$.

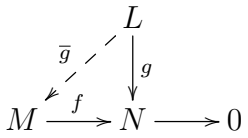
O próximo resultado mostra que todo R-módulo é a imagem homeomórfica de um R-módulo livre.

Proposição 1.36 *Todo R-módulo M é isomorfo a um quociente de um R-módulo livre.*

Demonstração. [23, Proposição 2.5.3]. ∎

Proposição 1.37 *Seja L um R-módulo livre. Dados dois R-módulos M e N, um epimorfismo $f : M \to N$ e um homomorfismo $g : L \to N$ sempre existe um homomorfismo $\overline{g} : L \to M$ tal que $f \circ \overline{g} = g$.*

Em outras palavras, dado o diagrama com traços contínuos abaixo, sempre existe $\overline{g}$, que faz com que o diagrama abaixo seja comutativo:

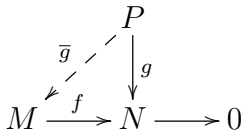


Demonstração. Como L é um R-módulo livre, L tem uma base. Seja $X = \{x_i\}_{i \in I}$ uma base de L. Calculamos $y_i = g(x_i) \in N, \forall i \in I$. Como f é um epimorfismo, existem elementos $m_i \in M$ tais que $f(m_i) = y_i, \forall i \in I$. Definindo g_1 sobre a base por $g_1(x_i) = m_i \forall i \in I$, pela Proposição 1.35, g_1 pode ser estendida a um único R-homomorfismo $\overline{g} : M \to N$ tal que $\overline{g}$ restringido a X coincida com g_1. Daí, segue imediatamente que $f \circ \overline{g} = g$. ∎

A propriedade da Proposição 1.37 é característica de uma classe mais ampla de módulos, que estudaremos agora.

Definição 1.38 *Um R-módulo P diz-se projetivo se, dados R-módulos M e N, um epimorfismo $f : M \to N$ e um homomorfismo $g : P \to N$, sempre existe um homomorfismo $\overline{g} : P \to M$ tal que $f \circ \overline{g} = g$.*

Em outras palavras, P é projetivo se para todo diagrama como o dado abaixo contínuos, existe um homomorfismo $\overline{g}$ que faz com que o diagrama completo seja comutativo:



A seguinte proposição dá uma caracterização dos módulos projetivos.

Proposição 1.39 *Seja P um R-módulo. As seguintes afirmações são equivalentes:*

(i) P *é projetivo;*

(ii) Qualquer sequência exata curta $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ *cinde.*

(iii) P *é somando direto de um* R*-módulo livre.*

Demonstração.

$(i) \Rightarrow (ii)$ Suponha que P é um R-módulo projetivo. Seja $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ uma sequência exata e considere o diagrama

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle I_P} & & \\ N & \xrightarrow{g} & P & \longrightarrow & 0 \end{array}$$

Como P é projetivo, existe $g' : P \to N$ tal que o diagrama é comutativo

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{g'} & \downarrow{\scriptstyle I_P} & & \\ N & \xrightarrow{g} & P & \longrightarrow & 0 \end{array}$$

ou seja, $g \circ g' = I_P$. Como existe $g' : P \to N$ tal que $g' \circ g = I_N$, pela Proposição 1.27, a sequência $0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$ cinde.

$(ii) \Rightarrow (iii)$ Como todo R-módulo é a imagem homeomórfica de um R-módulo livre (Proposição 1.36), então existe um R-módulo livre L e uma projeção $\pi : L \to M$, assim temos a sequência exata

$$0 \longrightarrow P' \xrightarrow{i} L \xrightarrow{\pi} P \longrightarrow 0.$$

Como P satisfaz (ii), então a sequência acima cinde e $L \simeq P \oplus P'$.

$(iii) \Rightarrow (i)$ Seja L um R-módulo livre tal que $L = P \oplus S$. Dados R-módulos M e N, um epimorfismo $f : M \to N$ e um homomorfismo $g : P \to N$, podemos estender g a um homomorfismo $g' : L \to N$ definido por

$$g'(x) = \begin{cases} g(x), & \text{se} \quad x \in P, \\ 0, & \text{se} \quad x \in S. \end{cases}$$

Dado $x \in L$, escreva $x = x_1 + x_2$ de maneira única com $x_1 \in P, x_2 \in S$ e $g(x) = g(x_1)$. Como L é livre, pela Proposição 1.37, existe um homomorfismo $\overline{g}' : L \to M$ tal que $f \circ \overline{g}' = g'$, conforme o digrama.

$$\begin{array}{ccccc} & & L & \xleftarrow{i} & P \\ & \swarrow^{\overline{g}'} & \downarrow{\scriptstyle g'} & \swarrow_{g} & \\ M & \xrightarrow{f} & N & \longrightarrow & 0 \end{array}$$

Considerando a inclusão $i : P \to L$, temos que $\overline{g} = \overline{g}' \circ i : P \to M$ e

$$f \circ \overline{g} = f \circ \overline{g}' \circ i = g' \circ i = g.$$

Portanto, P é projetivo. ∎

Observação 1.40 *Todo módulo livre é projetivo.*

Proposição 1.41 *Seja $\{P_i\}_{i\in I}$ uma família de R-módulos. A soma direta $\oplus_{i\in I} P_i$ é projetivo, se e somente se, cada P_i o é.*

Demonstração. [17, Proposição 3.5]. ∎

Teorema 1.42 (Lema da Base Dual) *Seja P um R-módulo à esquerda. Então, P é projetivo se, e somente se, existem conjuntos $\{x_i\}_{i\in I} \subset P$ e $\{f_i\}_{i\in I} \subset Hom_R(P, R)$ (I conjunto de índices) tais que*

(i) para qualquer $x \in P$, $f_i(x) = 0$ a menos de um número finito de I; e

(ii) para qualquer $x \in P$, $\sum_i f_i(x)x_i = x$.

Além disso, I é um conjunto finito se, e somente se, P é finitamente gerado. A coleção $\{f_i, x_i\}_{i\in I}$ é chamada base dual de P.

Demonstração. Suponha que P é projetivo, então existe um conjunto I tal que P é isomorfo como R-módulo à esquerda a um somando direto do módulo livre $R^{(I)}$, pela Proposição 1.39. Equivalentemente, existe uma aplicação R-linear $\varphi : P \to R^{(I)}$ e $\pi : R^{(I)} \to P$ tal que $\pi \circ \varphi = I_P$. Podemos considerar $R^{(I)}$ como um conjunto de funções de I em R.

Seja $\pi_i : R^{(I)} \to R$ dada por $\pi_i(f) = f(i)$, para todo $f \in R^{(I)}$. Seja $b_i \in R^{(I)}$ a função dada por $b_i(j) = \delta_{i,j}$. Então, $\{\pi_i, b_i\}$ é uma base dual para $R^{(I)}$. De fato, para todo $f \in R^{(I)}$, temos

$$\left(\sum_{i\in I} \pi_i(f)b_i\right)(j) = \sum_{i\in I} \pi_i(f)(b_i(j)) = \pi_j(f)(j) = f(j),$$

para todo $j \in I$. Logo, para todo $f \in R^{(I)}$ temos

$$\sum_{i\in I} \pi_i(f)b_i = f.$$

Considere $m_i = \pi(b_i)$ e $f_i = \pi_i f$. Claramente, $f_i(m) = 0$ exceto para um número finito de índices $i \in I$ e para todo $m \in P$

$$\begin{aligned}\sum_{i\in I} f_i(m)m_i &= \sum_{i\in I} \pi_i(\varphi(m))\pi_i(b_i) \\ &= \pi\left(\sum_{i\in I} \pi_i(\varphi(m))b_i\right) \\ &= \pi(\varphi(m)) = m.\end{aligned}$$

Logo, $\{f_i, m_i\}$ é uma base dual para P.

Reciprocamente, se $\{f_i, m_i\}$ é uma base dual de P, defina $\varphi : P \to R^{(I)}$ por $\varphi(m)(i) = f_i(m)$ e $\pi : R^{(I)} \to P$ por $\pi(f) = \sum_{i\in I} f(i)m_i$. É imediato verificar que φ e π são homomorfismos de R-módulos e que

$$\pi(\varphi(m)) = \sum_{i\in I} f_i(m)m_i = m.$$

Assim, $\pi \circ \varphi = I_P$. Logo, P é isomorfo a um somando direto de $R^{(I)}$ e portanto é projetivo.

■

Suponha que R e S são anéis (possivelmente não comutativos) e $\theta : R \to S$ um homomorfismo de anéis. Então S tem uma estrutura de R-módulo via

$$r \cdot s = \theta(r)s.$$

Isso induz naturalmente uma estrutura de R-módulo em qualquer S-módulo M por:

$$r \cdot m = \theta(r)m,$$

para todo $r \in R$ e $m \in M$.

Agora, vejamos algumas aplicações do Lema da Base Dual.

Proposição 1.43 (Transitividade dos módulos projetivos) *Sejam R e S anéis e $\theta : R \to S$ um homomorfismo de anéis tal que S é projetivo como um R-módulo. Então, qualquer S-módulo projetivo P é projetivo como um R-módulo. Além disso, se P é finitamente gerado sobre S e S é finitamente gerado sobre R, então P é finitamente gerado sobre R.*

Demonstração. Como P é um S-módulo projetivo, pelo Lema da Base Dual (Teorema 1.42), exitem $\{x_i\} \subset P$ e $\{f_i\} \subset Hom_S(P, S)$, $i \in I$ com $f_i(x) = 0$ para quase todo $i \in I$ e $\sum_i f_i(x)x_i = x$, para todo $x \in P$. Analogamente, já que S é projetivo como um

R-módulo, existem $\{s_j\} \subset S$ e $\{g_j\} \subset Hom_R(S,R)$, $j \in J$ com $g_j(s) = 0$ para quase todo $j \in J$ e $\sum_j g_j(s)s_j = s$, para todo $s \in S$. Temos que $g_j f_i \in Hom_R(P,R)$ e $s_j x_i \in P$ (P é um S-módulo), com $g_j f_i(x) = 0$ para quase todo $(i,j) \in I \times J$. Observe que:

$$\sum_{i,j} g_j f_i(x) s_j x_i = \sum_i \left(\sum_j g_j f_i(x) s_j \right) x_i = \sum_i f_i(x) x_i = x, \forall x \in P.$$

Assim, $\{g_j f_i, s_j m_i\}$ é base dual de P, o que mostra que P é um R-módulo projetivo. A última afirmação é imediata, pois agora temos um conjunto finito de índices. ■

Proposição 1.44 *Sejam $R \subset S$ uma extensão de anéis comutativos e A_1, A_2 S-módulos projetivos e finitamente gerados. Então $A_1 \otimes_R A_2$ é um $S \otimes_R S$ módulo projetivo e finitamente gerado, onde a ação é dada por*

$$(s_1 \otimes s_2) \cdot (a_1 \otimes s_2) = s_1 a_1 \otimes s_2 a_2.$$

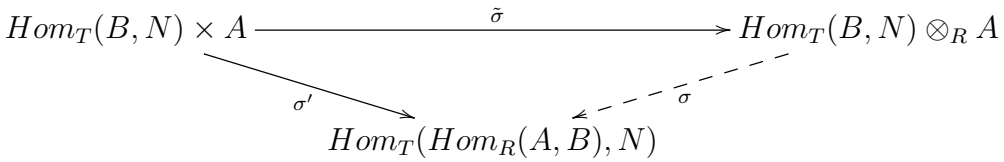
Demonstração. Suponha que A_1 é um S-módulo projetivo e finitamente gerado. Pelo Lema da Base Dual, existem $\{a_i\} \subset A_1$ e $\{f_i\} \subset Hom_S(A_1, S)$, $i = 1, \ldots, n$, tais que $\sum_{i=1}^n f_i(a)a_i = a$, para todo $a \in A_1$. Analogamente, sendo A_2 um S-módulo projetivo e finitamente gerado, existem $\{b_j\} \subset A_2$ e $\{g_j\} \subset Hom_S(A_2, S)$, $j = 1, \ldots, m$, tais que $\sum_{j=1}^m g_j(b)b_j = b$, para todo $b \in A_2$. Considere $f_i \otimes_R g_j \in Hom_{S \otimes_R S}(A_1 \otimes_R A_2, S \otimes_R S)$ e $a_i \otimes b_j \in A_1 \otimes_R A_2$, $i = 1, \ldots, n$ e $j = 1, \ldots, m$. Para todo $a \otimes b \in A_1 \otimes_R A_2$, temos:

$$\begin{aligned}
\sum_{i=1}^n \sum_{j=1}^m (f_i \otimes g_j)(a \otimes b) \cdot (a_i \otimes b_j) &= \sum_{i=1}^n \sum_{j=1}^m (f_i(a) \otimes g_j(b)) \cdot (a_i \otimes b_j) \\
&= \sum_{i=1}^n \sum_{j=1}^m f_i(a)a_i \otimes g_j(b)b_j \\
&= \sum_{i=1}^n f_i(a)a_i \otimes \sum_{j=1}^m g_j(b)b_j \\
&= a \otimes b.
\end{aligned}$$

Portanto, $\{f_i \otimes g_j, a_i \otimes b_j\}$ é base dual de $A_1 \otimes A_2$ e temos o resultado desejado.

■

Sejam R e T anéis. Dados ${}_RA, {}_RB_T$ e N_T módulos, existe um homomorfismo $\sigma : Hom_T(B,N) \otimes_R A \to Hom_T(Hom_R(A,B), N)$ definido por $[\sigma(f \otimes a)](g) = f(g(a))$ para $f \in Hom_T(B,N), g \in Hom_R(A,B), a \in A$. De fato, considere o diagrama abaixo:



Para verificar que σ está bem definida, basta mostrar que σ' é R-balanceada e, em seguida, utilizar a Propriedade Universal do produto tensorial. Observe que $Hom_R(B,N)$ tem uma estrutura de T-módulo à direita dada por:

$$(f \cdot t)(b) = f(t \cdot b)$$

para $f \in Hom_R(B,N), t \in T, b \in B$. Isto ocorre devido ao fato de B ser um T-módulo à direita.

Proposição 1.45 *Nas condições acima, se A é um R-módulo projetivo e finitamente gerado, então σ é um isomorfismo.*

Demonstração. [6, Proposição 5.2]. ∎

Para qualquer R-módulo M, vamos considerar o conjunto

$$\mathcal{T}_R(M) = \left\{ \sum_i f_i(m_i), f_i \in Hom_R(M,R), m_i \in M \right\}.$$

Como $Hom_R(M,R)$ é um R-módulo à direita via

$$(f \cdot r)(m) = f(m)r,$$

para todo $m \in M$, então

$$r\left(\sum_i f_i(m_i)\right) = \sum_i f_i(rm_i) \Rightarrow r\left(\sum_i f_i(m_i)\right) \in \mathcal{T}_R(M) \tag{1.1}$$

e

$$\left(\sum_i f_i(m_i)\right)r = \sum_i (f_i \cdot r)(m_i) \Rightarrow \left(\sum_i f_i(m_i)\right)r \in \mathcal{T}_R(M). \tag{1.2}$$

De (1.1) e (1.2), seque que $\mathcal{T}_R(M)$ é um ideal de R, chamado de *ideal traço* de M.

Definição 1.46 *Dizemos que um R-módulo M é um gerador se $\mathcal{T}_R(M) = R$.*

Observação 1.47 *M é um R-gerador se, e somente se, existem $\{f_i\} \subset Hom_R(M,R)$ e $\{m_i\} \subset M$, com $i \in I$, tais que $\sum_i f_i(m_i) = 1$.*

Proposição 1.48 (Transitividade dos módulos geradores) *Sejam R e S anéis e $\theta : R \to S$ um homomorfismo de anéis tal que S é um R-módulo gerador. Então, qualquer S-módulo gerador M é um R-módulo gerador.*

Demonstração. Como M é um S-módulo gerador, pela Observação 1.47, existem $\{f_i\} \subset Hom_S(M,S)$ e $\{m_i\} \subset M$ tais que $\sum_i f_i(m_i) = 1$. Analogamente, já que S é um R-módulo gerador, existem $\{g_j\} \subset Hom_R(S,R)$ e $\{s_j\} \subset S$ tais que $\sum_j g_j(s_j) = 1$. Então, $g_j f_i \in Hom_R(M,R)$ e $s_j m_i \in M$ com

$$\sum_{i,j} g_j f_i(s_j m_i) = \sum_{i,j} g_j(s_j \cdot f_i(m_i)) = \sum_j g_j(s_j \cdot \sum_i f_i(m_i) = \sum_j g_j(s_j) = 1.$$

Portanto, M é um R-gerador. ∎

Podemos definir agora a noção de módulo progerador.

Definição 1.49 *Um R-módulo M é um R-progerador se M é finitamente gerado, projetivo e um gerador sobre R.*

Das Proposições 1.43 e 1.48, podemos concluir o seguinte:

Proposição 1.50 (Transitividade dos módulos progeradores) *Sejam R e S anéis e $\theta : R \to S$ um homomorfismo de anéis tal que S é um R-módulo progerador. Então, qualquer S-módulo progerador M é um R-módulo progerador.*

Proposição 1.51 *Seja R um anel comutativo e M um R-módulo projetivo e finitamente gerado. Então, $\mathcal{T}_R(M) \oplus Anl_R(M) = R$, onde $Anl_R(M)$ é o anulador de M em R.*

Demonstração. [9, Corolário 1.8]. ∎

Corolário 1.52 *Se R é um anel comutativo, um R-módulo M é um progerador, se e somente se, M é projetivo, finitamente gerado e fiel.*

Demonstração. Suponha que M é um R-progerador. Então, M é finitamente gerado, projetivo e um gerador sobre R. Pela Proposição 1.51, temos que $\mathcal{T}_R(M) \oplus Anl_R(M) = R$. Além disso, $\mathcal{T}_R(M) = R$, pois M é um R-gerador. Assim, $R \oplus Anl_R(M) = R$, o que implica em $Anl_R(M) = (0)$. Logo, M é um R-módulo fiel.

Reciprocamente, suponha que M é projetivo, finitamente gerado e fiel. Para mostrar que M é um progerador, resta mostrar que M é um gerador sobre R. Aplicando a Proposição 1.51, temos que $\mathcal{T}_R(M) \oplus Anl_R(M) = R$. Como M é fiel, segue que $\mathcal{T}_R(M) = R$, mostrando que M é um R-gerador. ∎

Capítulo 2

Álgebras Separáveis

Neste capítulo, trataremos das álgebras separáveis. Inicialmente, trazemos a descrição das álgebras separáveis com base em [9]. Como um caso das álgebras separáveis, temos as álgebras centrais separáveis ou também como são chamadas de álgebras de Azumaya, devido as fortes contribuições do matemático japonês Goro Azumaya em 1951 para este tipo de álgebra. O Teorema 2.22 caracteriza as álgebras de Azumaya por meio dos módulos progeradores e do homomorfismo de R-álgebras $\varphi : A^e \to Hom_R(A, A)$. Mostramos que uma R-álgebra A é separável se, e somente se, A é separável sobre seu centro e seu centro é uma R-álgebra separável (Teorema 2.26). Por fim, abordaremos a noção de H-separabilidade, que foi introduzida na literatura por Hirata [16]. O Teorema 2.41 mostra que extensões de anéis H-separáveis são separáveis. Além disso, podemos relacionar a H-separabilidade com as álgebras de Azumaya. Trazemos alguns resultados a respeito disso por meio de [18], [24], entre outros.

2.1 Definições, exemplos e propriedades

Suponha que R é um anel comutativo. Uma R-álgebra A é um anel com um homomorfismo de anéis $\theta : R \to C(A)$. Isso induz uma estrutura de R-módulo em A definida por

$$r \cdot a = \theta(r)a,$$

para todo $r \in R$ e $a \in A$. Observe que

$$r \cdot (ab) = (r \cdot a)b = a(r \cdot b), \tag{2.1}$$

para todo $r \in R$ e $a, b \in A$. De fato,

$$r \cdot (ab) = \theta(r)(ab) = (\theta(r)a)b = (r \cdot a)b.$$

Além disso, como $\theta(r) \in C(A)$, temos

$$r \cdot (ab) = \theta(r)(ab) = (\theta(r)a)b = (a\theta(r))b = a(\theta(r)b) = a(r \cdot b).$$

Reciprocamente, se A é um anel que também é um R-módulo que satisfaz a condição (2.1), então $\theta : R \to C(A)$, definida por $\theta(r) = r \cdot 1$, é um homomorfismo de anéis e portanto A é uma R-álgebra. De fato, inicialmente vejamos que θ está bem-definida, ou seja, $\theta(r) \in C(A)$. Dado $a \in A$, temos

$$\theta(r)a = (r \cdot 1)a = r \cdot (1a) = r \cdot (a1) = a(r \cdot 1) = a\theta(r).$$

Logo, $\theta(r) \in C(A)$. Além disso, para $r, r' \in R$, temos

$$\theta(r)\theta(r') = (r \cdot 1)(r' \cdot 1) = r \cdot (1(r' \cdot 1)) = r \cdot (r' \cdot 1) = (rr') \cdot 1 = \theta(rr').$$

Vamos denotar por $R \cdot 1$ a imagem de R por θ e vamos usar as duas definições de álgebra intercaladamente. Em particular, uma R-álgebra A é fiel se, e somente se, θ é injetor.

Exemplo 2.1 *Todo anel R é uma R-álgebra, ou seja, todo anel é uma álgebra sobre si mesmo.*

Definição 2.2 *Sejam A e B álgebras sobre um anel R. Dizemos que um homomorfismo de módulos $f : A \to B$ é um homomorfismo de álgebras se $f(aa') = f(a)f(a')$, para quaisquer $a, a' \in A$.*

Agora, vamos definir a ideia de centralizador e centro que utilizaremos em todo o trabalho. Para qualquer subconjunto não vazio X de um anel A e qualquer subanel B de A, denotaremos por

$$C_B(X) = \{b \in B \mid bx = xb, \text{ para todo } x \in X\},$$

o centralizador de X em B. Se $X = B$, obtemos o centro de B, e vamos denotar por simplicidade por

$$C(B) = \{b \in B \mid bx = xb, \text{ para todo } x \in B\}.$$

Sejam R um anel comutativo e A uma R-álgebra. A álgebra $A^e = A \otimes A^o$ é chamada de *álgebra envolvente de* A, onde A^o é o anel oposto de A, sendo $A^o = A$ como grupo aditivo e a multiplicação $*$ definida por $a * b = ba$, onde ba denota o produto de b com a no anel A. Para simplificar a notação, supriremos a notação $*$, já que o contexto deixará claro se estamos operando em A ou A^o.

A álgebra A tem uma estrutura de A^e-módulo à esquerda induzida por

$$(a \otimes b) \cdot x = axb,$$

para $a, x \in A$ e $b \in A^o$. Considere a aplicação $\mu : A^e \to A$ definida por

$$\mu\Big(\sum_{i=1}^{n} a_i \otimes b_i\Big) = \sum_{i=1}^{n} a_i b_i.$$

É fácil verificar que μ é um homomorfismo de A^e-módulos e que se A é comutativa, então μ é um homomorfismo sobrejetor de anéis. Denotando por J o núcleo de μ, temos a sequência exata

$$0 \longrightarrow J \xrightarrow{i} A^e \xrightarrow{\mu} A \longrightarrow 0 \tag{2.2}$$

de A^e-módulos à esquerda, onde i denota o homomorfismo inclusão.

Observação 2.3 *J é o ideal à esquerda gerado por $\{a \otimes 1 - 1 \otimes a, a \in A\}$. De fato, seja I o ideal á esquerda de A^e gerado por $\{a \otimes 1 - 1 \otimes a, a \in A\}$. Para todo $a \in A$, temos que*

$$\mu(a \otimes 1 - 1 \otimes a) = \mu(a \otimes 1) - \mu(1 \otimes a) = a \cdot 1 - 1 \cdot a = a - a = 0.$$

Logo, $a \otimes 1 - 1 \otimes a \in J$ para todo $a \in A$ e assim $I \subset J$. Por outro lado, seja $\sum_{i=1}^{n} a_i \otimes b_i \in J$, então $\sum_{i=1}^{n} a_i b_i = 0$ e assim

$$\begin{aligned}\sum_{i=1}^{n}(a_i \otimes 1)\underbrace{(b_i \otimes 1 - 1 \otimes b_i)}_{\in I} &= \sum_{i=1}^{n}(a_i b_i \otimes 1 - a_i \otimes b_i) \\ &= \Big(\sum_{i=1}^{n} a_i b_i\Big) \otimes 1 - \sum_{i=1}^{n} a_i \otimes b_i \\ &= -\sum_{i=1}^{n} a_i \otimes b_i.\end{aligned}$$

Logo,

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

Portanto, $J = I$.

Proposição 2.4 *Seja A uma R-álgebra. São equivalentes:*

(i) *A é um A^e-módulo projetivo;*

(ii) $0 \longrightarrow J \xrightarrow{i} A^e \xrightarrow{\mu} A \longrightarrow 0$ *cinde como uma sequência exata de A^e-módulos à esquerda;*

(iii) *Existe um elemento $e \in A^e$ tal que $\mu(e) = 1$ e $Je = 0$.*

Demonstração.

$(i) \Leftrightarrow (ii)$ Segue diretamente da Proposição 1.39.

$(ii) \Leftrightarrow (iii)$ Vamos assumir que a sequência (2.2) cinde. Então pela Proposição 1.27 existe um A^e-homomorfismo $\varphi : A \to A^e$ tal que $\mu\varphi = I_A$. Seja $e = \varphi(1) \in A^e$, então $\mu(e) = \mu(\varphi(1)) = 1$. Além disso, para todo $a \in A$, temos

$$\begin{aligned}(a \otimes 1)e = (a \otimes 1)\varphi(1) &= \varphi((a \otimes 1) \cdot 1) \\ &= \varphi(a) = \varphi((1 \otimes a) \cdot 1) \\ &= (1 \otimes a)\varphi(1) = (1 \otimes a)e.\end{aligned}$$

Ou seja, $(a \otimes 1 - 1 \otimes a)e = 0$. Segue então da Observação 2.3 que $Je = 0$.

Reciprocamente, suponha que existe $e \in A^e$ tal que $\mu(e) = 1$ e $Je = 0$. Considere a aplicação $\varphi : A \to A^e$ definida por

$$\varphi(a) = (a \otimes 1)e = (1 \otimes a)e.$$

Observe que φ é um A^e-homomorfismo, pois

$$\begin{aligned}\varphi((a \otimes b) \cdot c) = \varphi(acb) &= (acb \otimes 1)e \\ &= (ac \otimes 1)(b \otimes 1)e = (ac \otimes 1)(1 \otimes b)e \\ &= (ac \otimes b)e = (a \otimes b)(c \otimes 1)e \\ &= (a \otimes b)\varphi(c),\end{aligned}$$

para todo $a \otimes b \in A^e$ e $c \in A$. Além disso, para todo $a \in A$, temos

$$\mu\varphi(a) = \mu((a \otimes 1)e) = (a \otimes 1)\mu(e) = (a \otimes 1) \cdot 1 = a.$$

Logo, a sequência $0 \longrightarrow J \xrightarrow{i} A^e \xrightarrow{\mu} A \longrightarrow 0$ cinde. ∎

Definição 2.5 *Dizemos que uma R-álgebra A é separável se satisfaz uma e, portanto, todas as condições da Proposição 2.4.*

Observe que o elemento e da condição (iii) da Proposição 2.4 é necessariamente um idempotente, pois

$$e^2 - e = (e - 1 \otimes 1)e \in Je = 0.$$

Este elemento é chamado de idempotente de separabilidade de A. Veja que um idempotente de separabilidade para uma álgebra não reside na própria álgebra, mas em sua álgebra envolvente.

Observação 2.6 *A condição (iii) da Proposição 2.4 é equivalente a dizer que existe $\sum_i a_i \otimes b_i \in C_{A\otimes A}(A)$ tal que $\sum_i a_i b_i = 1$, para todo $a \in A$. De fato, suponha que existe um elemento $e = \sum_i a_i \otimes b_i \in A^e$ tal que $\mu(e) = 1$ e $Je = 0$. Inicialmente, como $A \otimes A^o = A \otimes A$, como conjunto, então $e \in A \otimes A$. Agora, dado $a \in A$, temos que $a \otimes 1 - 1 \otimes a \in J$ e assim*

$$(a \otimes 1 - 1 \otimes a)e = (a \otimes 1 - 1 \otimes a) \sum_i a_i \otimes b_i = \sum_i aa_i \otimes b_i - \sum_i a_i \otimes b_i a.$$

Como $Je = 0$, segue que $\sum_i aa_i \otimes b_i - \sum_i a_i \otimes b_i a = 0$ e daí $\sum_i aa_i \otimes b_i = \sum_i a_i \otimes b_i a$, para todo $a \in A$, ou seja, $\sum_i a_i \otimes b_i \in C_{A\otimes A}(A)$. A recíproca é imediata. Sendo assim, vamos utilizar essas condições sem distinção.

Observação 2.7 *Sejam A um anel e B um subanel de A. Dizemos que é separável sobre B, ou uma extensão separável, se a sequência exata*

$$A \otimes_B A \xrightarrow{\mu} A \longrightarrow 0$$

cinde, onde $\mu(a \otimes a') = aa'$, para $a, a' \in A$. De fato, temos que isso ocorre pela Proposição 2.4 (ii).

A seguir, trazemos alguns exemplos de álgebras separáveis.

Exemplo 2.8 *O anel R é uma R-álgebra separável. De fato, tomando $e = 1 \otimes 1 \in R \otimes R^o$, temos que $\mu(e) = 1$ e $Je = 0$, ou seja, e é um idempotente de separabilidade de R sobre R.*

Exemplo 2.9 *Seja $M_n(R)$ o anel das matrizes $n \times n$ com entradas em R. Denote por e_{ij} a matriz que tem 1 na entrada (i, j) e 0 nas demais entradas. Fixado j entre 1 e n, considere $e = \sum_{i=1}^{n} e_{ij} \otimes e_{ji}$, então*

$$\mu(e) = \sum_{i=1}^{n} e_{ij}e_{ji} = \sum_{i=1}^{n} e_{ii} = I_n.$$

Para $1 \leq k, l \leq n$, *temos*

$$\begin{aligned}(e_{kl} \otimes 1 - 1 \otimes e_{kl})e &= \sum_{i=1}^{n}(e_{kl}e_{ij} \otimes e_{ji} - e_{ij} \otimes e_{ji}e_{kl}) \\ &= e_{kj} \otimes e_{jl} - e_{kj} \otimes e_{jl} = 0.\end{aligned}$$

Como e_{kl} *gera* $M_n(R)$ *como um* R*-módulo, segue então que* $Je = 0$. *Logo,* $e = \sum_{i=1}^{n} e_{ij} \otimes e_{ji}$ *é um idempotente de separabilidade de* $M_n(R)$ *sobre* R. *Portanto,* $M_n(R)$ *é separável sobre* R.

Exemplo 2.10 *Seja* G *um grupo finito cuja a ordem* n *é uma unidade de* R. *Então a álgebra de grupo* $R(G)$ *é separável sobre* R. *De fato, considere* $e = \frac{1}{n}\sum_{\sigma \in G} \sigma \otimes \sigma^{-1} \in R(G)^e$. *Temos que* e *é um idempotente de separabilidade de* $R(G)$ *sobre* R *e, portanto,* $R(G)$ *é uma* R*-álgebra separável.*

Como vimos no Exemplo 2.9, o idempotente de separabilidade e nem sempre é único. Porém, se A é uma álgebra comutativa, então e é único. De fato, sejam e_1 e $e_2 \in A^e$ tais que $\mu(e_1) = \mu(e_2) = 1$ e $Je_1 = Je_2 = 0$. Observe que

$$\mu(e_1 - e_2) = \mu(e_1) - \mu(e_2) = 1 - 1 = 0,$$

ou seja, $e_1 - e_2 \in J$. Assim,

$$(e_1 - e_2)e_1 = e_1^2 - e_2e_1 = e_1 - e_2e_1 \in Je_1 = 0.$$

O que implica que $e_1 - e_2e_1 = 0$. Da mesma forma,

$$(e_2 - e_1)e_2 = e_2^2 - e_1e_2 = e_2 - e_1e_2 \in Je_2 = 0,$$

e assim, $e_2 - e_1e_2 = 0$. Segue então da igualdade que $e_1 - e_2e_1 = e_2 - e_1e_2$. Como A é comutativa, devemos ter $e_1 = e_2$.

Seja A uma R-álgebra e M um A-módulo à esquerda, então M herda uma estrutura de R-módulo à esquerda definida por

$$r \cdot m = (r \cdot 1) \cdot m, \forall r \in R \text{ e } m \in M.$$

Da mesma forma, se M é um A-módulo à direita, então M herda uma estrutura de R-módulo à direita definida por

$$m \cdot r = m \cdot (r \cdot 1), \forall r \in R \text{ e } m \in M.$$

Um A/R-*módulo bilateral* M é um A-A-bimódulo que é central como R-módulo. Mais explicitamente, um A/R-módulo bilateral M é um A-módulo à esquerda que também é um A-módulo à direita satisfazendo que

(i) $(a \cdot m) \cdot a' = a \cdot (m \cdot a'), \quad$ para todo $m \in M, a, a' \in A$;

(ii) $(r \cdot 1) \cdot m = m \cdot (r \cdot 1), \quad$ para todo $m \in M, r \in R$.

Observação 2.11 *Os conceitos de A/R-módulo bilateral e A^e-módulo são equivalentes. De fato, seja M um A^e-módulo à esquerda, então M pode ser considerado como um A/R-módulo bilateral definindo*

$$a \cdot m = (a \otimes 1)m \quad e \quad m \cdot a = (1 \otimes a)m,$$

para $a \in A$ e $m \in M$. Inicialmente, vejamos que M é um A-módulo à esquerda. Como as outras condições são de fácil verificação, mostraremos apenas que $(aa') \cdot m = a \cdot (a' \cdot m)$, para quaisquer $a, a' \in A$ e $m \in M$. Como M é um A^e-módulo à esquerda, temos:

$$\begin{aligned}(aa') \cdot m &= (aa' \otimes 1)m = ((a \otimes 1)(a' \otimes 1))m \\ &= (a \otimes 1)((a' \otimes 1)m) = a \cdot ((a' \otimes 1)m) \\ &= a \cdot (a' \cdot m).\end{aligned}$$

Assim, M é um A-módulo à esquerda. Analogamente mostra-se que M é um A-módulo à direita. Para $a, a' \in A$ e $m \in M$, temos

$$\begin{aligned}(a \cdot m) \cdot a' &= (a \otimes 1)m \cdot a' = (1 \otimes a')(a \otimes 1)m \\ &= (a \otimes a')m = (a \otimes 1)(1 \otimes a')m \\ &= a \cdot [(1 \otimes a')m] = a \cdot (m \cdot a'),\end{aligned}$$

o que mostra que M é um A-bimódulo. Agora, note que para $r \in R$,

$$m \cdot (r \cdot 1) = (1 \otimes r \cdot 1)m = (1 \cdot r \otimes 1)m = (r \cdot 1) \cdot m.$$

Então, M é um A/R-módulo bilateral.

Reciprocamente, qualquer A/R-módulo bilateral M pode ser considerado como um A^e-módulo via

$$(a \otimes a') \cdot m = ama', \text{ para} \, m \in M, a, a' \in A.$$

Da observação acima, temos que, em particular, A é um A-bimódulo se, e somente se, A é um A^e-módulo.

Para todo A/R-módulo bilateral M, vamos denotar por M^A o R-submódulo

$$M^A = \{m \in M \mid a \cdot m = m \cdot a, \text{ para todo} \, a \in A\}.$$

Em particular, $A^A = \{a \in A \mid ax = xa, \text{ para todo} \, x \in A\} = C(A)$ que é o centro da álgebra A.

Lema 2.12 *Para qualquer A/R-módulo bilateral M, $Hom_{A^e}(A,M) \simeq M^A$ como R-módulos sobre a correspondência $f \mapsto f(1)$, para todo $f \in Hom_{A^e}(A,M)$. Para qualquer outro A/R-módulo bilateral N e qualquer $g \in Hom_{A^e}(M,N)$, o diagrama*

$$\begin{array}{ccc} Hom_{A^e}(A,M) & \xrightarrow{Hom_{A^e}(A,g)} & Hom_{A^e}(A,N) \\ \downarrow & & \downarrow \\ M^A & \xrightarrow[g|]{} & N^A \end{array}$$

comuta.

Demonstração. Primeiramente, observe que se $f \in Hom_{A^e}(A,M)$, então

$$\begin{aligned} a \cdot f(1) &= (a \otimes 1)f(1) = f((a \otimes 1) \cdot 1) = f(a) \\ &= f((1 \otimes a) \cdot 1) = (1 \otimes a)f(1) \\ &= f(1) \cdot a. \end{aligned}$$

Assim, $f(1) \in M^A$ e portanto a aplicação

$$\begin{array}{rccc} \varphi: & Hom_{A^e}(A,M) & \to & M^A \\ & f & \mapsto & f(1) \end{array}$$

está bem-definida.

Seja $m \in M^A$, considere a função definida por $f(a) = a \cdot m$. Então, $f \in Hom_{A^e}(A,M)$, pois para $a, a', b \in A$, temos

$$\begin{aligned} f((a \otimes b) \cdot a') &= f(aa'b) = (aa'b)m = aa'(bm) \\ &= aa'(mb) = a(a'm)b = (a \otimes b) \cdot f(a'). \end{aligned}$$

Além disso, temos que

$$\varphi(f) = f(1) = 1 \cdot m = m.$$

Logo, φ é sobrejetora. Vejamos que φ é injetora. Sejam $f, g \in Hom_{A^e}(A,M)$ tais que $f(1) = g(1)$. Para todo $a \in A$, temos

$$f(a) = f((1 \otimes a) \cdot 1) = (1 \otimes a)f(1) = (1 \otimes a)g(1) = g((1 \otimes a) \cdot 1) = g(a).$$

Assim, $f = g$. Portanto, φ é um isomorfismo.

Sejam $\varphi : Hom_{A^e}(A,M) \to M^A$ e $\varphi' : Hom_{A^e}(A,N) \to N^A$ os isomorfismos dados acima. Então, para cada $f \in Hom_{A^e}(A,M)$, temos

$$\varphi'(g \circ f) = g \circ f(1) = g(f(1))$$

e por outro lado

$$g(\varphi(f)) = g(f(1)).$$

Logo, o diagrama é comutativo. ∎

Corolário 2.13 *$Hom_{A^e}(A, A) \simeq C(A)$.*

Demonstração. Fazendo $A = M$ no Lema 2.12, temos $Hom_{A^e}(A, A) \simeq A^A = C(A)$. ∎

Corolário 2.14 *Seja $Anl_{A^e}(J)$ o anulador à direita de J em A^e. Então, $Hom_{A^e}(A, A^e) \simeq Anl_{A^e}(J)$. Além disso, se A é R-separável, então $\mu(Anl_{A^e}(J)) = C(A)$.*

Demonstração. Pelo Lema 2.12, temos

$$\begin{aligned} Hom_{A^e}(A, A^e) \simeq (A^e)^A &= \{x \in A^e \mid a \cdot x = x \cdot a, \forall a \in A\} \\ &= \{x \in A^e \mid (a \otimes 1)x = (1 \otimes a)x, \forall a \in A\} \\ &= \{x \in A^e \mid (a \otimes 1 - 1 \otimes a)x = 0, \forall a \in A\} \\ &= Anl_{A^e}(J). \end{aligned}$$

Agora, se A é R-separável, então A é um A^e-módulo projetivo. Assim, pela Proposição A.3, o funtor $Hom_{A^e}(A, \quad)$ é exato e daí a sequência

$$Hom_{A^e}(A, A^e) \overset{Hom_{A^e}(A,\mu)}{\longrightarrow} Hom_{A^e}(A, A) \longrightarrow 0$$

é exata. Então,

$$\mu(Hom_{A^e}(A, A^e)) = Hom_{A^e}(A, A).$$

Como $Hom_{A^e}(A, A^e) \simeq Anl_{A^e}(J)$ e $Hom_{A^e}(A, A) \simeq C(A)$, pelo Corolário 2.13, então a igualdade acima é equivalente a $\mu(Anl_{A^e}(J)) = C(A)$. ∎

Proposição 2.15 (Transitividade da Separabilidade) *Sejam S uma R-álgebra separável e comutativa e A uma S-álgebra separável. Então, A é uma R-álgebra-separável.*

Demonstração. Sejam $e_1 = \sum_{i=1}^{n} a_i \otimes b_i \in A \otimes_S A$ e $e_2 = \sum_{j=1}^{m} \alpha_j \otimes \beta_j \in S \otimes_R S$ os idempotentes de separabilidade de A sobre S e de S sobre R, respectivamente, que existem pela Proposição 2.4. Então, a aplicação

$$\begin{array}{rccc} \psi: & A \otimes_S A & \to & A \otimes_R A \\ & x \otimes y & \mapsto & \sum\limits_j x\alpha_j \otimes \beta_j y \end{array}$$

é uma aplicação bem-definida. Para verificar que ψ está bem-definida, precisamos verificar que ψ é S-balanceada e utilizar a Propriedade Universal do produto tensorial. Sendo $e_2 \in C_{S\otimes_R S}(S)$, para $x, y \in A$ e $b \in B$, segue que:

$$\begin{aligned}\psi(xs, y) &= \sum_{j=1}^{m}(xs)\alpha_j \otimes \beta_j y = xs\left(\sum_{j=1}^{m}\alpha_j \otimes \beta_j\right)y \\ &= x\left(\sum_{j=1}^{m}\alpha_j \otimes \beta_j\right)sy = x\sum_{j=1}^{m}\alpha_j \otimes \beta_j sy \\ &= \psi(x, sy).\end{aligned}$$

Segue que ψ é S-balanceada e pela Propriedade Universal do produto tensorial, existe uma única aplicação $\psi : A \otimes_S A \to A \otimes_R A$ tal que $\psi(x \otimes y) = \sum\limits_j x\alpha_j \otimes \beta_j y$.

Temos que $e = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i\alpha_j \otimes \beta_j b_i$ é o idempotente de separabilidade de A sobre R. De fato, representando por μ o homomorfismo referente a R-álgebra A, temos:

$$\begin{aligned}\mu(e) &= \sum_{i=1}^{n}\sum_{j=1}^{m} a_i\alpha_j\beta_j b_i = \sum_{i=1}^{n} a_i\left(\sum_{j=1}^{m}\alpha_j\beta_j\right)b_i \\ &= \sum_{i=1}^{n} a_i 1 b_i = 1.\end{aligned}$$

Além disso, $e \in C_{A\otimes_R A}(A)$, pois como $a \in C_{A\otimes_R A}(A)$, para $a \in A$, temos:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} aa_i\alpha_j \otimes \beta_j b_i = \psi(\sum_{i=1}^{n} aa_i \otimes b_i) = \psi(\sum_{i=1}^{n} a_i \otimes b_i a) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i\alpha_j\beta_j b_i a.$$

Portanto, A é uma R-álgebra separável. ∎

Proposição 2.16 *Sejam S uma R-álgebra comutativa e A uma S-álgebra que é separável sobre R. Então, A é uma S-álgebra separável.*

Demonstração. Suponha que A é separável sobre R. Então, pela Proposição 2.4, existe $e_1 = \sum_{i=1}^{n} a_i \otimes b_i \in A \otimes_R A$ um idempotente de separabilidade de A sobre R. Da Propriedade Universal do produto tensorial sobre R e sabendo que S é uma R-álgebra, existe um homomorfismo de $A \otimes_R A$-módulos à esquerda $\psi : A \otimes_R A \to A \otimes_S A$ dado por

$$\psi(a \otimes b) = a \otimes b \in A \otimes_S A,$$

para $a \otimes b \in A \otimes_R A$. O elemento $e = \psi(\sum_{i=1}^{n} a_i \otimes b_i)$ é um idempotente de separabilidade de A sobre S. De fato, representando por μ o homomorfismo referente a R-álgebra A, temos

que $\mu(e) = 1$, pois $\sum_{i=1}^{n} a_i b_i = 1$, por hipótese. Além disso, como ψ é um homomorfismo de $A \otimes_R A$-módulos à esquerda, para todo $a \in A$, temos que

$$(a \otimes 1)e = (a \otimes 1)\psi(\sum_{i=1}^{n} a_i \otimes b_i) = \psi\left(\sum_{i=1}^{n} aa_i \otimes b_i\right)$$
$$= \psi\left(\sum_{i=1}^{n} a_i \otimes b_i a\right) = (1 \otimes a)\psi\left(\sum_{i=1}^{n} a_i \otimes b_i\right).$$

Logo, $e \in C_{A\otimes_R A}(A)$. Assim, A é uma R-álgebra separável. ∎

O seguinte resultado é imediato das Proposições 2.15 e 2.16.

Corolário 2.17 *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 se A é uma R-álgebra separável, então A também é uma álgebra separável sobre seu centro. Na seção seguinte, provaremos um teorema (Teorema 2.26) que generaliza esse resultado.

2.2 Álgebras de Azumaya

Sejam R um anel comutativo e A uma R-álgebra. Pelo Corolário 2.17, vimos que se A é uma R-álgebra separável, então A é separável quando considerada como uma álgebra sobre seu centro. Agora, vamos nos dedicar ao estudo desse tipo de álgebra.

Dizemos que A é *central* se A é um R-módulo fiel e $R \cdot 1$ coincide com o centro de A. Ao lidar com álgebras fiéis, identificamos R com $R \cdot 1$ e, portanto, consideramos R como um subanel do centro de A. Uma R-álgebra A é uma álgebra de Azumaya se A é central e separável. Também nos referimos a este tipo de álgebra como sendo as álgebras centrais separáveis.

Para qualquer R-álgebra A temos que A pode ser considerada como um A^e-módulo à esquerda através do produto

$$(a \otimes b) \cdot x = axb, \text{ para } a, x \in A \text{ e } b \in A^o.$$

Esta estrutura induz um homomorfismo de R-álgebras $\varphi : A^e \to Hom_R(A, A)$ definido por

$$\varphi\left(\sum_{i=1}^{m} a_i \otimes b_i\right)(x) = \sum_{i=1}^{m} (a_i \otimes b_i) \cdot x = \sum_{i=1}^{m} a_i x b_i. \tag{2.3}$$

Nesta seção, vamos provar que se A é uma R-álgebra de Azumaya, então φ é na verdade um isomorfismo.

Lema 2.18 *Seja A uma R-álgebra de Azumaya, então R é um R-somando direto de A.*

Demonstração. Como A é uma álgebra de Azumaya, então A é central e separável sobre R. Seja $e \in A^e$ um idempotente de separabilidade de A sobre R. Seja φ a aplicação definida em (2.3) e considere o homomorfismo $\varphi(e) \in Hom_R(A, A)$. Como φ é um homomorfismo de anéis, então $\varphi(e)$ é um idempotente. Assim, temos que $\varphi(e)$ é uma projeção de A em A. Daí, $A = Im(\varphi(e)) \oplus ker(\varphi(e))$, pelo Lema 1.25. Vamos mostrar que $R = Im(\varphi(e))$. Como $Je = 0$, então para todo $a, b \in A$, temos

$$\begin{aligned} a\varphi(e)(b) &= (a \otimes 1) \cdot \varphi(e)(b) = (a \otimes 1) \cdot (e \cdot b) \\ &= ((a \otimes 1)e) \cdot b = ((1 \otimes a)e) \cdot b \\ &= (1 \otimes a) \cdot (e \cdot b) = (1 \otimes a) \cdot \varphi(e)(b) \\ &= \varphi(e)(b)a. \end{aligned}$$

Donde, $\varphi(e)(b) \in C(A) = R$. Logo, $Im(\varphi(e)) \subseteq R$. Por outro lado, representando por μ o homomorfismo de A sobre R, segue que $\mu(e) = 1$ e daí $\varphi(e)(1) = 1 \in Im(\varphi(e))$, provando a outra inclusão. Logo, $Im(\varphi(e)) = R$, o que mostra que R é um R-somando direto de A. ∎

Corolário 2.19 *Seja A uma R-álgebra de Azumaya. Se I é um ideal de R, então $IA \cap R = I$.*

Demonstração. Pelo Lema 2.18, temos que $A = L \oplus R$ para algum R-submódulo L de A. Então,

$$IA \cap R = I(L \oplus R) \cap R = (IL \oplus I) \cap R.$$

Como $R \cap L = \{0\}$, então $I \cap L = \{0\}$ e daí $IL \subset I \cap L = \{0\}$. Segue então que $IL \oplus I = I$ e portanto

$$IA \cap R = (IL \oplus I) \cap R = I \cap R = I.$$

∎

Proposição 2.20 *Sejam A e B R-álgebras de Azumaya, então $A \otimes B$ também é uma R-álgebra de Azumaya.*

Demonstração. [9, Proposição 3.3]. ∎

A seguir, apresentaremos um resultado técnico que será utilizado na demonstração do teorema de caracterização das álgebras de Azumaya.

Lema 2.21 *Sejam A uma R-álgebra de Azumaya e M um ideal maximal de A. Então, existe um ideal I de R tal que $IA = M$.*

Demonstração. [9, Lema 3.5]. ∎

O próximo teorema caracteriza as álgebras de Azumaya por meio do homomorfismo de R-álgebras φ e dos módulos progeradores.

Teorema 2.22 *Seja A uma R-álgebra. As seguintes afirmações são equivalentes:*

(i) A é uma álgebra de Azumaya;

(ii) A é um A^e-progerador e A é R-central;

(iii) A é um R-progerador e a aplicação $\varphi : A^e \to Hom_R(A, A)$ é um isomorfismo.

Demonstração.

$(ii) \Rightarrow (i)$ Suponha que (ii) seja verdadeiro. Em particular, A é A^e-projetivo e, portanto, A é R-separável, pela Proposição 2.4. Além disso, já que A é R-central, segue que A é uma álgebra de Azumaya.

$(ii) \Rightarrow (iii)$ Seja A um A^e-módulo progerador e R-central, então pelo Corolário 2.13

$$R \simeq C(A) \simeq Hom_{A^e}(A, A).$$

Pelos Teoremas de Morita (Corolário B.4), temos que A é um R-progerador. Além disso, pelo mesmo resultado, A^e é isomorfo a $Hom_R(A, A)$ através da aplicação dada pelo produto escalar, ou seja, a aplicação $\theta : A^e \to Hom_R(A, A)$ definida por

$$\theta(a \otimes b)(x) = \sum_{i=1}^{n} a_i x b_i = \varphi(a \otimes b)(x),$$

para $a \otimes b = \sum_{i=1}^{n} a_i \otimes b_i \in A^e$, $x \in A$ e φ definida como em 2.3.

$(iii) \Rightarrow (ii)$ Suponha que A é um R-progerador e a aplicação $\varphi : A^e \to Hom_R(A, A)$ é um isomorfismo. Pelos Teoremas de Morita, temos que A é um $Hom_R(A, A)$-progerador e assim A é um A^e-progerador. Além disso, temos que

$$R \simeq Hom_{Hom_R(A,A)}(A, A) \simeq Hom_{A^e}(A, A) \simeq C(A).$$

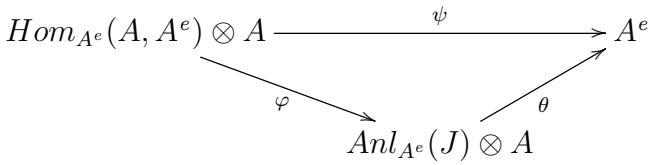
Logo, A é R-central.

$(i) \Rightarrow (ii)$ Suponha que A é uma álgebra de Azumaya. Por definição, temos que A é um A^e-módulo projetivo e claramente 1 gera A sobre A^e, então A é finitamente gerado sobre

A^e. Resta verificar que A é um A^e-gerador.Pelo item (ii) do Lema B.2, basta mostrar que a aplicação

$$\begin{array}{rccc} \psi: & A^* \otimes_R A & \to & A^e \\ & f \otimes a & \mapsto & f(a) \end{array}$$

é um isomorfismo, onde $A^* \otimes_{R=Hom_{A^e}(A,A)} A = Hom_{A^e}(A, A^e) \otimes A$. Pelo Corolário 2.14, $A^* = Hom_{A^e}(A, A^e)$ é isomorfo a $Ann_{A^e}(J)$ sobre a aplicação $f \mapsto f(1)$. Assim, considere o diagrama



onde

$$\begin{array}{rccc} \varphi: & Hom_{A^e}(A, A^e) \otimes A & \to & Anl_{A^e}(J) \otimes A \\ & f \otimes a & \mapsto & f(1) \otimes a \end{array}.$$

Definindo

$$\begin{array}{rccc} \theta: & Anl_{A^e}(J) \otimes A & \to & A^e \\ & b \otimes a & \mapsto & (1 \otimes a)b = (a \otimes 1)b \end{array},$$

temos que o diagrama é comutativo, pois

$$\begin{aligned} (\theta \circ \varphi)(f \otimes a) &= \theta(\varphi(f \otimes a)) = \theta(f(1) \otimes a) \\ &= (1 \otimes a)f(1) = f((1 \otimes a)1) \\ &= f(a) = \psi(f \otimes a). \end{aligned}$$

Como φ é um isomorfismo, então basta provar que θ é um isomorfismo, pois a composição de isomorfismos é ainda um isomorfismo.

Afirmação 2.23 *θ é um isomorfismo se, e somente se, $A^e Anl_{A^e}(J) = A^e$. De fato, suponha que θ é um isomorfismo. Observe que $A^e \subseteq A^e Anl_{A^e}(J)$, pois dado $y \in A^e$, existe $\sum_{i=1} b_i \otimes a_i \in Anl_{A^e}(J) \otimes A$ tal que $y = \theta(\sum_{i=1}^n b_i \otimes a_i) = \sum_{i=1}^n (1 \otimes a_i)b_i \in A^e Anl_{A^e}(J)$. A outra inclusão é imediata. Daí, temos a igualdade.*

Reciprocamente, suponha que $A^e Anl_{A^e}(J) = A^e$. Vamos construir uma inversa para θ. Seja $x \in A^e$, então $x = \sum_i (a_i \otimes b_i)c_i$, onde $\sum_i a_i \otimes b_i \in A^e$ e $c_i \in Anl_{A^e}(J)$. Sendo assim, defina

$$\begin{array}{rccc} \theta^{-1}: & A^e & \to & Anl_{A^e}(J) \otimes A \\ & x & \mapsto & \sum_i c_i \otimes a_i b_i \end{array}.$$

Agora, veja que:

$$\begin{aligned}\theta \circ \theta^{-1}(x) &= \theta\Big(\sum_i c_i \otimes a_i b_i\Big) = \sum_i (1 \otimes a_i b_i)c_i \\ &= \sum_i (1 \otimes b_i)(1 \otimes a_i)c_i = \sum_i (1 \otimes b_i)(a_i \otimes 1)c_i, \text{ pois } c_i \in Anl_{A^e}(J) \\ &= \sum_i (a_i \otimes b_i)c_i = x\end{aligned}$$

e

$$\theta^{-1} \circ \theta(b \otimes a) = \theta^{-1}((1 \otimes a)b) = b \otimes 1a = b \otimes a.$$

Portanto, θ é um isomorfismo, com inversa θ^{-1}.

Suponha por absurdo que $A^e Anl_{A^e}(J) \neq A^e$, ou seja, $A^e Anl_{A^e}(J)$ é um ideal próprio de A^e. Assim, existe um ideal maximal M de A^e que contém $A^e Anl_{A^e}(J)$. Como A e A^o são álgebras de Azumaya, então $A \otimes A^o = A^e$ também é uma álgebra de Azumaya. Pelo Lema 2.21, existe um ideal próprio I de R tal que $M = IA^e$. Então,

$$A^e Anl_{A^e}(J) \subseteq M = IA^e.$$

Aplicando a μ, temos

$$A^e \mu(Anl_{A^e}(J)) \subseteq \mu(IA^e) = IA.$$

Pelo Corolário 2.14, $\mu(Anl_{A^e}(J)) = C(A) = R$, então $A^e R = A \subseteq IA$. Daí, temos que $A = IA$ e isto implica que

$$A^e = IA^e = M.$$

O que é um absurdo, já que M é maximal. Portanto, $A^e Anl_{A^e}(J) = A^e$ e A é um A^e-gerador. Sendo assim, concluímos que A é um A^e-gerador e como A é uma álgebra de Azumaya, em particular, é R-central. ∎

Como decorrência do Teorema acima, temos os dois seguintes corolários que podem ser encontrados em [9].

Corolário 2.24 *Se A é uma Álgebra de Azumaya sobre R, então para qualquer R-módulo M, a aplicação*

$$\begin{array}{ccc}(M \otimes A)^A & \to & M \\ m \otimes 1 & \mapsto & m\end{array}$$

é um isomorfismo de R-módulos. Além disso, para qualquer A/R-módulo bilateral N, a aplicação

$$\begin{array}{ccc}N^A \otimes A & \to & N \\ \sum_i n_i \otimes a_i & \mapsto & \sum_i n_i a_i\end{array}$$

é um isomorfismo.

Corolário 2.25 *Seja A uma Álgebra de Azumaya sobre R. Então existe uma correspondência biunívoca entre os ideais I de R e os ideais U de A dada por*

$$I \mapsto IA \quad e \quad U \mapsto U \cap R.$$

Agora, vamos provar um resultado que justifica nossa divisão de estudo das álgebras separáveis em casos centrais e comutativos.

Teorema 2.26 *Uma R-álgebra A é separável se, e somente se, A é separável como uma álgebra sobre seu centro e seu centro é uma R- álgebra separável.*

Demonstração.

($\Rightarrow$) Suponha que A é uma R-álgebra separável, então A é separável e central sobre seu centro. Basta mostrar que $C(A)$ é separável sobre R. Como A é central separável sobre seu centro, então pelo Teorema 2.22, segue que A e A^o são $C(A)$-progerador e, em particular, A e A^o são $C(A)$-projetivo, assim temos que $A^e = A \otimes A^o$ é $C(A) \otimes C(A)$-projetivo, pela Proposição 1.44. Temos também, pela separabilidade de A, que A é um A^e-módulo projetivo. Assim, pela transitividade dos módulos projetivos (Proposição 1.43), temos que A é um $C(A) \otimes C(A)$-módulo projetivo. Logo, qualquer $C(A) \otimes C(A)$-somando direto de A é um $C(A) \otimes C(A)$-módulo projetivo, pela Proposição 1.41, pois qualquer somando direto de um módulo projetivo é também projetivo. Mas, como $C(A)$ é o centro de A, qualquer $C(A)$-somando direto de A é um $C(A) \otimes C(A)$-somando direto. Por A ser uma $C(A)$-álgebra separável central, segue do Lema 2.18 que $C(A)$ é um $C(A)$-somando direto de A. Logo, $C(A)$ é um $C(A) \otimes C(A)$-módulo projetivo e portanto $C(A)$ é separável sobre R, pela Proposição 2.4.

($\Leftarrow$) Reciprocamente, suponha que A é separável como uma álgebra sobre seu centro e seu centro é uma R- álgebra separável. Pela transitividade da separabilidade (Proposição 2.15), temos que A é R-separável. ∎

Proposição 2.27 *Seja E um R-progerador. Então, $A = Hom_R(E, E)$ é uma R-álgebra de Azumaya.*

Demonstração. [9, Proposição 4.1]. ∎

Corolário 2.28 *Seja A uma R-álgebra que é um R-módulo progerador. Então, R é um R-somando direto de qualquer subálgebra B de A.*

Demonstração. Seja B uma subálgebra de A. Pela Proposição 2.27, $Hom_R(A,A)$ é uma R-álgebra de Azumaya. Pelo Lema 2.18, R é um R-somando direto de $Hom_R(A,A)$, ou seja, existe um R-submódulo L de $Hom_R(A,A)$ tal que $L \cap R = \{0\}$ e $L + R = Hom_R(A,A)$. Podemos considerar A com uma subálgebra de $Hom_R(A,A)$, onde para cada $a \in A$, podemos identificá-lo com $\varphi_a \in Hom_R(A,A)$ dado por $\varphi_a(x) = ax$ para todo $x \in A$. Assim, temos as inclusões $R \subset B \subset A \subset Hom_R(A,A)$. Temos $R \cap (B \cap L) = \{0\}$ e pela lei modular (Proposição 1.5)

$$R + (B \cap L) = (R + L) \cap B = Hom_R(A,A) \cap B = B.$$

Logo, R é um R-somando direto de B. ∎

Sejam A uma R-álgebra e B uma subálgebra de A. Então, A é naturalmente um B/R-módulo bilateral e assim temos $A^B = \{a \in A \mid ab = ba, \text{ para todo } b \in B\}$. Observe que A^B é uma R-subálgebra de A que comuta com B.

Teorema 2.29 *Seja A uma R-álgebra de Azumaya. Suponha que B é uma subálgebra separável de A que contém R e considere $C = A^B$. Então, C é uma subálgebra separável de A e $A^C = B$. Se B é central, então C também é central e a aplicação de R-álgebras $B \otimes C \to A$ dada por $b \otimes c \mapsto bc$ é um isomorfismo.*

Demonstração. [9, Teorema 4.3]. ∎

Teorema 2.30 *Seja A uma R-álgebra de Azumaya. Suponha que B e C são subálgebras tais que*

$$\begin{array}{ccc} B \otimes C & \to & A \\ b \otimes c & \mapsto & bc \end{array}$$

é um isomorfismo de R-álgebras. Então, B e C são R-álgebras de Azumaya com $A^B = C$ e $A^C = B$.

Demonstração. [9, Teorema 4.4]. ∎

2.3 H-separabilidade

Nesta seção, sejam R um anel, A e B dois R-módulos à esquerda, $S = End_R(A)$ e $T = End_R(B)$. Vamos assumir também que todos os anéis têm unidade e todos os subanéis contém este elemento.

Temos que $Hom({}_RB, {}_RA)$ é um T-módulo à esquerda sobre a operação

$$h \cdot g = g \circ h, \text{ para todo } h \in T \text{ e } g \in Hom({}_RB, {}_RA).$$

Analogamente, $Hom({}_RB, {}_RA)$ é um S-módulo à direita com a operação

$$g \cdot f' = f' \circ g, \text{ para todo } f' \in S \text{ e } g \in Hom({}_RB, {}_RA).$$

É fácil ver que $Hom_R(B, A)$ é um (T, S)-bimódulo. Analogamente, temos que $Hom_R(A, B)$ é um (S, T)-bimódulo. Além disso, S e T operam à direita de A e B, respectivamente, e temos que A e B são (R, S)-bimódulos. Por fim, se $f \in Hom_R(A, B)$ e $g \in Hom_R(B, A)$, então $f \cdot g = g \circ f \in S$ e $g \cdot f = f \circ g \in T$.

Denotamos por $B|A$ se o R-módulo B é isomorfo a um somando direto de uma soma direta finita de cópias de ${}_RA$. Em outras palavras, $B|A$ se existe um R-módulo à esquerda B' tal que $A^{(n)} \simeq B \oplus B'$, para algum $n \in \mathbb{N}$.

Lema 2.31 *Sejam A e B R-módulos à esquerda. Então $B|A$ se, e somente se, existem homomorfismos de R-módulos à esquerda $f_j : A \to B$ e $g_j : B \to A$, com $j = 1, 2, \ldots, n$, tais que $\sum_{j=1}^{n} f_j \circ g_j = I_B$.*

Demonstração. Se $B|A$, então existem $n \in \mathbb{N}$ e um R-módulo à esquerda T tais que $A^{(n)} \simeq B \oplus T$. Considere

$$f_j = \pi \circ i_j : A \xrightarrow{i_j} A^{(n)} \xrightarrow{\pi} B \quad \text{e} \quad g_j = \pi_j \circ i : B \xrightarrow{i} A^{(n)} \xrightarrow{\pi_j} A,$$

para $j = 1, 2, \ldots, n$, onde π_j e i_j são as projeções e inclusões canônicas, respectivamente. Então, f_j e g_j são R-homomorfismos à esquerda e

$$\begin{aligned} \sum_{j=1}^{n} f_j \circ g_j &= \sum_{j=1}^{n} (\pi \circ i_j \circ \pi_j \circ i) = \pi \circ \sum_{j=1}^{n} (i_j \circ \pi_j) \circ i \\ &= \pi \circ I_{A^{(n)}} \circ i = I_B. \end{aligned}$$

Reciprocamente, suponha que existem $f_j : A \to B$ e $g_j : B \to A$, com $j = 1, 2, \ldots, n$, tais que $\sum_{j=1}^{n} f_j \circ g_j = I_B$. Considere $g : B \to A^n$ definida por $g(b) = (g_1(b), \ldots, g_n(b))$. Como g_j possui inversa à esquerda, então g_j é injetora, para todo $j = 1, 2, \ldots, n$, e daí g é também injetora. Além disso, sendo $Im(g)$ um submódulo de $A^{(n)}$, podemos considerar a projeção $\pi : A^{(n)} \to \frac{A^{(n)}}{Im(g)}$. Assim, temos a sequência exata (Exemplo 1.19 (v))

$$0 \longrightarrow B \xrightarrow{g} A^{(n)} \xrightarrow{\pi} \frac{A^{(n)}}{Im(g)} \longrightarrow 0 \tag{2.4}$$

Considerando $f : A^{(n)} \to B$ definida por

$$f(x_1, \ldots, x_n) = \sum_{j=1}^{n} f_j(x_j),$$

é imediato verificar que f é um R-homomorfismo à esquerda. Além disso, temos

$$f \circ g(b) = f(g(b)) = f(g_1(b), \ldots, g_n(b)) = \sum_{j=1}^{n} f_j(g_j(b)) = b.$$

Logo, pela Proposição 1.27, a sequência (2.4) cinde e portanto B é um somando direto de $A^{(n)}$, provando que $B|A$.

■

Existe um homomorfismo $\rho : Hom({}_RB, {}_RA) \otimes_S Hom({}_RA, {}_RB) \to Hom({}_RB, {}_RB) = T$ definido por $\rho(g \otimes f) = f \circ g$. De fato, para $f \in Hom({}_RA, {}_RB)$, $g \in Hom({}_RB, {}_RA)$ e $h \in S = End_R(A)$, observe que:

$$\rho(g \cdot h, f) = \rho(h \circ g, f) = f \circ h \circ g.$$

Por outro lado,

$$\rho(g, h \cdot f) = \rho(g, f \circ h) = f \circ h \circ g.$$

Logo, $\rho(g \cdot h, f) = \rho(g, h \cdot f)$, para quaisquer $f \in Hom({}_RA, {}_RB)$, $g \in Hom({}_RB, {}_RA)$ e $h \in S = End_R(A)$. Pela Propriedade Universal do produto tensorial, existe um único homomorfismo $\rho : Hom({}_RB, {}_RA) \otimes_S Hom({}_RA, {}_RB) \to Hom({}_RB, {}_RB) = T$ tal que $\rho(g \otimes f) = f \circ g$.

Proposição 2.32 *[16,* Proposição 1.1] *Vale que $B|A$ se, e somente se, ρ é um epimorfismo. Se ρ é um epimorfismo, então ρ é um isomorfismo.*

Demonstração. Suponha que $B|A$. Então, pelo Lema 2.31, existe um número finito de $g_i \in Hom({}_RB, {}_RA)$ e $f_i \in Hom({}_RA, {}_RB)$, $i = 1, \ldots, n$, tais que $\sum_{i=1}^{n} f_i \circ g_i = I_B$. Seja $\varphi \in T$. Considere $\varphi_i = g_i \circ \varphi \in Hom({}_RB, {}_RA)$, para todo $i = 1, 2, \ldots, n$, então:

$$\rho\left(\sum_{i=1}^{n} \varphi_i \otimes f_i\right) = \sum_{i=1}^{n} f_i \circ \varphi_i = \left(\sum_{i=1}^{n} f_i \circ g_i\right) \circ \varphi = I_B \circ \varphi = \varphi.$$

Logo, ρ é sobrejetora. Como ρ já é um homomorfismo, segue que ρ é um epimorfismo. Reciprocamente, suponha que ρ é um epimorfismo. Então, existem aplicações $g_i \in Hom({}_RB, {}_RA)$ e $f_i \in Hom({}_RA, {}_RB)$ tais que $\rho\big(\sum_{i=1}^{n} g_i \otimes f_i\big) = I_B$, ou seja, $\sum_{i=1}^{n} f_i \circ g_i = I_B$. Pelo Lema 2.31, $B|A$.

Agora, suponha que ρ é um epimorfismo e vejamos que ρ é um isomorfismo. Pelo que vimos acima, $B|A$, ou seja, existem $g_i \in Hom({}_RB, {}_RA)$ e $f_i \in Hom({}_RA, {}_RB)$, $i =$

$1, 2, \ldots, n$, tais que $\sum_{i=1}^{n} f_i \circ g_i = I_B$. Vamos construir uma inversa para ρ. Defina

$$\begin{array}{rccl} \overline{\rho}: & T & \to & Hom({}_RB, {}_RA) \otimes_S Hom({}_RA, {}_RB) \\ & \varphi & \mapsto & \sum_{i=1}^{n} g_i \circ \varphi \otimes f_i \end{array}.$$

Como $g_i \circ \varphi \in Hom({}_RB, {}_RA)$, para todo $i = 1, 2, \ldots, n$, então $\overline{\rho}$ está bem-definida. Sejam $\varphi \in T, g \in Hom({}_RB, {}_RA)$ e $f \in Hom({}_RA, {}_RB)$. Temos:

$$\begin{aligned} \rho \circ \overline{\rho}(\varphi) = \rho(\overline{\rho}(\varphi)) &= \rho\left(\sum_{i=1}^{n} g_i \circ \varphi \otimes f_i\right) \\ &= \sum_{i=1}^{n} f_i \circ (g_i \circ \varphi) = \sum_{i=1}^{n} (f_i \circ g_i) \circ \varphi \\ &= I_B \circ \varphi = \varphi. \end{aligned}$$

Por outro lado,

$$\begin{aligned} \overline{\rho} \circ \rho(g \otimes f) = \overline{\rho}(\rho(g \otimes f)) = \overline{\rho}(f \circ g) &= \sum_{i}^{n} g_i \circ (f \circ g) \otimes f_i \\ &= \sum_{i}^{n} (g_i \circ f) \circ g \otimes f_i = \sum_{i=1}^{n} g \cdot \underbrace{(g_i \circ f)}_{\in S} \otimes f_i \\ &= \sum_{i=1}^{n} g \otimes (g_i \circ f) \cdot f_i = \sum_{i=1}^{n} g \otimes f_i \circ g_i \circ f \\ &= g \otimes \left(\sum_{i=1}^{n} f_i \circ g_i\right) \circ f = g \otimes I_B \circ f \\ &= g \otimes f. \end{aligned}$$

Portanto, $\overline{\rho}$ é a inversa de ρ. Como ρ é um homomorfismo com inversa $\overline{\rho}$, então ρ é um isomorfismo. ∎

Observação 2.33 *$Hom(Hom({}_RB, {}_RA)_S, S_S)$ é um (S,T)-bimódulo. Inicialmente, vamos determinar a estrutura de S-módulo à esquerda que $Hom(Hom({}_RB, {}_RA)_S, S_S)$ possui. Sejam $\varphi \in Hom(Hom({}_RB, {}_RA)_S, S_S)$ e $f \in S$. Dado $g \in Hom({}_RB, {}_RA)$, defina*

$$(f \cdot \varphi)(g) = \varphi(f \circ g).$$

Vejamos que essa operação faz de $Hom(Hom({}_RB, {}_RA)_S, S_S)$ um S-módulo à esquerda. Sejam $\varphi \in Hom(Hom({}_RB, {}_RA)_S, S_S), f, f' \in S$ e $g \in Hom({}_RB, {}_RA)$. Já que $Hom({}_RB, {}_RA)$ é um S-módulo à direita, temos:

$$((f \cdot f') \cdot \varphi)(g) = \varphi((f \cdot f') \circ g) = \varphi(g \cdot (f \cdot f')) = \varphi((g \cdot f) \cdot f')$$

e

$$(f \cdot (f' \cdot \varphi))(g) = (f' \cdot \varphi)(g \cdot f) = \varphi((g \cdot f) \cdot f').$$

Como as outras propriedades são de fácil verificação, segue que $Hom(Hom({}_RB, {}_RA)_S, S_S)$ *é um* S*-módulo à esquerda.*

Além disso, $Hom(Hom({}_RB, {}_RA)_S, S_S)$ *é um* T*-módulo à direita com a operação*

$$(\varphi \cdot h)(g) = \varphi(g \circ h),$$

para todo $\varphi \in Hom(Hom({}_RB, {}_RA)_S, S_S), h \in T$ *e* $g \in Hom({}_RB, {}_RA)$.

Agora, sendo ${}_THom({}_RB, {}_RA)_S$*, observe que para todo* $\varphi \in Hom(Hom({}_RB, {}_RA)_S, S_S)$, $f' \in S$ *e* $h \in T$*, temos:*

$$\begin{aligned}((f' \cdot \varphi) \cdot h)(g) &= (f' \cdot \varphi)(g \circ h) = (f' \cdot \varphi)(h \cdot g) \\ &= \varphi((h \cdot g) \cdot f') = \varphi(h \cdot (g \cdot f')) \\ &= (\varphi \cdot h)(g \cdot f) = (f' \cdot (\varphi \cdot h))(g).\end{aligned}$$

Isso mostra que $Hom(Hom({}_RB, {}_RA)_S, S_S)$ *é um* (S, T)*-bimódulo.*

Existe um homomorfismo $\psi : Hom({}_RA, {}_RB) \to Hom(Hom({}_RB, {}_RA)_S, S_S)$ definido por $\psi(f)(g) = g \circ f$ para $f \in Hom({}_RA, {}_RB)$ e $g \in Hom({}_RB, {}_RA)$. De fato, vejamos que ψ está bem-definida. Para isso, devemos verificar que $\psi(f)$ é S-linear à direita, ou seja, $\psi(f)(g \cdot h) = \psi(f)(g) \cdot h$, para todo $h \in S$. Observe que:

$$\psi(f)(g \cdot h) = \psi(f)(h \circ g) = (h \circ g) \circ f = h \circ (g \circ f) = h \circ \psi(f)(g) = \psi(f)(g) \cdot h,$$

para todo $h \in S$. Para $f' \in S$, observe que:

$$\psi(f' \cdot f)(g) = \psi(f \circ f')(g) = g \circ f \circ f'. \tag{2.5}$$

Por outro lado,

$$(f' \cdot \psi(f))(g) = \psi(f)(g \cdot f') = \underbrace{\psi(f)(g)}_{\in S} \cdot f' = g \circ f \circ f'. \tag{2.6}$$

De (2.5) e (2.6), concluímos que ψ é S-linear à esquerda.

Agora, vejamos que ψ é T-linear à direita. Sabendo que $Hom(Hom({}_RA, {}_RB)_S, S_S)$ é um T-módulo à direita, para $f \in Hom({}_RA, {}_RB), g \in Hom({}_RB, {}_RA)$ e $h \in T$, temos:

$$\psi(f \cdot h)(g) = \psi(h \circ f)(g) = g \circ h \circ f$$

e

$$(\psi(f) \cdot h)(g) = \psi(f)(g \circ h) = g \circ h \circ f.$$

Portanto, ψ é (S,T)-homomorfismo.

Analogamente, o conjunto $Hom({}_SHom({}_RB,{}_RA),{}_SS)$ é um (T,S)-bimódulo com ações definidas por

$$(g\cdot\varphi)(f)=\varphi(g\circ f)\quad\text{e}\quad(\varphi\cdot h)(f)=\varphi(f\circ h),$$

para $\varphi\in Hom({}_SHom({}_RB,{}_RA),{}_SS), g\in T, f\in Hom({}_RB,{}_RA)$ e $h\in S$. A aplicação $\psi' : Hom({}_RB,{}_RA)\to Hom({}_SHom({}_RA,{}_RB),{}_SS)$ definida por $\psi'(g)(f)=g\circ f$ é um (T,S)-homomorfismo.

Lema 2.34 *Considere as seguintes aplicações:*

(a) $I\otimes\psi : A\otimes_S Hom({}_RA,{}_RB)\to A\otimes_S Hom(Hom({}_RB,{}_RA)_S,S_S)$ *definida por* $(I\otimes\psi)(a\otimes f)=a\otimes\psi(f)$*;*

(b) $\tau : A\otimes_S Hom({}_RA,{}_RB)\to B$ *definida por* $\tau(a\otimes f)=f(a)$*;*

(c) $i : B\to Hom(Hom({}_RB,{}_RA)_S,A_S)$ *definida por* $i(b)(g)=g(b)$*;*

(d) $\nu : A\otimes_S Hom(Hom({}_RB,{}_RA)_S,S_S)\to Hom(Hom({}_RB,{}_RA)_S,A_S)$ *definida por* $\nu(a\otimes h)(g)=h(g)(a)$*;*

onde $a\in A, f\in Hom({}_RA,{}_RB), b\in B, g\in Hom({}_RB,{}_RA)$ *e* $h\in Hom(Hom({}_RB,{}_RA)_S,S_S)$. *Temos que todas as aplicações acima definidas são* (R,T)*-homomorfismos. Além disso,*

$$i\circ\tau=\nu\circ(I\otimes\psi).$$

Demonstração. Vejamos cada um dos casos:

(a) Como ψ é um T-homomorfismo à direita, segue imediatamente que $I\otimes\psi$ é um (R,T)-homomorfismo.

(b) Inicialmente, provaremos que τ está bem-definida. Considere $f,f'\in S$ e $a\in A$, temos:

$$\tau(a\cdot f',f)=\tau(f'(a),f)=f(f'(a))$$

e

$$\tau(a,f'\cdot f)=\tau(a,f\circ f')=f\circ f'(a)=f(f'(a)).$$

Logo, τ é S-balanceada. Pela Propriedade Universal do produto tensorial, garantimos a existência do homomorfismo τ. Como f é R-linear à esquerda, segue que τ também é R-linear à esquerda. Além disso, para $a\in A, f\in Hom({}_RA,{}_RB)$ e $g'\in T$, temos

$$\tau(r\cdot a\otimes f)=f(r\cdot a)=r\cdot f(a)=r\cdot\tau(a\otimes f)$$

e

$$\tau(a \otimes f \cdot g') = \tau(a \otimes g' \circ f) = g'(f(a)) = \tau(a \otimes f) \cdot g'.$$

Logo, τ é T-linear à direita.

(c) Inicialmente, mostremos que i está bem-definida, ou seja, $i(b)$ é S-linear á direita. Sejam $f \in S, g \in Hom({}_RB, {}_RA)$ e $b \in B$, temos:

$$i(b)(g \cdot f) = i(b)(f \circ g) = f(g(b)).$$

Por outro lado,

$$i(b)(g) \cdot f = f(i(b)(g)) = f(g(b)).$$

Agora, vejamos que i é um (R, T)-homomorfismo. Como g é R-linear à esquerda, segue que i também é. Além disso, seja $g' \in T, g \in Hom({}_RB, {}_RA)$ e $b \in B$, temos:

$$i(b \cdot g')(g) = i(g'(b))(g) = g(g'(b))$$

e por outro lado

$$(i(b) \cdot g')(g) = i(b)(g \circ g') = g(g'(b)).$$

Logo, i é T-linear à direita.

(d) Vejamos a boa definição da aplicação ν. Seja $f' \in S$. Observe que:

$$\nu(a \cdot f', h)(g) = h(g)(a \cdot f') = h(g)(f'(a)) = (h(g) \circ f')(a)$$

e

$$\nu(a, f' \cdot h)(g) = (f' \cdot h)(g)(a) = h(g \cdot f')(a) = (\underbrace{h(g)}_{\in S} \cdot f')(a) = (h(g) \circ f')(a),$$

pois h é S-linear à direita. Pela Propriedade Universal do produto tensorial sobre S, temos que ν está bem-definida. Dado $r \in R$, temos:

$$\nu(r \cdot a \otimes h)(g) = h(g)(r \cdot a) = r \cdot h(g)(a) = r \cdot \nu(a \otimes h)(g).$$

Agora, seja $h' \in T$, temos:

$$\nu[(a \otimes h) \cdot h'](g) = (h \cdot h')(g)(a) = h(g \circ h')(a).$$

Por outro lado,

$$[(\nu(a \otimes h)) \cdot h'](g) = \nu(a \otimes h)(g \circ h') = h(g \circ h')(a).$$

Logo, ν é (R,T)-linear.

Agora, para $a \in A, f \in Hom({}_RA, {}_RB), g \in Hom({}_RB, {}_RA)$, temos:

$$\begin{aligned} i \circ \tau(a \otimes f)(g) &= i(\tau(a \otimes f))(g) = i(f(a))(g) \\ &= g(f(a)) = g \circ f(a) \end{aligned}$$

e por outro lado

$$\begin{aligned} \nu \circ (I \otimes \psi)(a \otimes f)(g) &= \nu((I \otimes \psi)(a \otimes f))(g) = \nu(a \otimes \psi(f))(g) \\ &= \psi(f)(g)(a) = g \circ f(a). \end{aligned}$$

Assim, $i \circ \tau = \nu \circ (I \otimes \psi)$.

■

Pelo Lema 2.34, obtemos o diagrama comutativo

$$\begin{array}{ccc} A \otimes_S Hom({}_RA, {}_RB) & \xrightarrow{I \otimes \psi} & A \otimes_S Hom(Hom({}_RB, {}_RA)_S, S_S) \\ \downarrow{\scriptstyle \tau} & \circlearrowleft & \downarrow{\scriptstyle \nu} \\ B & \xrightarrow[i]{} & Hom(Hom({}_RB, {}_RA)_S, A_S) \end{array}$$

Teorema 2.35 *Se $B|A$, então temos:*

(i) ψ e ψ' são isomorfismos;

(ii) Todos os homomorfismos do Lema 2.34 são isomorfismos;

(iii) $Hom({}_RA, {}_RB)$ é um S-módulo à esquerda projetivo e finitamente gerado assim como é um T-módulo gerador à direita. $Hom({}_RB, {}_RA)$ é um S-módulo à direita projetivo e finitamente gerado assim como é um T-módulo gerador à esquerda.

(iv) $Hom({}_SHom({}_RA, {}_RB), {}_SHom({}_RA, {}_RB)) \simeq T$ e $Hom(Hom({}_RB, {}_RA)_S, Hom({}_RB, {}_RA)_S) \simeq T$ como anéis.

Demonstração. [16, Teorema 1.2]. ■

Definição 2.36 *Seja $A \supseteq R$ anéis com a mesma unidade. Dizemos que A é uma extensão H-separável de R se $A \otimes_R A$ é isomorfo a um somando direto de uma soma direta finita de cópias de A como A-bimódulo, ou seja, $A \otimes_R A|A$.*

Lema 2.37 *Sejam A um anel com unidade e R um subanel de A com a mesma unidade. Considere os A-bimódulos $A \otimes_R A$ e A. Então, temos os seguintes isomorfismos de A-bimódulos:*

(i) $Hom(A, A) \simeq C(A)$.

(ii) $Hom(A \otimes_R A, A \otimes_R A) \simeq C_{A\otimes_R A}(R) = \{\varepsilon \in A \otimes_R A \mid r\varepsilon = \varepsilon r, \textit{ para todo } r \in R\}$.

(iii) $Hom(A \otimes_R A, A) \simeq C_A(R)$.

(iv) $Hom(A, A \otimes_R A) \simeq C_{A\otimes_R A}(A)$.

Demonstração. Como o procedimento para verificar cada uma das identificações acima é semelhante, vamos provar apenas (iii). Defina

$$\begin{array}{rccc} \varphi: & Hom(A \otimes_R A, A) & \to & C_A(R) \\ & f & \mapsto & f(1 \otimes 1) \end{array}.$$

Vejamos que φ está bem-definida. Como $R \subset A$ e $f \in Hom(A \otimes_R A, A)$, temos:

$$\begin{aligned} r \cdot f(1 \otimes 1) &= f(r \cdot (1 \otimes 1)) = f(r \otimes 1) \\ &= f(1 \otimes r \cdot 1) = f(1 \otimes 1 \cdot r) \\ &= f(1 \otimes 1) \cdot r. \end{aligned}$$

Assim, $f(1 \otimes 1) \in C_A(R)$. Dado $d \in C_A(R)$, defina a aplicação

$$\begin{array}{rccc} \varphi_d: & A \otimes_R A & \to & A \\ & x \otimes y & \mapsto & xdy \end{array}.$$

Dado $r \in R$, temos

$$\varphi_d(xr, y) = xrdy = xdry = \varphi_d(x, ry).$$

Logo, φ_d é R-balanceada e portanto está bem-definida.

Vejamos que a inversa de φ é dada por

$$\begin{array}{rccc} \varphi^{-1}: & C_A(R) & \to & Hom(A \otimes_R A, A) \\ & d & \mapsto & \varphi_d \end{array}.$$

De fato, para $d \in C_A(R)$, $f \in Hom(A \otimes_R A, A)$ e $x \otimes y \in A \otimes_R A$, temos:

$$\varphi \circ \varphi^{-1}(d) = \varphi(\varphi_d) = \varphi_d(1 \otimes 1) = 1d1 = d$$

e

$$\varphi^{-1} \circ \varphi(f)(x \otimes y) = \varphi^{-1}(f(1 \otimes 1))(x \otimes y) = xf(1 \otimes 1)y = f(x \otimes y).$$

Logo, φ é um isomorfismo, com inversa φ^{-1}.

■

Teorema 2.38 *[24,* Teorema 1.1] *Sejam $A \supseteq R$ anéis com a mesma unidade. Então, $A \supseteq R$ é uma extensão H-separável se, e somente se, $C_A(R)$ é um $C(A)$-módulo projetivo e finitamente gerado e $\eta : A \otimes_R A \to Hom_{C(A)}(C_A(R), A)$ tal que $\eta(x \otimes y)(d) = xdy$ é um isomorfismo de A-bimódulos.*

Demonstração. Suponha que A é uma extensão H-separável de R. Como $A \otimes_R A$ pode ser visto como um R-módulo à esquerda ($R \subseteq A$), aplicando as conclusões do Teorema 2.35, temos o seguinte diagrama comutativo, onde todos os homomorfismos do diagrama são na verdade isomorfismos.

$$\begin{array}{ccc} A \otimes_S Hom({}_RA, A \otimes_R A) & \xrightarrow{I \otimes \psi} & A \otimes_S Hom(Hom(A \otimes_R A, {}_RA)_S, S_S) \\ \downarrow{\scriptstyle \tau} & \circlearrowleft & \downarrow{\scriptstyle \nu} \\ A \otimes_R A & \xrightarrow[i]{} & Hom(Hom(A \otimes_R A, {}_RA)_S, A_S) \end{array}$$

Pelo Lema 2.37, sabemos que $Hom({}_AA_A, {}_AA_A) \simeq C(A)$ e $\varphi : Hom(A \otimes_R A, {}_AA_A) \to C_A(R)$ dada por $\varphi(f) = f(1 \otimes 1)$ é um isomorfismo, para todo $f \in Hom(A \otimes_R A, {}_AA_A)$. Assim, $S = End_R(A) \simeq C(A)$ e temos que $i : A \otimes_R A \to Hom_{C(A)}(C_A(R), A)$ é um isomorfismo. Então, temos o diagrama comutativo

$$\begin{array}{ccc} A \otimes_R A & \xrightarrow{\quad i \quad} & Hom_{C(A)}(Hom(A \otimes_R A, A), A) \\ & {\scriptstyle \eta} \searrow \quad \swarrow {\scriptstyle Hom(\varphi, A)} & \\ & Hom_{C(A)}(C_A(R), A) & \end{array}$$

onde $Hom(\varphi, A)(f) = f \circ \varphi^{-1}$, com $\varphi^{-1} : C_A(R) \to Hom_{A-A}(A \otimes_R A, A)$. De fato, para todo $d \in C_A(R)$ e $x \otimes y \in A \otimes_R A$, temos:

$$\begin{aligned} Hom(\varphi, A) \circ i(x \otimes y)(d) &= Hom(\varphi, A)(i(x \otimes y))(d) = i(x \otimes y)(\varphi^{-1}(d)) \\ &= \varphi^{-1}(d)(x \otimes y) = xdy \\ &= \eta(d)(x \otimes y). \end{aligned}$$

Logo, $\eta = Hom(\varphi, A) \circ i$ é um isomorfismo.

Além disso, pelo item (iii) do Teorema 2.35, segue que $Hom(A \otimes_R A, A) \simeq C_A(R)$ é um $C(A)$-módulo projetivo e finitamente gerado.

Reciprocamente, suponha que $C_A(R)$ é um $C(A)$-módulo projetivo e finitamente gerado e $\eta : A \otimes_R A \to Hom_{C(A)}(C_A(R), A)$ tal que $\eta(x \otimes y)(d) = xdy$ é um isomorfismo de A-bimódulos. Uma vez que $C_A(R)$ é um $C(A)$-módulo projetivo e finitamente gerado e o centro de A é um anel comutativo, segue que

$$\psi : C_A(R) \otimes_{C(A)} Hom_{A^e}(A, A \otimes_R A) \to Hom_{A^e}(Hom_{C(A)}(C_A(R), A), A \otimes_R A)$$

dado por $\psi(d \otimes f)(h) = f(h(d))$ é um isomorfismo (Proposição 1.45). Pelo Lema 2.37, temos que

$$\begin{array}{rccc} \varphi: & Hom_{A^e}(A \otimes_R A, A) & \to & C_A(R) \\ & f & \mapsto & f(1 \otimes 1) \end{array}$$

é um isomorfismo. Então, temos os isomorfismos,

$$\begin{array}{c} Hom_{A^e}(A \otimes_R A, A) \otimes_{C(A)} Hom_{A^e}(A, A \otimes_R A) \\ \downarrow{\scriptstyle \varphi \otimes I} \\ C_A(R) \otimes_{C(A)} Hom_{A^e}(A, A \otimes_R A) \\ \downarrow{\scriptstyle \psi} \\ Hom_{A^e}(Hom_{C(A)}(C_A(R), A), A \otimes_R A) \\ \downarrow{\scriptstyle Hom(\eta^{-1}, A \otimes_R A)} \\ Hom_{A^e}(A \otimes_R A, A \otimes_R A) \end{array}$$

onde $Hom(\eta^{-1}, A \otimes_R A)(f) = f \circ \eta$. A composição $\psi' : Hom_{A^e}(A \otimes_R A, A) \otimes_{C(A)} Hom_{A^e}(A, A \otimes_R A) \to Hom_{A^e}(A \otimes_R A, A \otimes_R A)$ é dada por $\psi'(f \otimes g) = g \circ f$. De fato, veja que:

$$\begin{aligned} \psi'(f \otimes g)(a \otimes b) &= Hom(\eta^{-1}, A \otimes_R A) \circ \psi \circ (\varphi \otimes I)(f \otimes g)(a \otimes b) \\ &= Hom(\eta^{-1}, A \otimes_R A)(\psi(\varphi(f) \otimes g))(a \otimes b) \\ &= Hom(\eta^{-1}, A \otimes_R A)(\psi(f(1 \otimes 1) \otimes g))(a \otimes b) \\ &= \psi(f(1 \otimes 1) \otimes g)(\eta(a \otimes b)) = g(\eta(a \otimes b)(f(1 \otimes 1)) \\ &= g(af(1 \otimes 1)b) = g((a \otimes b) \cdot f(1 \otimes 1)), \text{ pois f é } A^e\text{-linear} \\ &= g(f(a \otimes b)(1 \otimes 1)) = g(f(a \otimes b)) = g \circ f(a \otimes b), \end{aligned}$$

para todo $a \otimes b \in A \otimes_R A$. Portanto, $\psi' : Hom_{A^e}(A \otimes_R A, A) \otimes_{C(A)} Hom_{A^e}(A, A \otimes_R A) \to Hom_{A^e}(A \otimes_R A, A \otimes_R A)$ tal que $\psi'(f \otimes g) = g \circ f$ é um isomorfismo e, em particular, é um epimorfismo. Pela Proposição 2.32, segue que $A \otimes_R A | A$, onde A tem uma estrutura de A^e-módulo à esquerda, assim como $A \otimes_R A$. Pela Observação 2.11, temos que $A \otimes_R A$ é um A-bimódulo e daí $A \otimes_R A | A$, ou seja, A é uma extensão H-separável de R.

■

Observação 2.39 *Como $C(A) \subseteq C_A(R)$, então $C_A(R)$ é $C(A)$-fiel. Se $A \otimes_R A | A$, pelo Teorema 2.38, $C_A(R)$ é um $C(A)$-módulo projetivo e finitamente gerado. Sendo $C(A)$ um anel comutativo e $C_A(R)$ um $C(A)$-módulo projetivo, finitamente gerado e fiel, segue que $C_A(R)$ é um $C(A)$-progerador (Corolário 1.52). Pelo Corolário 2.28, $C(A)$ é um $C(A)$-somando direto de $C_A(R)$.*

Proposição 2.40 *Sejam A um anel e Δ um subanel de A contendo $C(A)$. Defina um epimorfismo de A-bimódulos $\varphi_0 : Hom_{C(A)}(\Delta, A) \to A$ por $\varphi_0(f) = f(1)$. Então, existe um homomorfismo de A-bimódulos $\psi_0 : A \to Hom_{C(A)}(\Delta, A)$ tal que $\varphi_0 \circ \psi_0 = I_A$ se, e somente se, $C(A)$ é um $C(A)$-somando direto de Δ.*

Demonstração. Inicialmente, observe que $Hom_{C(A)}(\Delta, A)$ é um A-bimódulo, com as ações à esquerda e à direita definidas por

$$(a \cdot g)(d) = ag(d) \quad \text{e} \quad (g \cdot a)(d) = g(d)a,$$

para todo $a \in A$, $g \in Hom_{C(A)}(\Delta, A)$ e $d \in \Delta$. Agora, suponha que existe um homomorfismo de A-bimódulos $\psi_0 : A \to Hom_{C(A)}(\Delta, A)$ tal que $\varphi_0 \circ \psi_0 = I_A$. Considere $g = \psi_0(1) \in Hom_{C(A)}(\Delta, A)$. Mostremos que $g \in Hom_{C(A)}(\Delta, C(A))$ e $g^2 = g$. Para $a \in A$, temos:

$$a \cdot g = a \cdot \psi_0(1) = \psi_0(a1) = \psi_0(1a) = \psi_0(1) \cdot a = g \cdot a.$$

Assim $(a \cdot g)(d) = (g \cdot a)(d)$, para todo $a \in A$ e $d \in \Delta$, então $ag(d) = g(d)a$. Logo, $g(d) \in C(A)$. Isso mostra que $g \in Hom_{C(A)}(\Delta, C(A))$. Observe que:

$$1 = \varphi_0 \circ \psi_0(1) = \varphi_0 \circ g = \varphi_0(g) = g(1).$$

Sendo $c \in C(A)$ e $g \in Hom_{C(A)}(\Delta, C(A))$, segue que

$$g(c) = g(c1) = cg(1) = c1 = c.$$

Como $g(d) \in C(A)$, pela igualdade acima, obtemos que

$$g(g(d)) = g(d), \text{ para todo } d \in \Delta.$$

Portanto, $g^2 = g$. Assim, $C(A)$ é um somando direto de Δ, pela Proposição 1.25.

Reciprocamente, suponha que $C(A)$ é um $C(A)$-somando direto de Δ. Então, existe $p \in Hom_{C(A)}(\Delta, C(A))$ tal que $p^2 = p$. Assim, $p(d) \in C(A)$ para todo $d \in \Delta$ e $p(1) = 1$. Logo, $ap(d) = p(d)a$, para todo $a \in A$. Defina

$$\begin{array}{rccc} \psi_0 : & A & \to & Hom_{C(A)}(\Delta, A) \\ & a & \mapsto & a \cdot p = p \cdot a \end{array}.$$

Nessas condições, temos que ψ_0 é um homomorfismo de A-bimódulos. Agora, veja que para todo $a \in A$, temos:

$$\begin{aligned}\varphi_0 \circ \psi_0(a) &= \varphi_0(\psi_0(a)) = \varphi_0((a \cdot p)) \\ &= (a \cdot p)(1) = ap(1) \\ &= a1 = a.\end{aligned}$$

e portanto $\varphi_0 \circ \psi_0 = I_A$. ∎

A partir desses resultados, conseguimos provar que se A é uma extensão H-separável de R, então A é uma extensão separável de R, onde $A \supseteq R$ são anéis com mesma unidade.

Teorema 2.41 *[16,* Teorema 2.2] *Sejam A um anel e R um subanel de A. Se $A \otimes_R A$ é isomorfo a um somando direto de uma soma direta finita de cópias de A como A-bimódulos (ou seja, A é uma extensão H-separável de R), então $C_A(R)$ é um $C(A)$-módulo projetivo e finitamente gerado e A é uma extensão separável de R.*

Demonstração. Como $A \otimes_R A|A$, então $C_A(R)$ é uma $C(A)$-módulo projetivo e finitamente gerado e $\eta : A \otimes_R A \to Hom_{C(A)}(C_A(R), A)$ tal que $\eta(x \otimes y)(d) = xdy$ é um isomorfismo de A-bimódulos, pelo Teorema 2.38. Considere o diagrama

$$\begin{array}{ccc} A \otimes_R A & \xrightarrow{\eta} & Hom_{C(A)}(C_A(R), A) \\ & {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\varphi_0} & \\ & A & \end{array}$$

onde $\eta(x \otimes y)(d) = xdy, \varphi(x \otimes y) = xy$ e $\varphi_0(f) = f(1)$. Observe que:

$$\begin{aligned}\varphi_0 \circ \eta(x \otimes y) &= \varphi_0(\eta(x \otimes y)) = \eta(x \otimes y)(1) \\ &= x1y = xy = \varphi(x \otimes y).\end{aligned}$$

Logo, $\varphi_0 \circ \eta = \varphi$, mostrando que o diagrama acima é comutativo. Pela Observação 2.39, $C(A)$ é um $C(A)$-somando direto de $C_A(R)$. Aplicando a Proposição 2.40, temos que existe um homomorfismo de A-bimódulos $\psi_0 : A \to Hom_{C(A)}(C_A(R), A)$ tal que $\varphi_0 \circ \psi_0 = I_A$. Uma vez que η é um isomorfismo de A-bimódulos, existe a inversa $\eta^{-1} : Hom_{C(A)}(C_A(R), A) \to A \otimes_R A$. Defina $\psi = \eta^{-1} \circ \psi_0$. Assim, ψ é um homomorfismo de A-bimódulos. Além disso,

$$\varphi \circ \psi = \varphi_0 \circ \eta \circ \eta^{-1} \circ \psi_0 = \varphi_0 \circ \psi_0 = I_A.$$

Portanto, a sequência cinde, o que mostra que A é separável sobre R, pela Observação 2.7. ∎

A seguinte definição pode ser encontrada em [15].

Definição 2.42 *Sejam R um anel e M um R-bimódulo. Dizemos que M é centralmente projetivo sobre R se M é isomorfo a um somando direto de uma soma direta finita de cópias de R como um R-bimódulo.*

Lema 2.43 *Um R-bimódulo M é centralmente projetivo sobre R se, e somente se, existem $g_i \in Hom({}_RM_R, {}_RR_R)$ e $m_i \in C_M(R), i = 1, 2, \ldots, n$, tais que $m = \sum_{i=1}^{n} g_i(m)m_i$, para todo $m \in M$.*

Demonstração. Pelo Lema 2.31, existem homomorfismos de R-bimódulos $f_i : R \to M$ e $g_i : M \to R$, com $i = 1, 2, \ldots, n$, tais que $\sum_{i=1}^{n} f_i \circ g_i = I_M$. Observe que $f_i(1) \in C_M(R)$, pois para todo $i = 1, 2, \ldots, n$, temos

$$f_i(1) \cdot r = f_i(1r) = f_i(r1) = r \cdot f_i(1).$$

Assim, para todo $m \in M$, temos:

$$m = \sum_{i=1}^{n} f_i(g_i(m)) = \sum_{i=1}^{n} g_i(m)f_i(1) = \sum_{i=1}^{n} g_i(m)m_i,$$

onde $m_i = f_i(1)$, para todo $i = 1, 2, \ldots, n$; ∎

Tendo em vista esses resultados, podemos provar o seguinte Teorema.

Teorema 2.44 *[26,* Proposição 1] *Sejam A um anel e R um subanel de A. Então, A é uma extensão H-separável de R se, e somente se, existem elementos $x_i \in C_A(R)$ e $y_i \in C_{A\otimes_R A}(A), 1 \leq i \leq n$, tais que $\sum_{i=1}^{n} x_i y_i = 1 \otimes 1$. O conjunto $\{x_i, y_i \mid 1 \leq i \leq n\}$ é chamado um sistema H-separável de A sobre R.*

Demonstração. Pelo Lema 2.43, A é uma extensão H-separável de R se, e somente se, existem $\varphi_i \in Hom(A \otimes_R A, {}_AA)$ e $\delta_i \in C_{A\otimes_R A}(A), i = 1, 2, \ldots, n$, tais que $\sum_{i=1}^{n} \varphi_i(x \otimes y)\delta_i = x \otimes y$, para todo $x \otimes y \in A \otimes_R A$. Em particular, $\sum_{i=1}^{n} \varphi_i(1 \otimes 1)\delta_i = 1 \otimes 1$, já que $1 \otimes 1$ gera $A \otimes_R A$ como A-bimódulos. Por outro lado, $Hom(A \otimes_R A, {}_AA_A)$ é isomorfo a $C_A(R)$ pela aplicação $\varphi \mapsto \varphi(1 \otimes 1)$, onde cada homomorfismo de A-bimódulos φ de $A \otimes_R A$ em A é dado pela multiplicação de algum $d \in C_A(R)$. Assim, φ_i e δ_i existem se, e somente se, existem $d_i \in C_A(R)$ e $\delta_i \in C_{A\otimes_R A}(A)$ tais que $\sum_{i=1}^{n} d_i\delta_i = 1 \otimes 1$, $1 \leq i \leq n$. Tomando $x_i = d_i$ e $\delta_i = y_i$, $1 \leq i \leq n$, temos o resultado desejado. ∎

Os próximos resultados relacionam as extensões H-separáveis com as álgebras de Azumaya, mostrando que todo anel que é Azumaya é também H-separável sobre seu centro.

Proposição 2.45 *Seja A uma álgebra sobre um anel comutativo R e $C(A)$ o seu centro. Então, A é uma extensão H-separável de R se, e somente se, A é separável sobre $C(A)$ e $C(A) \otimes_R C(A) \simeq C(A)$ pela aplicação φ tal que $\varphi(x \otimes y) = xy$.*

Demonstração. [24, Proposição 1.1]. ∎

Corolário 2.46 *Seja $A \supseteq R$ uma extensão de anéis com mesma unidade. A é uma extensão H-separável de $C(A)$ se, e somente se, A é uma $C(A)$-álgebra de Azumaya.*

Demonstração. Suponha que A é uma extensão H-separável de $C(A)$, então pelo Teorema 2.41, A é separável sobre $C(A)$ e assim A é uma $C(A)$-álgebra de Azumaya. Reciprocamente, suponha que A é uma $C(A)$-álgebra de Azumaya. Como A é separável sobre $C(A)$ e $C(A) \otimes_{C(A)} C(A) \simeq C(A)$, temos que A é uma extensão H-separável de $C(A)$, pela Proposição 2.45. ∎

Proposição 2.47 *Se A é uma extensão H-separável de R tal que R é um R-somando direto de A à esquerda (ou a direita), então $C_A(C_A(R)) = R$.*

Demonstração. [24, Proposição 1.2]. ∎

Proposição 2.48 *Seja A uma extensão H-separável de R tal que ${}_RR_R|{}_RA_R$. Então, $C_A(R)$ é separável sobre $C(A)$ e $C_A(C_A(R)) = R$.*

Demonstração. [25, Proposição 1.3]. ∎

Teorema 2.49 *[18,* Teorema 1] *Sejam A uma $C(A)$-álgebra de Azumaya e B um subanel de A, onde $A \supset B \supset C(A)$. Se A_B é projetivo e finitamente gerado, então A é uma extensão H-separável de B.*

Demonstração. Suponha que A é uma $C(A)$-álgebra de Azumaya, em particular, A é uma extensão separável de $C(A)$. Assim, pela Proposição 2.4 (iii), existe um elemento $\sum_i r_i \otimes s_i \in A \otimes_{C(A)} A$ tal que $\sum_i r_i s_i = 1$ e $\sum_i ar_i \otimes s_i = \sum_i r_i \otimes s_i a$, para todo $a \in A$. Além disso, como A_B é projetivo e finitamente gerado, pelo Lema da Base Dual, existe um número finito de elementos $t_j \in A$ e $f_j \in Hom(A_B, B_B)$ tal que $\sum_j t_j f_j(a) = a$, para todo $a \in A$. Considere a aplicação $\theta : A \otimes_{C(A)} A \to A \otimes_{C(A)} A$, dada por $\theta(u \otimes v) = \sum_j ut_j \otimes f_j(v)$. Temos que $\theta \in End_A(A \otimes_{C(A)} A)$. De fato, para todo $r \in C(A)$, temos:

$$\begin{aligned}
\theta(ur, v) &= \sum_j urt_j \otimes f_j(v) = \sum_j ut_j r \otimes f_j(v), \text{ pois } r \in C(A) \\
&= \sum_j ut_j \otimes rf_j(v) = \sum_j ut_j \otimes f_j(v)r, \text{ pois } f_j(v) \in B \subset A \text{ e } r \in C(A) \\
&= \sum_j ut_j \otimes f_j(vr) = \sum_j ut_j \otimes f_j(rv), \text{ pois } f \text{ é } B\text{-linear e } C(A) \subset B \\
&= \theta(u, rv).
\end{aligned}$$

Sendo assim, já que θ é $C(A)$-balanceada, pela Propriedade Universal do produto tensorial, existe uma único homomorfismo $\theta : A \otimes_{C(A)} A \to A \otimes_{C(A)} A$ tal que $\theta(u \otimes v) = \sum_j u t_j \otimes f_j(v)$. Defina agora

$$\begin{array}{rccc} \phi: & A \otimes_B A & \to & A \otimes_{C(A)} A \\ & x \otimes y & \mapsto & \sum_{i,j} r_i t_j \otimes f_j(s_i x) y \end{array}.$$

Pela Propriedade Universal do produto tensorial sobre B, garantimos a boa-definição da aplicação ϕ. Agora, vejamos que ϕ é um homomorfismo de A-bimódulos. Sejam $a, x, y \in A$. Observe que:

$$\begin{aligned} \phi(a(x \otimes y)) = \phi(ax \otimes y) &= \sum_{i,j} r_i t_j \otimes f_j(s_i a x) y \\ &= \theta\Big(\sum_i r_i \otimes s_i a x\Big) y = \theta\Big(\sum_i a r_i \otimes s_i x\Big) y, \text{ pois } \sum_i r_i \otimes s_i \in C_{A \otimes_{C(A)} A}(A) \\ &= \sum_{i,j} a r_i t_j \otimes f_j(s_i x) y = a \sum_{i,j} r_i t_j \otimes f_j(s_i x) y \\ &= a\phi(x \otimes y) \end{aligned}$$

e

$$\phi((x \otimes y)a) = \phi(x \otimes ya) = \sum_{i,j} r_i t_j \otimes f_j(s_i x) y a = \phi(x \otimes y)a.$$

Claramente, a aplicação canônica $\psi : A \otimes_{C(A)} A \to A \otimes_B A$ é um homomorfismo de A-bimódulos. Agora, observe que para todo $x \otimes y \in A \otimes_B A$, temos:

$$\begin{aligned} \psi \circ \phi(x \otimes_B y) = \psi(\phi(x \otimes_B y)) &= \psi\Big(\sum_{i,j} r_i t_j \otimes_{C(A)} f_j(s_i x) y\Big) \\ &= \sum_{i,j} r_i t_j \otimes_B f_j(s_i x) y = r_i t_j f_j(s_i x) \otimes_B y \\ &= \sum_i r_i \Big(\sum_j t_j f_j(s_i x)\Big) \otimes_B y = \sum_i r_i s_i x \otimes_B y \\ &= 1x \otimes_B y = x \otimes_B y \\ &= I_{A \otimes_B A}(x \otimes_B y). \end{aligned}$$

Logo, $\psi \circ \phi = I_{A \otimes_B A}$. Assim, temos $A \otimes_B A \xrightarrow{\phi} A \otimes_{C(A)} A \xrightarrow{\psi} A \otimes_B A$ homomorfismos de A-bimódulos tais que $\psi \circ \phi = I_{A \otimes_B A}$. Então, ϕ é um monomorfismo e ψ é um epimorfismo, pela Proposição 1.11. Logo, a sequência $0 \longrightarrow A \otimes_B A \xrightarrow{\phi} A \otimes_{C(A)} A$ é exata, já que ϕ é um monomorfismo. Como existe um homomorfismo de (A, A)-módulos ψ tal que $\psi \circ \phi = I_{A \otimes_B A}$, temos que a sequência acima cinde (Proposição 1.27). Nessas condições,

$A \otimes_{C(A)} A = Im(\phi) \oplus ker(\psi)$. Como ϕ é injetora, pelo Teorema do Homomorfismo para módulos (Teorema 1.14), $A \otimes_B A \simeq Im(\phi)$. Daí, segue que $A \otimes_B A | A \otimes_{C(A)} A$. Pelo Corolário 2.46, A é uma extensão H-separável de $C(A)$ (A é uma $C(A)$-álgebra de Azumaya), ou seja, $A \otimes_{C(A)} A | A$. Pela transitividade, segue que $A \otimes_B A | A$, mostrando que A é uma extensão H-separável de B. ■

Proposição 2.50 *Sejam A uma extensão H-separável de B e ${}_AM$ um A-módulo com unidade. Se ${}_BM$ é um gerador, então ${}_AM$ também é um gerador.*

Demonstração. [18, Lema]. ■

Proposição 2.51 *[7,* Proposição 2.1] *Seja $A \subseteq B$ uma extensão de anéis tal que B é um A-módulo projetivo à esquerda (ou à direita) e A é um somando direto de B como um A-bimódulo. São equivalentes:*

(i) B é Azumaya e $C(B) \subseteq A$;

(ii) B é uma extensão H-separável de A e A é separável sobre $C(B) \cap A$.

Demonstração. Suponha que B é Azumaya e $C(B) \subseteq A$. Observe que $B \supseteq A \supseteq C(B)$. Sendo B um A-módulo projetivo à esquerda (ou à direita), pelo Teorema 2.49, segue que B é uma extensão H-separável de A. Como A é um somando direto de B como um A-bimódulo, utilizando a Proposição 2.48, temos que $C_B(A)$ é uma extensão separável de $C(B)$ e $C_B(C_B(A)) = A$. Observe que $C(B) = C(B) \cap A$, já que $C(B) \subseteq A$. Pelo Teorema 2.29, sabemos que $C_B(C_B(A))$ é uma extensão separável de $C(B)$. Dessa forma, temos que A é uma extensão separável de $C(B) \cap A$.

Reciprocamente, suponha que B é uma extensão H-separável de A e A é separável sobre $C(B) \cap A$. Daí, B é uma extensão separável de A (Teorema 2.41). Pela transitividade da separabilidade, temos que B é uma extensão separável de $C(B) \cap A$. Como B é uma extensão H-separável de A e A é um somando direto de B como um (A, A)-bimódulo, então pela Proposição 2.48, $C_B(C_B(A)) = A$. Uma vez que $C(B) \subseteq C_B(C_B(A))$, temos que $C(B) \subseteq A$. Logo, $C(B) \cap A = C(B)$. Assim, B é uma extensão separável de $C(B)$, ou seja, B é Azumaya. ■

Capítulo 3

Ações parciais e teoria de Galois

Neste capítulo, estudaremos as ações parciais de um grupo G em uma álgebra associativa A e o seu respectivo anel de grupo skew parcial, baseado em [10]. Usando a álgebra dos multiplicadores, conseguimos condições necessárias e suficientes para que o anel de grupo skew parcial seja associativo. Por meio de [11], apresentamos a teoria de Galois parcial para anéis comutativos. Por fim, trazemos o estudo das ações parciais torcidas, com base em [12], apresentando o produto cruzado parcial correspondente e as suas principais características. O Teorema 3.18 mostra que o produto cruzado parcial por uma ação parcial torcida é associativo.

3.1 Ações parciais

Definição 3.1 *Sejam G um grupo com elemento neutro 1 e A uma K-álgebra associativa (não necessariamente unitária). Uma ação parcial α de G em A é uma coleção de ideais $D_g \subseteq A\,(g \in G)$ e isomorfismos de álgebras $\alpha_g : D_{g^{-1}} \to D_g$ tais que*

(i) $D_1 = A$ *e* α_1 *é a aplicação identidade de* A*;*

(ii) $D_{(gh)^{-1}} \supseteq \alpha_h^{-1}(D_h \cap D_{g^{-1}})$*;*

(iii) $\alpha_g \circ \alpha_h(x) = \alpha_{gh}(x)$ *para cada* $x \in \alpha_h^{-1}(D_h \cap D_{g^{-1}})$.

A ação parcial α é um par e é normalmente representada por $\alpha = (\{D_g\}_{g\in G}, \{\alpha_g\}_{g\in G})$.

Da definição acima, podemos perceber algumas propriedades das ações parciais. Inicialmente, observe que as condições (ii) e (iii) mostram que a função α_{gh} é uma extensão da função $\alpha_g \circ \alpha_h$. Além disso, $\alpha_h^{-1} = \alpha_{h^{-1}}$, para todo $h \in G$. De fato, primeiramente

observe que α_h^{-1} e $\alpha_{h^{-1}}$ têm o mesmo domínio e contradomínio. Pelas condições (i) e (iii), temos que para todo $x \in D_{h^{-1}}$, $\alpha_{h^{-1}} \circ \alpha_h(x) = \alpha_{h^{-1}h}(x) = \alpha_1(x) = x$. Analogamente, temos que $\alpha_h \circ \alpha_{h^{-1}}(x) = x$, para todo $x \in D_h = \alpha_{h^{-1}}^{-1}(D_{h^{-1}} \cap D_{h^{-1}})$.

Note que a condição (ii) da Definição 3.1 é equivalente a dizer que

$$\alpha_h^{-1}(D_h \cap D_{g^{-1}}) = D_{h^{-1}} \cap D_{(gh)^{-1}}. \tag{3.1}$$

Por definição, $\alpha_h^{-1}(D_h \cap D_{g^{-1}}) \subseteq D_{(gh)^{-1}} \cap D_{h^{-1}}$, para todo $g, h \in G$. Substituindo h por h^{-1} e g por gh, obtemos que

$$\alpha_{h^{-1}}^{-1}(D_{h^{-1}} \cap D_{(gh)^{-1}}) \subseteq D_{g^{-1}} \cap D_h. \tag{3.2}$$

Aplicando $\alpha_{h^{-1}}$ em (3.2), encontramos que

$$D_{h^{-1}} \cap D_{(gh)^{-1}} \subseteq \alpha_{h^{-1}}(D_{g^{-1}} \cap D_h).$$

Como $\alpha_{h^{-1}} = \alpha_h^{-1}$, segue que

$$D_{h^{-1}} \cap D_{(gh)^{-1}} \subseteq \alpha_h^{-1}(D_{g^{-1}} \cap D_h).$$

Portanto, temos a igualdade. Reciprocamente, se a equação (3.1) é satisfeita, é imediato que a condição (ii) da Definição 3.1 é verificada.

Diante disso, podemos reescrever as condições da Definição 3.1 da seguinte forma:

(i) $D_1 = A$ e α_1 é a aplicação identidade de A;

(ii) $\alpha_g(D_{g^{-1}} \cap D_h) = D_g \cap D_{gh}$;

(iii) $\alpha_g \circ \alpha_h(x) = \alpha_{gh}(x)$, para todo $x \in D_{h^{-1}} \cap D_{(gh)^{-1}}$.

Observação 3.2 *Se $D_g = X$, para todo $g \in G$, então $\alpha = (\{D_g\}_{g\in G}, \{\alpha_g\}_{g\in G})$ é uma ação global de G sobe X. Dessa forma, as ações globais são um caso particular das ações parciais.*

Agora, vejamos um exemplo que mostra a construção de uma ação parcial a partir de uma ação global dada.

Exemplo 3.3 *Sejam G um grupo e B uma álgebra. Suponha que existe uma ação global β de G sobre B, ou seja, existe uma aplicação $\beta : G \to Aut(B)$, dada por $\beta(g) = \beta_g$, satisfazendo que $\beta_1 = I_B$ é a identidade sobre B e que $\beta_{gh} = \beta_g \circ \beta_h$, para todo $g, h \in G$. Considere A um ideal de B. Podemos obter uma ação parcial α de G sobre A por restrição de β a A. Defina*

$$D_g = A \cap \beta_g(A), \forall g \in G.$$

Como A é um ideal de B e β_g é um isomorfismo, então $\beta_g(A)$ também é um ideal de B, logo $D_g = A \cap \beta_g(A)$ é ideal de B.
Defina agora

$$\alpha_g = \beta_g|_{D_{g^{-1}}}.$$

Veja que $\beta_g(D_{g^{-1}}) = D_g$. De fato, seja $y \in D_{g^{-1}} = A \cap \beta_{g^{-1}}(A)$, então $y \in A$ e $y = \beta_{g^{-1}}(x)$, onde $x \in A$. Logo,

$$\beta_g(y) = \beta_g(\beta_{g^{-1}}(x)) = \beta_{gg^{-1}}(x) = \beta_1(x) = x \in A \cap \beta_g(A) = D_g.$$

Assim, $\beta_g(D_{g^{-1}}) \subseteq D_g$. Agora, seja $y \in D_g$. Então, $y \in A$ e $x = \beta_g(x)$, onde $x \in A$. Assim,

$$\beta_{g^{-1}}(y) = \beta_{g^{-1}}(\beta_g(x)) = x \in \beta_{g^{-1}}(A) \cap A = D_{g^{-1}}.$$

Logo, $x \in D_{g^{-1}}$ e então

$$y = \beta_g(x) \in \beta_g(D_{g^{-1}}).$$

Assim, $D_g \subseteq \beta_g(D_{g^{-1}})$ e portanto vale a igualdade. Desta forma, as aplicações

$$\alpha_g = \beta_g|_{D_{g^{-1}}} : D_{g^{-1}} \to D_g$$

são isomorfismos de álgebras.
Agora, observe que:
(i) $D_1 = A \cap \beta_1(A) = A \cap A = A$ e $\alpha_1 = \beta_1|_A = I_A$.
(ii) $\alpha_g(D_{g^{-1}} \cap D_h) \subseteq D_g \cap D_{gh}$, para todo $g, h \in G$. Com efeito, seja $y \in \alpha_g(D_{g^{-1}} \cap D_h)$, então existe $x \in D_{g^{-1}} \cap D_h$ tal que $y = \alpha_g(x) \in D_g$. Como $x \in D_h$ e $\alpha_h : D_{h^{-1}} \to D_h$ é um isomorfismo, então existe $z \in D_{h^{-1}}$ tal que $x = \alpha_h(z)$. Assim,

$$y = \alpha_g(x) = \alpha_g(\alpha_h(z)) = \beta_g(\beta_h(z)) = \beta_{gh}(z) \in \beta_{gh}(A).$$

Ou seja, $y \in \beta_{gh}(A) \cap A = D_{gh}$. Logo, $y \in D_{gh} \cap D_g$ e com isso $\alpha_g(D_{g^{-1}} \cap D_h) \subseteq D_g \cap D_{gh}$.
(iii) $\alpha_{gh}(x) = \alpha_g \circ \alpha_h(x)$, para todo $x \in D_{h^{-1}} \cap D_{(gh)^{-1}}$. Com efeito, já que $x \in D_{h^{-1}} \cap D_{(gh)^{-1}}$ e $\alpha_g(D_{g^{-1}} \cap D_h) \subseteq D_g \cap D_{gh}$, para todo $g, h \in G$, então $\alpha_h(D_{h^{-1}} \cap D_{(gh)^{-1}}) \subseteq D_h \cap D_{g^{-1}}$ e, em particular, $\alpha_h(x) \in D_{g^{-1}}$. Assim, para todo $x \in D_{h^{-1}} \cap D_{(gh)^{-1}}$, temos que

$$\begin{aligned}\alpha_{gh}(x) &= \beta_{gh}(x) = \beta_g(\beta_h(x)) = \beta_g(\alpha_h(x)) \\ &= \alpha_g(\alpha_h(x)) = \alpha_g \circ \alpha_h(x).\end{aligned}$$

Portanto, as condições da Definição 3.1 são satisfeitas e α é uma ação parcial de G sobre A.

Definição 3.4 *Dada uma ação parcial α de um grupo G sobre uma álgebra A, o anel de grupo skew parcial $A \rtimes_\alpha G$ correspondente a α é o conjunto de todas as somas finitas $\{\sum_{g \in G} a_g \delta_g : a_g \in D_g\}$, onde δ_g são símbolos. A adição é definida de forma usual e a multiplicação é determinada por*

$$(a_g \delta_g)(b_h \delta_h) = \alpha_g(\alpha_{g^{-1}}(a_g) b_h) \delta_{gh}.$$

É imediato verificar que a aplicação $A \to A \rtimes_\alpha G$, $a \mapsto a\delta_1$, é uma imersão que nos permite identificar A com $A\delta_1$. A primeira questão que surge sobre o anel de grupo skew parcial $A \rtimes_\alpha G$ é se o mesmo é ou não associativo. Em geral, isso não ocorre. O exemplo a seguir justifica esse fato.

Exemplo 3.5 *Seja A um K-espaço vetorial de dimensão 4 com base $\{1_A, u, v, t\}$. A adição é definida de forma usual e a multiplicação sobre A é dada por:*

$$\begin{aligned} u^2 &= v^2 = uv = vu = tu = ut = t^2 = 0 \\ tv &= vt = u \\ 1_A a &= a1_A = a, \text{ para todo } a \in A. \end{aligned}$$

Então, A é uma álgebra associativa com unidade 1_A. Considere o grupo $G = \{1, g\}$, com $g^2 = 1$, e I o ideal gerado por v. Temos que $A \rtimes_\alpha G$ não é associativo.

De fato, observe que quando I é visto como um subespaço vetorial de A, temos que I é gerado por u e v, pois

$$\begin{aligned} I = \langle v \rangle &= \{xv;\ x \in A\} \\ &= \{(a1_A + bu + cv + dt)v;\ a, b, c, d \in K\} \\ &= \{av + buv + cv^2 + dtv;\ a, b, c, d \in K\} \\ &= \{av + du;\ a, d \in K\}. \end{aligned}$$

Agora, considere os ideias $D_1 = A$, $D_g = I$ e a ação parcial de α sobre A definida por $\alpha_1 = I_A$ e $\alpha_g : I \to I$, dada por $\alpha_g(au + bv) = av + bu$, para todo $a, b \in K$. Seja $A \rtimes_\alpha G$ o anel de grupo skew parcial correspondente a α. Tome $x = t\delta_1 + u\delta_g \in A \rtimes_\alpha G$. Temos que $xx = v\delta_g$, pois

$$\begin{aligned} xx = (t\delta_1 + u\delta_g)(t\delta_1 + u\delta_g) &= t\delta_1 t\delta_1 + t\delta_1 u\delta_g + u\delta_g t\delta_1 + u\delta_g u\delta_g \\ &= t^2\delta_1 + tu\delta_g + \alpha_g(\alpha_{g^{-1}}(u)t)\delta_g + \alpha_g(\alpha_{g^{-1}}(u)u)\delta_1 \\ &= \alpha_g(vt)\delta_g + \alpha_g(vu)\delta_1 \\ &= v\delta_g. \end{aligned}$$

Assim,

$$\begin{aligned} (xx)x = v\delta_g(t\delta_1 + u\delta_g) &= v\delta_g t\delta_1 + v\delta_g u\delta_g \\ &= \alpha_g(\alpha_{g^{-1}}(v)t)\delta_g + \alpha_g(\alpha_{g^{-1}}(v)u)\delta_1 \\ &= \alpha_g(ut)\delta_g + \alpha_g(u^2)\delta_1 = 0. \end{aligned}$$

Por outro lado,

$$\begin{aligned} x(xx) = (t\delta_1 + u\delta_g)(v\delta_g) &= t\delta_1 v\delta_g + u\delta_g v\delta_g \\ &= tv\delta_g + \alpha_g(\alpha_{g^{-1}}(u)v)\delta_1 \\ &= u\delta_g + \alpha_g(v^2)\delta_1 = u\delta_g. \end{aligned}$$

Logo, $(xx)x \neq x(xx)$. Portanto, $A \rtimes_\alpha G$ não é associativo.

Nas próximas seções, veremos algumas condições que tornam o anel de grupo skew parcial associativo.

3.2 Álgebra dos multiplicadores

Sejam K um corpo, A uma álgebra associativa com unidade e I um ideal de A. Tome um elemento $x \in I$ e considere as aplicações $L_x : I \to I$ e $R_x : I \to I$ definidas pela multiplicação à esquerda e à direita por x, respectivamente, ou seja,

$$L_x(a) = xa \quad \text{e} \quad R_x(a) = ax,$$

para todo $a \in I$. Então, $L = L_x$ e $R = R_x$ são transformações lineares tais que as seguintes propriedades são satisfeitas, para todo $a, b \in I$:

(i) $L(ab) = L(a)b$;

(ii) $R(ab) = aR(b)$;

(iii) $R(a)b = aL(b)$.

Definição 3.6 *A álgebra de multiplicadores de A de uma álgebra I é o conjunto $\mathcal{M}(I)$ de todos os pares ordenados (L, R), onde L e R são transformações lineares de I que satisfazem as propriedades (i)-(iii) descritas acima. Para quaisquer $\alpha \in K$ e $(L, R), (L', R') \in \mathcal{M}(I)$, as operações são dadas por*

$$\alpha(L, R) = (\alpha L, \alpha R),$$

$$(L, R) + (L', R') = (L + L', R + R'),$$

$$(L, R)(L', R') = (L \circ L', R' \circ R).$$

Dizemos que R é um multiplicador à direita e L é um multiplicador á esquerda de I.

É imediato verificar que $\mathcal{M}(I)$ é uma álgebra associativa com unidade (L_1, R_1), onde (L_1, R_1) são as aplicações identidade (que no caso de um ideal I em uma álgebra com unidade A pode ser considerada como as multiplicações pelo elemento de unidade de A à esquerda e à direita, respectivamente).

Defina a aplicação $\phi : I \to \mathcal{M}(I)$ por $\phi(x) = (L_x, R_x), x \in I$. Vejamos que ϕ é um homomorfismo de álgebras. Inicialmente, observe que para $x, y, a \in I$, temos:

$$R_{xy}(a) = a(xy) = (ax)y = (R_x(a))y = R_y(R_x(a)) = R_y \circ R_x(a)$$

e

$$L_{xy}(a) = (xy)a = x(ya) = x(L_y(a)) = L_x(L_y(a)) = L_x \circ L_y(a).$$

Portanto,

$$\phi(xy) = (L_{xy}, R_{xy}) = (L_x \circ L_y, R_y \circ R_x) = (L_x, R_x)(L_y, R_y) = \phi(x)\phi(y).$$

É imediato verificar que ϕ é K-linear e $\phi(x+y) = \phi(x) + \phi(y)$, ou seja, ϕ é um homomorfismo de K-álgebras.

Definição 3.7 *Dizemos que uma álgebra I é não-degenerada se a aplicação $\phi : I \to \mathcal{M}(I)$ definida por $\phi(x) = (L_x, R_x)$ é injetora.*

Agora, vamos estudar o $ker(\phi)$. Observe que:

$$\begin{aligned} ker(\phi) &= \{x \in I;\ \phi(x) = (0,0)\} \\ &= \{x \in I;\ (L_x, R_x) = (0,0)\} \\ &= \{x \in I;\ R_x(a) = 0 \,\text{e}\, L_x(a) = 0, \text{para todo}\, a \in I\} \\ &= \{x \in I;\ ax = 0 \,\text{e}\, xa = 0, \text{para todo}\, a \in I\}. \end{aligned}$$

Ou seja, $ker(\phi)$ é a interseção do anulador á direita com o anulador à esquerda de I. Assim, I é não-degenerada se, e somente se, para todo elemento não-nulo $a \in I$ existe $b \in I$ tal que $ab \neq 0$ ou $ba \neq 0$.

Proposição 3.8 *[10,* Proposição 2.3] *As seguintes afirmações são válidas:*

(i) $\phi(I)$ é um ideal de $\mathcal{M}(I)$;

(ii) $\phi : I \mapsto \mathcal{M}(I)$ é um isomorfismo se, e somente se, I é uma álgebra com unidade.

Demonstração.

(i) Considere $x \in I$ e seja (L, R) um elemento arbitrário de $\mathcal{M}(I)$. Então, $(L_x, R_x)(L, R) = (L_x \circ L, R \circ R_x)$. Vamos verificar que $(L_x \circ L, R \circ R_x) \in \phi(I)$. Dado $a \in I$, temos:

$$(L_x \circ L)(a) = L_x(L(a)) = x(L(a)) = (R(x))a = L_{R(x)}(a) \Rightarrow L_x \circ L = L_{R(x)},$$

onde $R(x) \in I$, para todo $a \in I$. Assim, $L_x \circ L = L_{R(x)}$, com $R(x) \in I$. Analogamente, para todo $a \in I$, temos:

$$(R \circ R_x)(a) = R(R_x(a)) = R(ax) = aR(x) = R_{R(x)}(a) \Rightarrow R \circ R_x = R_{R(x)},$$

onde $R(x) \in I$. Assim, $R \circ R_x = R_{R(x)}$, com $R(x) \in I$. Logo,

$$(L_x, R_x)(L, R) = (L_{R(x)}, R_{R(x)}) \in \phi(I).$$

De forma análoga, obtemos que $(L,R)(L_x,R_x) = (L_{L(x)}, R_{L(x)}) \in \phi(I)$. Portanto, $\phi(I)$ é um ideal de $\mathcal{M}(I)$.

(ii) $(\Rightarrow)$ Suponha que $\phi : I \to \mathcal{M}(I)$ é um isomorfismo. Denote por (L_1, R_1) a unidade de $\mathcal{M}(I)$, ou seja,

$$L_1(x) = x \quad \text{e} \quad R_1(x) = x, \text{ para todo } x \in I.$$

Como ϕ é sobrejetora, existe $e \in I$ tal que $\phi(e) = (L_1, R_1)$, assim $(L_e, R_e) = (L_1, R_1)$, ou seja, $R_e = R_1$ e $L_e = L_1$. Logo, dado $a \in I$, temos:

$$ea = L_e(a) = L_1(a) = a \quad \text{e}$$
$$ae = R_e(a) = R_1(a) = a$$

Portanto, e é a unidade da álgebra I.

$(\Leftarrow)$ Suponha que $e \in I$ é a unidade da álgebra I. Então, $\phi(e) = (L_e, R_e) \in \phi(I)$.

Afirmação 3.9 *$\phi(e) = (L_e, R_e)$ é a unidade de $\mathcal{M}(I)$. De fato, dado $a \in I$, temos que $L_e(a) = ea = a$ e $R_e(a) = ae = a$. Logo, $(L_e, R_e) = (L_1, R_1) \in \phi(I)$.*

Por (i), temos que $\phi(I)$ é um ideal de $\mathcal{M}(I)$ e como $(L_1, R_1) \in \phi(I)$, segue que $\phi(I) = \mathcal{M}(I)$, ou seja, ϕ é sobrejetora.

Para mostrar que ϕ é injetora, considere $x, y \in I$ tais que $\phi(x) = \phi(y)$, ou seja, $(L_x, R_x) = (L_y, R_y)$. Assim, $L_x(a) = L_y(a)$, $\forall a \in I$. Em particular, $L_x(e) = L_y(e)$, ou seja, $xe = ye$ e daí $x = y$.

Dessa forma, ϕ é injetora e, portanto, ϕ é um isomorfismo. ∎

Seja I uma álgebra (não necessariamente unitária). Dados $(L,R), (L',R') \in \mathcal{M}(I)$ vamos nos concentrar na validade da fórmula

$$R' \circ L = L \circ R'. \tag{3.3}$$

Se $(L,R) = (L_x, R_x)$ e $(L',R') = (L_{x'}, R_{x'})$, com $x, x' \in I$, então (3.3) vale. De fato, para todo $a \in I$, temos:

$$\begin{aligned} R' \circ L(a) &= R'(L(a)) = R'(L_x(a)) = R'(xa) = R_{x'}(xa) \\ &= (xa)x' = x(ax') = x(R_{x'}(a)) = x(R'(a)) \\ &= L_x(R'(a)) = L(R'(a)) = (L \circ R')(a). \end{aligned}$$

No entanto, nem sempre a equação (3.3) é satisfeita.

Definição 3.10 *Uma álgebra I é (L,R)-associativa se, dado quaisquer dois multiplicadores (L,R) e $(L',R') \in \mathcal{M}(I)$, vale que $R' \circ L = L \circ R'$.*

O resultado a seguir lista duas condições suficientes para a (L,R)-associatividade.

Proposição 3.11 *[10,* Proposição 2.5] *A álgebra I é (L,R)-associativa quando qualquer uma das condições a seguir é satisfeita:*

(i) I é não-degenerada, ou

(ii) I é idempotente.

Demonstração.

(i) Sejam $(L,R),(L',R') \in \mathcal{M}(I)$. Dados $a,b \in I$, temos

$$R(L'(a))b = L'(a)L(b) = L'(aL(b)) = L'(R(a)b) = L'(R(a))b.$$

Assim, $(R(L'(a)) - L'(R(a)))b = 0$. Logo $R(L'(a)) - L'(R(a))$ pertence ao anulador à esquerda de I. De forma análoga, concluímos que $R(L'(a)) - L'(R(a))$ pertence ao anulador à direita de I, então $R(L'(a)) - L'(R(a)) \in ker(\phi)$. Como I é não-degenerada, segue que $R(L'(a)) - L'(R(a)) = 0$ e daí $R((L'(a))) = L'(R(a))$, para todo $a \in I$. Portanto, $R \circ L' = L' \circ R$, mostrando que I é (L,R)-associativa.

(ii) Suponha que a álgebra I é idempotente. Sejam $(L,R),(L',R') \in \mathcal{M}(I)$. Considere $a_1, a_2 \in I$ tais que $a = a_1 a_2$. Note que:

$$\begin{aligned} R(L'(a)) &= R(L'(a_1 a_2)) = R(L'(a_1)a_2) \\ &= L'(a_1)(R(a_2)) \\ &= L'(a_1(R(a_2))) \\ &= L'(R(a_1 a_2)) \\ &= L'(R(a)). \end{aligned}$$

Como a álgebra I é idempotente, então todo elemento de I é soma de produtos $a_1 a_2$, como $a_1, a_2 \in I$. Logo,

$$R(L'(a)) = L'(R(a)), \forall a \in I.$$

Ou seja, I é (L,R)-associativa. ∎

Proposição 3.12 *[10,* Proposição 2.7] *Seja $\pi : I \to J$ um isomorfismo de K-álgebras. Então, para $(L, R) \in \mathcal{M}(I)$, o par $(\pi \circ L \circ \pi^{-1}, \pi \circ R \circ \pi^{-1})$ é um elemento em $\mathcal{M}(J)$. Além disso, a aplicação $\tilde{\pi} : \mathcal{M}(I) \to \mathcal{M}(J)$, definida por*

$$\tilde{\pi}(L, R) = (\pi \circ L \circ \pi^{-1}, \pi \circ R \circ \pi^{-1}),$$

é um isomorfismo de K-álgebras.

Demonstração. De fato, vamos denotar $\varphi = \pi \circ L \circ \pi^{-1}$ e $\psi = \pi \circ R \circ \pi^{-1}$, então, para todo $a, b \in J$, temos

$$\begin{aligned}
\varphi(ab) &= \pi(L(\pi^{-1}(ab))) = \pi(L(\pi^{-1}(a)\pi^{-1}(b))) \\
&= \pi(L(\pi^{-1}(a))\pi^{-1}(b)) \\
&= \pi(L(\pi^{-1}(a)))\pi(\pi^{-1}(b)) \\
&= \varphi(a)b.
\end{aligned}$$

Analogamente, temos que $\psi(ab) = a\psi(b)$. Além disso,

$$\begin{aligned}
\psi(a)b &= \pi(R(\pi^{-1}(a)))b = \pi(R(\pi^{-1}(a)))\pi(\pi^{-1}(b)) \\
&= \pi(R(\pi^{-1}(a))\pi^{-1}(b)) \\
&= \pi(\pi^{-1}(a)L(\pi^{-1}(b))) \\
&= \pi(\pi^{-1}(a))\pi(L(\pi^{-1}(b))) \\
&= a\varphi(b).
\end{aligned}$$

Como as condições da Definição 3.6 são satisfeitas, segue que

$$(\pi \circ L \circ \pi^{-1}, \pi \circ R \circ \pi^{-1}) \in \mathcal{J}.$$

Agora, sejam $(L, R), (L', R') \in \mathcal{M}(I)$. Veja que:

$$\tilde{\pi}((L, R)(L', R')) = \tilde{\pi}(L \circ L', R' \circ R) = (\pi \circ L \circ L' \circ \pi^{-1}, \pi \circ R' \circ R \circ \pi^{-1}).$$

Por outro lado,

$$\begin{aligned}
\tilde{\pi}(L, R)\tilde{\pi}(L', R') &= (\pi \circ L \circ \pi^{-1}, \pi \circ R \circ \pi^{-1})(\pi \circ L' \circ \pi^{-1}, \pi \circ R' \circ \pi^{-1}) \\
&= (\pi \circ L \circ (\pi^{-1} \circ \pi) \circ L' \circ \pi^{-1}, \pi \circ R' \circ (\pi^{-1} \circ \pi) \circ R \circ \pi^{-1}) \\
&= (\pi \circ L \circ L' \circ \pi^{-1}, \pi \circ R' \circ R \circ \pi^{-1}).
\end{aligned}$$

Assim, $\tilde{\pi}$ é um homomorfismo de K-álgebras.

Defina a aplicação

$$\begin{array}{rccc} \pi': & \mathcal{M}(J) & \to & \mathcal{M}(I) \\ & (L,R) & \mapsto & (\pi^{-1}\circ L\circ\pi, \pi^{-1}\circ R\circ\pi) \end{array}.$$

Agora, observe que:

$$\begin{aligned} \tilde{\pi}\circ\pi'(L,R) &= \tilde{\pi}(\pi'(L,R)) = \tilde{\pi}(\pi^{-1}\circ L\circ\pi^{-1}, \pi^{-1}\circ R\circ\pi) \\ &= (\pi\circ\pi^{-1}\circ L\circ\pi\circ\pi^{-1}, \pi\circ\pi^{-1}\circ R\circ\pi\circ\pi^{-1}) \\ &= (L,R). \end{aligned}$$

e

$$\begin{aligned} \pi'\circ\tilde{\pi}(L,R) &= \pi'(\tilde{\pi}(L,R)) \\ &= \pi'(\pi\circ L\circ\pi^{-1}, \pi\circ R\circ\pi^{-1}) \\ &= (\pi^{-1}\circ\pi\circ L\circ\pi^{-1}\circ\pi, \pi^{-1}\circ\pi\circ R\circ\pi^{-1}\circ\pi) \\ &= (L,R). \end{aligned}$$

Portanto, π' é a inversa de $\tilde{\pi}$ e com isso $\tilde{\pi}$ é um isomorfismo de K-álgebras. ∎

Agora, vamos tratar da questão da associatividade para o anel de grupo skew parcial

Teorema 3.13 *[10,* Teorema 3.1] *Se A é uma álgebra e α é uma ação parcial de um grupo G sobre A tal que cada D_g $(g\in G)$ é (L,R)-associativo, então o anel de grupo skew parcial $A\rtimes_\alpha G$ é associativo.*

Demonstração. Observe que $A\rtimes_\alpha G$ é associativo se, e somente se,

$$((a\delta_h)(b\delta_g))c\delta_f = a\delta_h((b\delta_g)(c\delta_f)) \tag{3.4}$$

para todos $h,g,f\in G$ e $a\in D_h, b\in D_g, c\in D_f$. Desenvolvendo o lado esquerdo de (3.4), temos

$$((a\delta_h)(b\delta_g))c\delta_f = \alpha_h(\alpha_{h^{-1}}(a)b)\delta_{hg}c\delta_f = \alpha_{hg}\{\alpha_{(hg)^{-1}}[\alpha_h(\alpha_{h^{-1}}(a)b)]c\}\delta_{hgf},$$

com $\alpha_{h^{-1}}(a)b\in D_{h^{-1}}\cap D_g$ e daí $\alpha_h(\alpha_{h^{-1}}(a)b)\in\alpha_h(D_{h^{-1}}\cap D_g) = D_h\cap D_{hg}$, pela condição (ii) da Definição 3.1. Então

$$\alpha_{(hg)^{-1}}[\alpha_h(\alpha_{h^{-1}}(a)b)] = \alpha_{g^{-1}}\{\alpha_{h^{-1}}[\alpha_h(\alpha_{h^{-1}}(a)b)]\} = \alpha_{g^{-1}}(\alpha_{h^{-1}}(a)b).$$

Como $\alpha_{g^{-1}}(\alpha_{h^{-1}}(a)b)\in\alpha_{g^{-1}}(D_{h^{-1}}\cap D_g) = D_{g^{-1}}\cap D_{(hg)^{-1}}$, então podemos aplicar α_{hg} e obtemos $\alpha_{hg} = (\alpha_{g^{-1}}(\alpha_{h^{-1}}(a)b)) = \alpha_h\{\alpha_g[\alpha_{g^{-1}}(\alpha_{h^{-1}}(a)b)c]\}$. Assim,

$$((a\delta_h)(b\delta_g))c\delta_f = \alpha_h\{\alpha_g[\alpha_{g^{-1}}(\alpha_{h^{-1}}(a)b)c]\}\delta_{hgf}.$$

Por outro lado,

$$a\delta_h((b\delta_g)(c\delta_f)) = a\delta_h(\alpha_g(\alpha_{g^{-1}}(b)c))\delta_{gf} = \alpha_h[\alpha_{h^{-1}}(a)\alpha_g(\alpha_{g^{-1}}(b)c)]\delta_{hgf}.$$

Aplicando $\alpha_{h^{-1}}$ na igualdade acima, temos que (3.4) é válida se, e somente se,

$$\alpha_g\{\alpha_{g^{-1}}(\alpha_{h^{-1}}(a)b)c\} = \alpha_{h^{-1}}(a)\alpha_g(\alpha_{g^{-1}}(b)c).$$

Como $\alpha_{h^{-1}} : D_h \to D_{h^{-1}}$ é um isomorfismo e $\alpha_{h^{-1}}(a) \in D_{h^{-1}}$, podemos escrever

$$\alpha_g\{\alpha_{g^{-1}}(ab)c\} = a\alpha_g(\alpha_{g^{-1}}(b)c),$$

com $a \in D_{h^{-1}}, b \in D_g, c \in D_f$ e $h, g, f \in G$. Se $h = f = 1$, então $D_h = D_f = A$ e assim $A \rtimes_\alpha G$ é associativo se, e somente se, (3.4) vale para todos $g \in G, b \in D_g$ e $a, c \in A$. Observe que:

$$\begin{aligned}\alpha_g\{\alpha_{g^{-1}}(ab)c\} &= \alpha_g(R_c(\alpha_{g^{-1}}(ab))) = \alpha_g(R_c(\alpha_{g^{-1}}(L_a(b))))\\ &= ((\alpha_g \circ R_c \circ \alpha_{g^{-1}}) \circ L_a)(b).\end{aligned}$$

Além disso, note que:

$$\begin{aligned}a\alpha_g(\alpha_{g^{-1}}(b)c) &= L_a(\alpha_g(\alpha_{g^{-1}}(b)c))L_a(\alpha_g(R_c(\alpha_{g^{-1}}(b))))\\ &= (L_a \circ (\alpha_g \circ R_c \circ \alpha_{g^{-1}}))(b).\end{aligned}$$

Assim, $A \rtimes_\alpha G$ é associativo se, e somente se,

$$(\alpha_g \circ R_c \circ \alpha_{g^{-1}}) \circ L_a = L_a \circ (\alpha_g \circ R_c \circ \alpha_{g^{-1}}) \tag{3.5}$$

é válida sobre D_g, para todo $g \in G$ e $a, c \in A$.

Considere R_c um multiplicador à direita de $D_{g^{-1}}$ e L_a um multiplicador à esquerda de D_g . Assim, pela Proposição 3.12, temos que $\alpha_g \circ R_c \circ \alpha_{g^{-1}}$ é um multiplicador à direita de D_g. Por D_g ser (L, R)-associativo, segue que (3.5) é valida e portanto $A \rtimes_\alpha G$ é associativo. ∎

Corolário 3.14 *[10,* Corolário 3.2] *Se α é uma ação parcial de um grupo G sobre uma álgebra A tal que cada $D_g\,(g \in G)$ é idempotente ou não-degenerado, então o anel de grupo skew parcial $A \rtimes_\alpha G$ é associativo.*

Demonstração. Como cada ideal $D_g\,(g \in G)$ é idempotente ou não-degenerado, pela Proposição 3.11, segue que cada $D_g\,(g \in G)$ é (L, R)-associativo. Assim, pelo Teorema 3.13, temos o resultado. ∎

3.3 Ações parciais torcidas

Sejam K um anel comutativo com unidade e A uma K-álgebra associativa (não necessariamente com unidade). Considerando um multiplicador $w = (L, R) \in \mathcal{M}(A)$ e um elemento $a \in A$, denotamos por $aw = R(a)$ e $wa = L(a)$, e dessa maneira sempre temos que $(aw)b = R(a)b = aL(b) = a(wb)$, para todo $a, b \in A$.

Definição 3.15 *Uma ação parcial torcida de um grupo G sobre A é uma tripla*

$$\alpha = (\{D_g\}_{g\in G}, \{\alpha_g\}_{g\in G}, \{w_{g,h}\}_{(g,h)\in G\times G}),$$

onde para cada $g \in G$, D_g é um ideal de A, $\alpha_g : D_{g^{-1}} \to D_g$ é um isomorfismo de K-álgebras, e para cada $(g, h) \in G \times G$, $w_{g,h}$ é um elemento invertível de $\mathcal{M}(D_g \cdot D_{gh})$, satisfazendo as seguintes condições, para todo $g, h, l \in G$:

(i) $D_g^2 = D_g$ *e* $D_g \cdot D_h = D_h \cdot D_g$;

(ii) $D_1 = A$ *e* α_1 *é a aplicação identidade* I_A *de* A;

(iii) $\alpha_g(D_{g^{-1}} \cdot D_h) = D_g \cdot D_{gh}$;

(iv) $\alpha_g \circ \alpha_h(a) = w_{g,h}\alpha_{gh}(a)w_{g,h}^{-1}, \forall a \in D_{h^{-1}} \cdot D_{h^{-1}g^{-1}}$;

(v) $w_{1,g} = w_{g,1} = I_{D_g}$;

(vi) $\alpha_g(aw_{h,t})w_{g,hl} = \alpha_g(a)w_{g,h}w_{gh,l}, \forall a \in D_{g^{-1}} \cdot D_h \cdot D_{hl}$.

Segue imediatamente do item (i) que um produto finito de ideais $D_g \cdot D_h \ldots$ é idempotente.

Pelas condições (i) e (iii), temos que

$$\alpha_g(D_{g^{-1}} \cdot D_h \cdot D_f) = D_g \cdot D_{gh} \cdot D_{gf},$$

para todo $g, h, f \in G$. De fato, por (i) e (iii), segue que:

$$\begin{aligned}
\alpha_g(D_{g^{-1}} \cdot D_h \cdot D_f) &= \alpha_g(D_{g^{-1}} \cdot D_h \cdot D_{g^{-1}} \cdot D_f) \\
&= \alpha_g(D_{g^{-1}} \cdot D_h)\alpha_g(D_{g^{-1}} \cdot D_f) \\
&= D_g \cdot D_{gh} \cdot D_g \cdot D_{gf} \\
&= D_g^2 \cdot D_{gh} \cdot D_{gf} \\
&= D_g \cdot D_{gh} \cdot D_{gf}.
\end{aligned}$$

Também segue imediatamente de (iii) que

$$\alpha_g^{-1}(D_g \cdot D_h) = D_{g^{-1}} \cdot D_{g^{-1}h}, \tag{3.6}$$

para todo $g, h \in G$. De fato, tomando $h := g^{-1}h$ em (iii), temos

$$\alpha_g(D_{g^{-1}} \cdot D_{g^{-1}h}) = D_g \cdot D_h.$$

Aplicando α_g^{-1} na igualdade acima, obtemos que

$$D_{g^{-1}} \cdot D_{g^{-1}h} = \alpha_g^{-1}(D_g \cdot D_h),$$

para todo $g, h \in G$.

Por (vi), vemos que os multiplicadores são aplicáveis.

Dada uma álgebra idempotente I, segue da Proposição 3.11 que I é (L, R)-associativa, assim

$$(wx)w' = w(xw'), \tag{3.7}$$

para todo $w, w' \in \mathcal{M}(I)$ e $x \in I$. Como os ideais D_g são idempotentes, segue que a igualdade (3.7) é válida e portanto não precisamos de parênteses no lado direito de (iv).

Definição 3.16 *Dada uma ação parcial torcida α de G sobre A, o produto cruzado parcial, denotado por $A \rtimes_{\alpha,\omega} G$, é a soma direta:*

$$\bigoplus_{g\in G} D_g\delta_g,$$

em que os δ_g's são usados simplesmente como marcadores de lugar. A adição é definida de forma usual e a multiplicação é dada pela regra:

$$(a_g\delta_g) \cdot (b_h\delta_h) = \alpha_g(\alpha_g^{-1}(a_g)b_h)w_{g,h}\delta_{gh}.$$

Nesse caso, $w_{g,h}$ age como um multiplicador à direita sobre $\alpha_g(\alpha_g^{-1}(a_g)b_h) \in \alpha_g(D_{g^{-1}} \cdot D_h) = D_g \cdot D_{gh}$.

Dado um isomorfismo $\alpha : I \to J$ e um multiplicador $u = (L, R)$ de I, temos que $u^\alpha = (\alpha L\alpha^{-1}, \alpha^{-1}R\alpha)$ é um multiplicador de J (Proposição 3.12). Observe que o efeito de $\alpha^{-1}R\alpha$ em $x \in I$ é $(\alpha^{-1}R\alpha) \cdot x = \alpha^{-1}R\alpha(x) = \alpha(R(\alpha^{-1}(x)))$, assim como $(\alpha L\alpha^{-1}) \cdot x = (\alpha L\alpha^{-1})(x) = \alpha(L(\alpha^{-1}(x)))$.

Para a demonstração da associatividade de $A \rtimes_{\alpha,\omega} G$, vamos precisar do seguinte resultado técnico.

Lema 3.17 *[12,* Lema 2.3] *Temos as duas seguintes propriedades:*

(i)

$$a\alpha_h(\alpha_h^{-1}(b)c) = \alpha_h(\alpha_h^{-1}(ab)c),$$

para quaisquer $a, c \in A, b \in D_h$ e $h \in G$.

(ii)

$$[\alpha_{gh}^{-1}(w_{g,h}\alpha_{gh}(x))]c = \alpha_{gh}^{-1}(w_{g,h}\alpha_{gh}(xc)),$$

para quaisquer $x \in D_{h^{-1}} \cdot D_{h^{-1}g^{-1}}, g, h \in G$ *e* $c \in A$.

Demonstração.

(i) Como $\alpha_h : D_{h^{-1}} \to D_h$ é um isomorfismo e (L_c, R_c) é um multiplicador de $D_{h^{-1}}$, então o par $(\alpha_h L_c \alpha_h^{-1}, \alpha_h^{-1} R_c \alpha_h)$ é um multiplicador de D_h (Proposição 3.12). Usando (3.7) para os multiplicadores $(\alpha_h L_c \alpha_h^{-1}, \alpha_h^{-1} R_c \alpha_h)$ e (L_a, R_a), temos que

$$L_a \cdot (b \cdot (\alpha_h^{-1} R_c \alpha_h)) = (L_a \cdot b) \cdot (\alpha_h^{-1} R_c \alpha_h).$$

Veja que:

$$\begin{aligned} L_a \cdot (b \cdot (\alpha_h^{-1} R_c \alpha_h)) &= (L_a \cdot b) \cdot (\alpha_h^{-1} R_c \alpha_h) \\ L_a \cdot (\alpha_h(\alpha_h^{-1}(b) \cdot R_c)) &= (ab) \cdot (\alpha_h^{-1} R_c \alpha_h) \\ L_a \cdot (\alpha_h(\alpha_h^{-1}(b)c)) &= \alpha_h(\alpha_h^{-1}(ab) \cdot R_c) \\ a\alpha_h(\alpha_h^{-1}(b)c) &= \alpha_h(\alpha_h^{-1}(ab)c). \end{aligned}$$

Logo, temos o resultado desejado.

(ii) Pelo item (iii) da Definição 3.15, sabemos que $\alpha_{gh}(D_{h^{-1}} \cdot D_{h^{-1}g^{-1}}) = D_{gh} \cdot D_g$ Assim, α_{gh} restrito a $D_{h^{-1}} \cdot D_{h^{-1}g^{-1}}$ fornece um isomorfismo $\alpha_{gh} : D_{h^{-1}} \cdot D_{h^{-1}g^{-1}} \to D_{gh} \cdot D_g$. Como $\alpha_{gh}^{-1} : D_g \cdot D_{gh} \to D_{h^{-1}} \cdot D_{h^{-1}g^{-1}}$ é um isomorfismo e $w_{g,h} \in \mathcal{M}(D_g \cdot D_{gh})$, temos que $w_{g,h}^{\alpha_{gh}^{-1}}$ é um multiplicador de $D_{h^{-1}} \cdot D_{h^{-1}g^{-1}}$. Considerando os multiplicadores $w_{g,h}^{\alpha_{gh}^{-1}}$ e (L_c, R_c), por (3.7), temos que

$$[(\alpha_{gh}^{-1} w_{g,h} \alpha_{gh}) \cdot x] \cdot R_c = (\alpha_{gh}^{-1} w_{g,h} \alpha_{gh}) \cdot [x \cdot R_c].$$

Veja que:

$$\begin{aligned} [(\alpha_{gh}^{-1} w_{g,h} \alpha_{gh}) \cdot x] \cdot R_c &= (\alpha_{gh}^{-1} w_{g,h} \alpha_{gh}) \cdot [x \cdot R_c] \\ [\alpha_{gh}^{-1}(w_{g,h}\alpha_{gh}(x))] \cdot R_c &= (\alpha_{gh}^{-1} w_{g,h} \alpha_{gh}) \cdot (xc) \\ [\alpha_{gh}^{-1}(w_{g,h}\alpha_{gh}(x))]c &= \alpha_{gh}^{-1}(w_{g,h}\alpha_{gh}(xc)). \end{aligned}$$

Logo, temos o resultado desejado. ∎

Para finalizar, vamos provar que o produto cruzado parcial por uma ação parcial torcida é sempre associativo.

Teorema 3.18 *[12,* Teorema 2.4 *]* *O produto cruzado* $A \rtimes_{\alpha,\omega} G$ *é associativo.*

Demonstração. Sabemos que $A \rtimes_{\alpha,\omega} G$ é associativo se, e somente se,

$$(a\delta_g b\delta_h)c\delta_t = a\delta_g(b\delta_h c\delta_t) \tag{3.8}$$

para arbitrários $g, h, t \in G$ e $a \in D_g, b \in D_h, c \in D_t$. Desenvolvendo o lado esquerdo da equação acima, temos

$$(a\delta_g b\delta_h)c\delta_t = \alpha_g(\alpha_g^{-1}(a)b)w_{g,h}c\delta_t = \alpha_{gh}\{\alpha_{gh}^{-1}[\alpha_g(\alpha_g^{-1}(a)b)w_{g,h}]c\}w_{gh,t}\delta_{ght}.$$

Por outro lado,

$$a\delta_g(b\delta_h c\delta_t) = a\delta_g\alpha_h(\alpha_h^{-1}(b)c)w_{h,t}\delta_{ht} = \alpha_g[\alpha_g^{-1}(a)\alpha_h(\alpha_h^{-1}(b)c)w_{h,t}]w_{g,ht}\delta_{ght}.$$

Veja que $\alpha_g^{-1}(a)\alpha_h(\alpha_h^{-1}(b)c) \in D_{g^{-1}} \cdot \alpha_h(D_{h^{-1}} \cdot D_t) = D_{g^{-1}} \cdot D_h \cdot D_{ht}$. Pela condição (vi) da Definição 3.15, segue

$$a\delta_g(b\delta_h c\delta_t) = \alpha_g[\alpha_g^{-1}(a)\alpha_h(\alpha_h^{-1}(b)c)]w_{g.h}w_{gh,t}\delta_{ght}.$$

Comparando os dois lados da equação (3.8), podemos cancelar $w_{gh,t}$ que é invertível. Além disso, para todo $g \in G, \alpha_g^{-1} : D_g \to D_{g^{-1}}$ é um isomorfismo, e podemos "identificar"a com $\alpha_g^{-1}(a)$, para todo $a \in D_{g^{-1}}$. Assim, temos que a equação (3.8) ocorre se, e somente se,

$$\alpha_{gh}\{\alpha_{gh}^{-1}[\alpha_g(ab)w_{g,h}]c\} = \alpha_g[a\alpha_h(\alpha_h^{-1}(b)c)]w_{g.h} \tag{3.9}$$

é verificada para quaisquer $g, h \in G$ e $a \in D_{g^{-1}}, b \in D_h, c \in A$ (faça $t = 1$ e podemos ver c como um elemento arbitrário em A). Aplicando o item (i) do Lema 3.17 no lado direito da equação (3.9), temos

$$\alpha_g[a\alpha_h(\alpha_h^{-1}(b)c)]w_{g.h} = \alpha_g[\alpha_h(\alpha_h^{-1}(ab)c)]w_{g,h}.$$

Agora, sendo $y = ab \in D_{g^{-1}} \cdot D_h$, precisamos mostrar que

$$\alpha_{gh}\{\alpha_{gh}^{-1}[\alpha_g(y)w_{g,h}]c\} = \alpha_g[\alpha_h(\alpha_h^{-1}(y)c)]w_{g,h} \tag{3.10}$$

é satisfeita para arbitrários $g, h \in G, y \in D_{g^{-1}} \cdot D_h, c \in A$. Escreva $x = \alpha_h^{-1}(y) \in \alpha_h^{-1}(D_{g^{-1}} \cdot D_h) = D_{h^{-1}} \cdot D_{h^{-1}g^{-1}}$. Daí, $y = \alpha_h(x)$. Então, aplicando a condição (iv) da Definição 3.15 e o item (ii) do Lema 3.17 no lado esquerdo da equação (3.10), obtemos

$$\begin{aligned}
\alpha_{gh}\{\alpha_{gh}^{-1}[\alpha_g(y)w_{g,h}]c\} &= \alpha_{gh}\{\alpha_{gh}^{-1}[\alpha_g(\alpha_h(x))w_{g,h}]c\} \\
&= \alpha_{gh}\{\alpha_{gh}^{-1}[w_{g,h}\alpha_{gh}(x)w_{g,h}^{-1}w_{g,h}]c\} \\
&= \alpha_{gh}\{\alpha_{gh}^{-1}[w_{g,h}\alpha_{gh}(x)]c\} \\
&= \alpha_{gh}\{\alpha_{gh}^{-1}[w_{g,h}\alpha_{gh}(xc)]\} \\
&= w_{g,h}\alpha_{gh}(xc).
\end{aligned}$$

Considere $z = xc$ e a equação (3.10) torna-se

$$w_{g,h}\alpha_{gh}(z) = \alpha_g[\alpha_h(z)]w_{g,h}, \tag{3.11}$$

para arbitrários $g, h \in G$ e $z \in D_{h^{-1}} \cdot D_{h^{-1}g^{-1}}$. Por fim, note que:

$$\alpha_g\alpha_h(z)w_{g,h} = w_{g,h}\alpha_{gh}(z)w_{g,h}^{-1}w_{g,h} = w_{g,h}\alpha_{gh}(z),$$

pelo item (iv) da Definição 3.15. Dessa forma, a equação (3.11) é verdadeira e, portanto, o produto cruzado parcial $A \rtimes_{\alpha,\omega} G$ é associativo. ∎

3.4 Teoria de Galois

3.4.1 Extensões de Galois para anéis comutativos

Nesta seção, vamos abordar a definição de extensão de Galois para o caso de anéis comutativos. Além desse caso, a teoria de Galois tem aplicações em outras áreas da matemática, como a teoria de Galois para anéis de divisão, ou mais geralmente, para anéis comutativos, assim como na teoria das equações diferenciais. Apresentaremos o conceito de extensão de Galois no contexto das ações parciais para anéis comutativos, definição esta que será usada como uma importante ferramenta de prova para a demonstração dos resultados principais.

No que segue R sempre denotará um anel comutativo com unidade 1 e o símbolo $\otimes$ significará $\otimes_R$.

Seja S uma R-álgebra comutativa com elemento identidade que também será denotado por 1. Dizemos que S é uma extensão de R se S é fiel como R-módulo. Logo, se S é uma extensão de R existe uma imersão natural $R \to S$ tal que $r \mapsto r \cdot 1$. Por simplicidade, identificamos R com sua imagem $R \cdot 1$ em S.

Dados uma extensão S de um anel R e G um subgrupo finito de $Aut(S)$ (todos os automorfismos de S), denotamos por $S \rtimes G$ o S-módulo livre com base $\{\delta_\sigma : \sigma \in G\}$. Sobre $S \rtimes G$ defina a multiplicação

$$\left(\sum_{\sigma\in G} a_\sigma\delta_\sigma\right)\left(\sum_{\tau\in G} b_\tau\delta_\tau\right) = \sum_{\sigma,\tau\in G} a_\sigma\sigma(b_\tau)\delta_{\sigma\tau}.$$

Esta multiplicação faz de $S \rtimes G$ um anel não comutativo (exceto se $G = \{I_S\}$) com unidade $1\delta_1 = \delta_1$ (também denotaremos o elemento neutro de G por 1). Observe que

$S \rtimes G$ é em particular um R-módulo e $S \rtimes G$ é uma R-álgebra se, e somente se, $G \subset Aut_R(S) = \{\sigma \in Aut(S) \mid \sigma(x) = x \,\text{para todo}\, x \in R\}$.

Sejam $A = Hom_R(S, S)$ e $\phi : S \rtimes G \to A$ dada por

$$\phi\Big(\sum_{\sigma\in G} a_\sigma \delta_\sigma\Big)(s) = \sum_{\sigma\in G} a_\sigma \sigma(s),$$

para qualquer $s \in S$.

Então A é uma R-álgebra com elemento identidade $1_A = I_S$. Por outro lado, A é também um S-módulo via a ação

$$(sf)(s') = sf(s') \,\text{para quaisquer}\, s, s' \in S \,\text{e}\, f \in A$$

e ϕ é um homomorfismo de S-módulos e, em particular, de R-módulos. Além disso, ϕ é um homomorfismo de anéis e se $G \subset Aut_R(S)$, então ϕ é também um homomorfismo de R-álgebras.

Considere uma mesma extensão S de R e o mesmo subgrupo finito $G \subset Aut(S)$. Denote por $\nabla(S : G)$ o S-módulo livre de base $\{\delta_\sigma \mid \sigma \in G\}$. Sobre $\nabla(S : G)$ definimos a multiplicação

$$\Big(\sum_{\sigma\in G} a_\sigma \delta_\sigma\Big)\Big(\sum_{\tau\in G} b_\tau \delta_\tau\Big) = \sum_{\sigma,\tau\in G} a_\sigma b_\tau \delta_{\sigma,\tau}\delta_\sigma,$$

onde

$$\delta_{\sigma,\tau} = \begin{cases} 1, & \text{se } \sigma = \tau \\ \\ 0, & \text{se } \sigma \neq \tau \end{cases}.$$

Esta multiplicação faz de $\nabla(S : G)$ uma S-álgebra (em particular uma R-álgebra) comutativa com elemento identidade $1 = \sum_{\sigma\in G} \delta_\sigma$. É fácil verificar que os elementos $\delta_\sigma, \sigma \in G$, são idempotentes (não nulos) que verificam $\delta_\sigma\delta_\tau = 0$ se $\sigma \neq \tau$. De fato,

$$\delta_\sigma^2 = \delta_\sigma\delta_\sigma = \delta_{\sigma,\sigma}\delta_\sigma = \delta_\sigma$$

e se $\sigma \neq \tau$, então

$$\delta_\sigma\delta_\tau = \delta_{\sigma,\tau}\delta_\sigma = 0.$$

Consequentemente, temos que $\nabla(S : G)$ é naturalmente isomorfo a S-álgebra $S \oplus \ldots \oplus S$.

Seja $\psi : S \otimes S \to \nabla(S : G)$ dada por

$$\Big(\sum_{1=1}^{n} a_i \otimes b_i\Big) = \sum_{1=1}^{n}\sum_{\sigma\in G} a_i\sigma(b_i)\delta_\sigma.$$

Considerando $S \otimes S$ como uma S-álgebra via a ação

$$s \cdot (a \otimes b) = (sa) \otimes b \,\text{para quaisquer}\, a, b, s \in S,$$

verifica-se que ψ é um homomorfismo de S-álgebras (em particular de R-álgebras).

Teorema 3.19 *Sejam S uma extensão de R e G um subgrupo finito de $Aut(S)$. Seja $S^G = \{x \in S \mid \sigma(x) = x, \text{ para todo } \sigma \in G\}$. As seguintes condições são equivalentes:*

(i) 1. *S é um R-módulo projetivo e finitamente gerado.*

2. *$\phi : S \rtimes G \to Hom_R(S, S)$ é um isomorfismo de R-álgebras.*

(ii) 1. *$S^G = R$.*

2. *$\psi : S \otimes S \to \nabla(S : G)$ é um isomorfismo de S-álgebras.*

(iii) 1. *$S^G = R$.*

2. *Existem elementos $x_1, \ldots, x_n, y_1, \ldots, y_n$ em S tais que*

$$\sum_{j=1}^{n} x_j \sigma(y_j) = \delta_{1,\sigma} = \begin{cases} 1, & \text{se } \sigma = 1 \\ 0, & \text{se } \sigma \neq 1 \end{cases}, \text{ para todo } \sigma \in G.$$

(iv) 1. *$S^G = R$.*

2. *Para cada $\sigma \neq 1$ em G e para cada ideal maximal M de S, existe $x \in S$ tal que $\sigma(x) - x \notin M$.*

(v) 1. *$S^G = R$.*

2. *para cada idempotente não nulo e em S e para cada par $\sigma \neq \tau$ em G existe $x \in S$ tal que $\sigma(x)e \neq \tau(x)e$.*

3. *S é separável sobre R.*

Demonstração. [22, Teorema 3.4]. ∎

Definição 3.20 *Sejam S uma extensão de R e $G \subset Aut(S)$ um subgrupo finito. Dizemos que S é uma extensão de Galois de R com grupo de Galois G, se satisfaz uma das condições equivalentes do Teorema 3.19.*

Corolário 3.21 *Sejam S uma extensão de R e $G \subset Aut(S)$ um subgrupo finito tal que $S^G = R$. Se S é um corpo, então S é uma extensão de Galois de R.*

Demonstração. Se S é um corpo, então a condição (iv) 2. do Teorema 3.19 é claramente satisfeita, uma vez que 0 é o único ideal maximal. ∎

3.4.2 A aplicação traço e subanéis fixos

Sejam G um grupo e S uma R-álgebra unitária. Nesta seção, vamos assumir que $\alpha = (\{S_g\}_{g\in G}, \{\alpha_g\}_{g\in G})$ é uma ação parcial de G sobre S, onde os ideais associados à ação serão denotados por S_g, salvo indicação contrária. Além disso, assumiremos que o grupo G é finito e qualquer R-álgebra S é comutativa, com unidade e fiel. Identificamos R com $R1_S$ e assim $R \subset S$. Também assumiremos que cada S_g é gerado por um elemento idempotente 1_g, ou seja, S_g é uma R-álgebra com identidade. Neste caso,

$$S_g \cap S_h = 1_g 1_h S.$$

De fato, seja $y \in S_g \cap S_h$. Então, $y = s1_g$, para algum $s \in S$. Além disso, $y = y1_h \in S_h$. Assim,

$$y = y1_h = s1_g 1_h = 1_g 1_h s \in 1_g 1_h S.$$

Logo, $S_g \cap S_h \subset 1_g 1_h S$. A outra inclusão segue do fato de S_g e S_h serem ideais de S. Portanto, temos a igualdade.

Observação 3.22 *Se cada S_g é gerado por um elemento idempotente 1_g, então a multiplicação em $S \rtimes_\alpha G$ é dada apenas por*

$$(a_g\delta_g)(b_h\delta_h) = a_g\alpha_g(b_h 1_{g^{-1}})\delta_{gh}.$$

De fato, para $a_g\delta_g, b_h\delta_h \in S \rtimes_\alpha G$, temos

$$\begin{aligned}(a_g\delta_g)(b_h\delta_h) &= \alpha_g(\alpha_{g^{-1}}(a_g)b_h)\delta_{gh} = \alpha_g(\alpha_{g^{-1}}(a_g)1_{g^{-1}}b_h)\delta_{gh}\\ &= \alpha_g(\alpha_{g^{-1}}(a_g))\alpha_g(b_h 1_{g^{-1}})\delta_{gh}\\ &= a_g\alpha_g(b_h 1_{g^{-1}})\delta_{gh}.\end{aligned}$$

O próximo resultado será usado com bastante frequência no restante do texto.

Lema 3.23 *Seja α uma ação parcial de um grupo G sobre uma R-álgebra S tal que cada R-álgebra S_g tem unidade 1_g. Então, as igualdades*

(i) $\alpha_g(1_{g^{-1}}1_h) = 1_g 1_{gh}$ *e*

(ii) $\alpha_g(\alpha_h(x1_{h^{-1}}1_{h^{-1}g^{-1}})) = \alpha_g(\alpha_h(x1_{h^{-1}})1_{g^{-1}}) = \alpha_{gh}(x1_{h^{-1}g^{-1}})1_g,$

valem para todo $g, h \in G$ e $x \in S$.

Demonstração.

(i) Como α é uma ação parcial de G sobre S, temos que $\alpha_g(S_{g^{-1}} \cap S_h) = S_g \cap S_{gh}$. Além disso, sendo α_g um isomorfismo de R-álgebras, para cada $g \in G$, segue que cada α_g preserva unidade, ou seja, $\alpha_g(1_{g^{-1}}1_h) = 1_g 1_{gh}$.
(ii) Usando o item (i), temos

$$\begin{aligned}\alpha_g(\alpha_h(x1_{h^{-1}}1_{h^{-1}g^{-1}})) &= \alpha_g(\alpha_h(x1_{h^{-1}}1_{h^{-1}}1_{h^{-1}g^{-1}}))\\ &= \alpha_g(\alpha_h(x1_{h^{-1}})\alpha_h(1_{h^{-1}}1_{h^{-1}g^{-1}}))\\ &= \alpha_g(\alpha_h(x1_{h^{-1}})1_h 1_{g^{-1}})\\ &= \alpha_g(\alpha_h(x1_{h^{-1}})1_{g^{-1}}).\end{aligned}$$

Por outro lado, já que $x1_{h^{-1}}1_{h^{-1}g^{-1}} \in S_{h^{-1}} \cap S_{h^{-1}g^{-1}} = \alpha_h(S_{h^{-1}} \cap S_{g^{-1}})$, usando novamente (i), temos que

$$\begin{aligned}\alpha_g(\alpha_h(x1_{h^{-1}}1_{h^{-1}g^{-1}})) &= \alpha_{gh}(x1_{h^{-1}}1_{h^{-1}g^{-1}})\\ &= \alpha_{gh}(x1_{h^{-1}}1_{h^{-1}g^{-1}}1_{h^{-1}g^{-1}})\\ &= \alpha_{gh}(x1_{h^{-1}g^{-1}})\alpha_{gh}(1_{h^{-1}}1_{h^{-1}g^{-1}})\\ &= \alpha_{gh}(x1_{h^{-1}g^{-1}})1_{gh}1_g\\ &= \alpha_{gh}(x1_{h^{-1}g^{-1}})1_g.\end{aligned}$$

■

O subanel dos invariantes de S segundo α é definido por

$$S^\alpha = \{x \in S \mid \alpha_g(x1_{g^{-1}}) = x1_g, \text{ para todo } g \in G\}.$$

Note que $x \in S^\alpha$ é equivalente a $\alpha_g(xa) = x\alpha_g(a)$, para todo $a \in S_{g^{-1}}, g \in G$. De fato, se $x \in S^\alpha$ e $a \in S_{g^{-1}}$, então

$$\alpha_g(xa) = \alpha_g(x1_{g^{-1}}a) = \alpha_g(x1_{g^{-1}})\alpha_g(a) = x1_g\alpha_g(a) = x\alpha_g(a).$$

Por outro lado, se $x \in S$ é tal que $\alpha_g(xa) = x\alpha_g(a)$, para todo $a \in S_{g^{-1}}, g \in G$, temos, em particular, que a igualdade vale para $a = 1_{g^{-1}} \in S_{g^{-1}}$. Assim, $\alpha_g(x1_{g^{-1}}) = x\alpha_g(1_{g^{-1}})$. Como para cada $g \in G, \alpha_g : S_{g^{-1}} \to S_g$ é um isomorfismo, segue que $\alpha_g(x1_{g^{-1}}) = x1_g$. Assim, $\alpha_g(x1_{g^{-1}}) = x1_g$ e portanto $x \in S^\alpha$.

Observação 3.24 *Como para cada $g \in G$, α_g é R-linear, ou seja, $\alpha_g(ra) = r\alpha_g(a)$, para quaisquer $r \in R, a \in S_{g^{-1}}$, então $R \subset S^\alpha$.*

A aplicação traço desempenha um papel importante quando se tem ações de grupos finitos em álgebras. No nosso caso, definimos

$$\begin{array}{rccc} tr_{S/R}: & S & \to & S^{\alpha} \\ & x & \mapsto & \sum_{g\in G}\alpha_g(x1_{g^{-1}}) \end{array}.$$

Vejamos que $tr_{S/R}$ está bem-definida, ou seja, $tr_{S/R}(x) \in S^{\alpha}$. De fato, como $tr_{S/R}(x) \in S$ é suficiente verificar que para cada $h \in G$, $\alpha_h(tr_{S/R}1_{h^{-1}}) = tr_{S/R}1_h$. Observe que:

$$\begin{aligned} \alpha_h(tr_{S/R}(x)1_{h^{-1}}) &= \alpha_h\left(\sum_{g\in G}\alpha_g(x1_{g^{-1}})1_{h^{-1}}\right) = \sum_{g\in G}\alpha_h(\alpha_g(x1_{g^{-1}})1_{h^{-1}}) \\ &= \sum_{g\in G}\alpha_{gh}(x1_{g^{-1}h^{-1}})1_h \\ &= tr_{S/R}(x)1_h, \end{aligned}$$

onde a terceira igualdade segue do Lema 3.23.

Observe que $tr_{S/R} : S \to S^{\alpha}$ é uma aplicação R-linear à esquerda e à direita, visto que α_g é R-linear, para todo $g \in G$.

3.4.3 Extensões de Galois Parciais

Nesta seção, vamos supor que o grupo G é finito e $\alpha = (\{S_g\}_{g\in G}, \{\alpha_g\}_{g\in G})$ é uma ação parcial de G sobre S. Vale salientar que as seguintes definições não precisam da comutatividade dos anéis em questão, mas, nesse caso, estamos trabalhando com anéis comutativos.

Definição 3.25 *Uma R-álgebra S é dita uma extensão de Galois parcial de R com ação parcial α (uma extensão de Galois α-parcial, abreviado) se $S^{\alpha} = R$ e existem $x_i, y_i \in S, 1 \leq i \leq n$, satisfazendo*

$$\sum_{i=1}^{n} x_i\alpha_g(y_i1_{g^{-1}}) = \delta_{1,g} = \begin{cases} 1_S, & se \quad g = 1 \\ 0, & se \quad g \neq 1 \end{cases}.$$

Os elementos x_i, y_i são chamados de coordenadas de Galois parciais de S.

Considere a aplicação natural $j : S \rtimes_{\alpha} G \to End_R(S)$ definida por

$$j\left(\sum_{g\in G} a_g\delta_g\right)(x) = \sum_{g\in G} a_g\alpha_g(x1_{g^{-1}}), \text{ para todo } x \in S.$$

Observe que estamos identificando S com $S\delta_1$ em $S \rtimes_{\alpha} G$.

Lema 3.26 *Temos que:*

(i) j é um homomorfismo de S-módulos á esquerda.

(ii) j é um homomorfismo de R-álgebras.

Demonstração.

(i) Sejam $s, x \in S$ e $\sum_{g\in G} a_g\delta_g \in S \rtimes_\alpha G$. Veja que:

$$\begin{aligned} j\left(s\sum_{g\in G} a_g\delta_g\right)(x) &= j\left(\sum_{g\in G} sa_g\delta_g\right)(x) \\ &= \sum_{g\in G} sa_g\alpha_g(x1_{g^{-1}}) \\ &= s\sum_{g\in G} a_g\alpha_g(x1_{g^{-1}}) \\ &= \left[sj\left(\sum_{g\in G} a_g\delta_g\right)\right](x). \end{aligned}$$

É imediato verificar que $j(a_g\delta_g+b_g\delta_g)(x) = j(a_g\delta_g)+j(b_g\delta_g)$. Assim, j é um homomorfismo de S-módulos à esquerda.

(ii) Para quaisquer $g, h \in G$ e $x \in S$, temos

$$j((a_g\delta_g)(b_h\delta_h))(x) = j(a_g\alpha_g(b_h1_{g^{-1}})\delta_{gh})(x) = a_g\alpha_g(b_h1_{g^{-1}})\alpha_{gh}(x1_{h^{-1}g^{-1}}).$$

Por outro lado,

$$\begin{aligned} j(a_g\delta_g)j(b_h\delta_h)(x) &= j(a_g\delta_g)(b_h\alpha_h(x1_{h^{-1}}))(x) \\ &= a_g\alpha_g(b_h\alpha_h(x1_{h^{-1}})1_{g^{-1}}) \\ &= a_g\alpha_g(b_h1_{g^{-1}})\alpha_g(\alpha_h(x1_{h^{-1}})1_{g^{-1}}) \\ &= a_g\alpha_g(b_h1_{g^{-1}})\alpha_{gh}(x1_{h^{-1}g^{-1}})1_g \\ &= a_g\alpha_g(b_h1_{g^{-1}})\alpha_{gh}(x1_{h^{-1}g^{-1}}). \end{aligned}$$

Portanto $j((a_g\delta_g)(b_h\delta_h))(x) = j(a_g\delta_g)j(b_h\delta_h)(x)$, para todo $x \in S$, mostrando que j é um homomorfismo de R-álgebras.

■

Seja M um $S \rtimes_\alpha G$-módulo. Defina

$$M^G = \{m \in M \mid (1_g\delta_g)m = 1_gm, \text{ para todo } g \in G\}$$

o R-submódulo formado pelos elementos de M invariantes por α. Note que M também pode ser visto como um S-módulo à esquerda através da imersão $x \mapsto x\delta_1$, já que $S \subset S \rtimes_\alpha G$.

A álgebra S pode ser considerada como um $S \rtimes_\alpha G$ módulo via a aplicação j, ou seja:

$$(a_g\delta_g)x = j(a_g\delta_g)(x) = a_g\alpha_g(x1_{g^{-1}}),$$

para todo $x \in S$ e $g \in G$. Então, o subanel de invariantes como definido acima é

$$\begin{aligned} S^G &= \{x \in S \mid (1_g\delta_g)x = 1_g x, \text{ para todo } g \in G\}\} \\ &= \{x \in S \mid 1_g\alpha_g(x1_{g^{-1}}) = 1_g x, \text{ para todo } g \in G\} \\ &= \{x \in S \mid \alpha_g(x1_{g^{-1}}) = 1_g x, \text{ para todo } g \in G\}. \end{aligned}$$

Ou seja, S^G coincide com a definição de S^α.

Agora, vejamos o resultado principal dessa seção.

Teorema 3.27 *Seja α uma ação parcial de um grupo G (finito) sobre uma R-álgebra S. Então, as seguintes afirmações são equivalentes:*

(i) S é uma extensão de Galois α-parcial de R.

(ii) S é um R-módulo projetivo e finitamente gerado e $j : S \rtimes_\alpha G \to End_R(S)$ é um isomorfismo de S-módulos à esquerda e R-álgebras.

(iii) $S^\alpha = R$, S é um R-módulo projetivo e finitamente gerado e para todo $S \rtimes_\alpha G$-módulo à esquerda a aplicação $\mu : S \otimes M^G \to M$, dada por $\mu(x \otimes m) = xm$, é um isomorfismo de S-módulos à esquerda.

(iv) $S^\alpha = R$, S é um R-módulo projetivo e finitamente gerado e a aplicação $\psi : S \otimes S \to \prod_{g\in G} S_g$, dada por $\psi(x \otimes y) = (x\alpha_g(y1_{g^{-1}}))_{g\in G}$, é um isomorfismo de S-módulos à esquerda.

Demonstração.

$(i) \Rightarrow (ii)$ Suponha que S é uma extensão α-parcial de Galois de R. Então, $S^\alpha = R$ e existem elementos $x_i, y_i \in S, 1 \leq i \leq n$, satisfazendo $\sum_{i=1}^n x_i\alpha_g(y_i1_{g^{-1}}) = \delta_{1,g}$. Para cada $i \in \{1, 2, \ldots, n\}$, defina $f_i \in Hom_R(S, R)$ por

$$f_i(x) = tr_{S/R}(y_i x) = \sum_{g\in G} \alpha_g(y_i x 1_{g^{-1}}), \forall x \in S.$$

Vamos mostrar que $\{x_i, f_i\}$ é uma base dual para S como R-módulo. De fato, dado $x \in S$, temos

$$\begin{aligned}\sum_{i=1}^{n} f_i(x)x_i &= \sum_{i=1}^{n} tr_{S/R}(y_i x)x_i = \sum_{i=1}^{n}\sum_{g\in G} \alpha_g(y_i x 1_{g^{-1}})x_i \\ &= \sum_{i=1}^{n}\sum_{g\in G} \alpha_g(y_i 1_{g^{-1}})\alpha_g(x1_{g^{-1}})x_i = \sum_{g\in G} \alpha_g(x1_{g^{-1}})\left[\sum_{i=1}^{n} \alpha_g(y_i 1_{g^{-1}})x_i\right] \\ &= \sum_{g\in G} \alpha_g(x1_{g^{-1}})\delta_{1,g} = \alpha_1(x1_S) = x.\end{aligned}$$

Portanto, pelo Lema da Base Dual (Teorema 1.42), S é um R-módulo projetivo e finitamente gerado. Agora, mostraremos que a aplicação j é um isomorfismo de R-álgebras. Pelo Lema 3.26, resta mostrar que j é injetora e sobrejetora. Dado $h \in End_R(S)$, considere

$$w = \sum_{g\in G}\sum_{i=1}^{n} h(x_i)\alpha_g(y_i 1_{g^{-1}})\delta_g \in S \rtimes_\alpha G.$$

Assim, para todo $x \in S$, temos

$$\begin{aligned}j(w)(x) &= \sum_{g\in G}\sum_{i=1}^{n} h(x_i)\alpha_g(y_i 1_{g^{-1}})\alpha_g(x1_{g^{-1}}) = \sum_{g\in G}\sum_{i=1}^{n} h(x_i)\alpha_g(y_i 1_{g^{-1}}x) \\ &= \sum_{i=1}^{n} h(x_i)\left[\sum_{g\in G} \alpha_g(y_i x 1_{g^{-1}})\right] = \sum_{i=1}^{n} h(x_i)f_i(x) \\ &= \sum_{i=1}^{n} h(x_i f_i(x)) = h\left(\sum_{i=1}^{n} x_i f_i(x)\right) = h(x).\end{aligned}$$

Logo, $j(w) = h$ e portanto j é sobrejetora. Finalmente, suponha que $v = \sum_{g\in G} a_g\delta_g \in ker(j)$. Então, $j(v)(x_i) = 0$, para todo $1 \leq i \leq n$. Observe que:

$$\begin{aligned}0 &= \sum_{h\in G}\sum_{i=1}^{n} j(v)(x_i)\alpha_h(y_i 1_{h^{-1}})\delta_h = \sum_{h\in G}\sum_{i=1}^{n}\sum_{g\in G} a_g\alpha_g(x_i 1_{g^{-1}})\alpha_h(y_i 1_{h^{-1}})\delta_h \\ &= \sum_{h\in G}\sum_{g\in G} a_g\left[\sum_{i=1}^{n} \alpha_g(x_i 1_{g^{-1}})1_g\alpha_h(y_i 1_{h^{-1}})\right]\delta_h \\ &= \sum_{h\in G}\sum_{g\in G} a_g\left[\sum_{i=1}^{n} \alpha_g(x_i 1_{g^{-1}})\alpha_g(\alpha_{g^{-1}}(1_g\alpha_h(y_i 1_{h^{-1}})1_g)\right]\delta_h \\ &= \sum_{h\in G}\sum_{g\in G} a_g\left[\sum_{i=1}^{n} \alpha_g(x_i\alpha_{g^{-1}}(\alpha_h(y_i 1_{h^{-1}})1_g))\right]\delta_h\end{aligned}$$

$$
\begin{aligned}
&= \sum_{h\in G}\sum_{g\in G} a_g\left[\sum_{i=1}^{n}\alpha_g(x_i\alpha_{g^{-1}h}(y_i 1_{h^{-1}g})1_{g^{-1}})\right]\delta_h, \text{ pelo Lema } 3.23\\
&= \sum_{h\in G}\sum_{g\in G} a_g\alpha_g(\delta_{1,g^{-1}h}1_{g^{-1}})\delta_h\\
&= \sum_{h\in G}\sum_{g\in G} a_g\alpha_g(\delta_{h,g}1_{g^{-1}})\delta_h\\
&= \sum_{h\in G} a_h\alpha_h(1_{h^{-1}})\delta_h\\
&= \sum_{h\in G} a_h 1_h\delta_h\\
&= \sum_{h\in G} a_h\delta_h = v.
\end{aligned}
$$

Logo, $v = 0$ e com isso concluímos que j é injetora, o que mostra que j é de fato um isomorfismo.

$(ii) \Rightarrow (iii)$ Como S é um R-módulo projetivo e finitamente gerado, pelo Lema da base dual, existem $x_i \in S$ e $f_i \in Hom_R(S,R)$, $1 \leq i \leq l$, tais que

$$x = \sum_{i=1}^{l} f_i(x)x_i, \text{ para todo } x \in S.$$

Já que j é sobrejetora e $f_i \in Hom_R(S,R) \subset End_R(S)$, existem $v_i \in S \rtimes_\alpha G$, $1 \leq i \leq l$, tais que

$$j(v_i) = f_i.$$

Então

$$
\begin{aligned}
j((1_g\delta_g)v_i)(x) &= j(1_g\delta_g)j(v_i)(x) = j(1_g\delta_g)(f_i(x))\\
&= 1_g\alpha_g(f_i(x)1_{g^{-1}})\\
&= 1_g f_i(x)1_g, \text{ pois } f_i(x) \in R \subset S^\alpha\\
&= 1_g f_i(x)\\
&= 1_g j(v_i)(x)\\
&= j(1_g v_i)(x), \text{ para todo } x \in S.
\end{aligned}
$$

Assim, $j((1_g\delta_g)v_i)(x) = j(1_g v_i)$. Como j é injetora, segue que

$$1_g\delta_g v_i = 1_g v_i = (1_g\delta_1)(v_i), \tag{3.12}$$

para todo $g \in G$. Suponha que M é um $S \rtimes_\alpha G$-módulo à esquerda, em particular, vale a associatividade dos escalares. Daí, para $m \in M$, temos por (3.12) que

$$(1_g\delta_g)(v_i m) = [(1_g\delta_g)]v_i m = (1_g v_i)m = 1_g(v_i m).$$

Ou seja, $v_i \in M^G$, para todo $1 \leq i \leq l$.

Defina

$$\begin{array}{rccc} \nu: & M & \to & S \otimes M^G \\ & m & \mapsto & \sum_{i=1}^{l} x_i \otimes v_i m \end{array}.$$

Observe que

$$j\left(\sum_{i=1}^{l} x_i v_i\right)(x) = \sum_{i=1}^{l} x_i j(v_i)(x) = \sum_{i=1}^{l} x_i f_i(x) = x,$$

para todo $x \in S$. Além disso, $j(1\delta_1)(x) = x$, para todo $x \in S$. Novamente, como j é injetora, devemos ter

$$\sum_{i=1}^{l} x_i v_i = 1\delta_1 \in S \rtimes_\alpha G. \tag{3.13}$$

Observe também que para todo $x \in S, v = \sum_{g\in G} b_g\delta_g \in S \rtimes_\alpha G$ e $m \in M^G$, temos

$$\begin{aligned} v(xm) = (vx)m &= \left(\sum_{g\in G}(b_g\delta_g)(x\delta_1)\right)m \\ &= \left(\sum_{g\in G} b_g\alpha_g(x1_{g^{-1}})\delta_g\right)m = \left(\sum_{g\in G}(b_g\alpha_g(x1_{g^{-1}})\delta_1)(1_g\delta_g)\right)m \\ &= \sum_{g\in G}(b_g\alpha_g(x1_{g^{-1}})\delta_1)((1_g\delta_g)m) = \sum_{g\in G}(b_g\alpha_g(x1_{g^{-1}})\delta_1)(1_g m) \\ &= \left(\sum_{g\in G}(b_g\alpha_g(x1_{g^{-1}})\delta_1)(1_g\delta_1)\right)m = \left(\sum_{g\in G} b_g\alpha_g(x1_{g^{-1}})\delta_1\right)m \\ &= j(v)(x)m. \end{aligned}$$

Nessas condições,

$$v(xm) = j(v)(x)m. \tag{3.14}$$

Vejamos que ν é a inversa de μ. Inicialmente, note que para todo $m \in M$, pela equação (3.13), temos:

$$(\mu \circ \nu)(m) = \mu\left(\sum_{i=1}^{l} x_i \otimes v_i m\right) = \sum_{i=1}^{l} x_i(v_i m) = \left(\sum_{i=1}^{l} x_i v_i\right)m = (1\delta_1)m = m = I_M(m).$$

Por outro lado, para todo $x \in S$ e $m \in M^G$, pela equação (3.14), temos

$$\begin{aligned} (\nu \circ \mu)(x \otimes m) &= \nu(\mu(x \otimes m)) = \nu(xm) \\ &= \sum_{i=1}^{l} x_i \otimes v_i(xm) = \sum_{i=1}^{l} x_i \otimes j(v_i)(x)m \\ &= \sum_{i=1}^{l} x_i \otimes f_i(x)m = \left(\sum_{i=1}^{l} x_i f_i(x)\right) \otimes m \\ &= x \otimes m = I_{S\otimes M^G}(x \otimes m). \end{aligned}$$

Assim, ν é a inversa de μ e portanto μ é um isomorfismo de S-módulos à esquerda. Resta mostrar apenas que $S^\alpha = R$. Pela Observação 3.24, a inclusão $R \subset S^\alpha$ ocorre. Seja $x \in S^\alpha = \{x \in S \mid \alpha_g(x1_{g^{-1}}) = x1_g, \text{ para todo } g \in G\}$. Note que $x \in C(S \rtimes_\alpha G)$. De fato, seja $a = \sum_{g\in G} a_g\delta_g \in S \rtimes_\alpha G$, então

$$\begin{aligned} xa &= (x\delta_1)\left(\sum_{g\in G} a_g\delta_g\right) = \sum_{g\in G} xa_g\delta_g \\ &= \sum_{g\in G} a_g x\delta_g = \sum_{g\in G} a_g 1_g x\delta_g \\ &= \sum_{g\in G} a_g\alpha_g(x1_{g^{-1}})\delta_g = \left(\sum_{g\in G} a_g\delta_g\right)(x\delta_1) \\ &= ax. \end{aligned}$$

Como j é um isomorfismo de R-álgebras, então j preserva elementos do centro, logo $j(x) \in C(End_R(S))$. Já que S é um R-módulo projetivo, finitamente gerado e fiel, temos que S é um R-progerador e portanto, pela Proposição 2.27, segue que $End_R(S)$ é central, ou seja, $C(End_R(S)) = R$. Logo, $j(x) \in R$. Isso significa que

$$j(x\delta_1)(s) = xs \in R, \text{ para todo } s \in S.$$

Em particular, para $s = 1_S$, temos

$$x = x1_S \in R.$$

Daí, $S^\alpha \subset R$ e assim $S^\alpha = R$.

$(iii) \Rightarrow (iv)$ Seja $\mathcal{F} = \{f : G \to S \mid f(g) \in S_g, \text{ para todo } g \in G\}$. Claramente, a aplicação

$$\begin{array}{rccc} \gamma: & \mathcal{F} & \to & \prod_{g\in G} S_g \\ & f & \mapsto & (f(g))_{g\in G} \end{array}$$

é um isomorfismo de S-módulos à esquerda. Além disso, observe que $\mathcal{F}$ tem estrutura de $S \rtimes_\alpha G$-módulo á esquerda dada por

$$[(a_g\delta_g f)](h) = a_g\alpha_g(f(g^{-1}h)1_{g^{-1}}),$$

para todo $f \in \mathcal{F}$ e $g, h \in G$. Por (iii), sabemos que a aplicação $\mu : S \otimes \mathcal{F}^G \to M$ é um isomorfismo de S-módulos á esquerda. Assim, $\overline{\mu} : S \otimes \mathcal{F}^G \to \prod_{g\in G} S_g$, definida por $\overline{\mu}(x \otimes f) = \gamma \circ \mu(x \otimes f) = (xf(g))_{g\in G}$, para todo $x \in S$ e $f \in \mathcal{F}$, é um isomorfismo de S-módulos à esquerda.

Considere agora a aplicação

$$\begin{array}{rccc} \varphi: & S & \to & \mathcal{F}^G \\ & x & \mapsto & f_x \end{array},$$

onde $f_x : G \to S$ é definida por

$$f_x(g) = \alpha_g(x1_{g^{-1}}), \text{ para todo } g \in G.$$

Vamos mostrar que φ está bem-definida, ou seja, $f_x \in \mathcal{F}^G$, onde $\mathcal{F}^G = \{f \in \mathcal{F} \mid (1_g\delta_g)f = 1_g f, \text{ para todo } g \in G\}$. De fato, para todo $h \in G$, pelo Lema 3.23, temos

$$\begin{aligned}[(1_g\delta_g)f_x](h) &= 1_g\alpha_g(f_x(g^{-1}h)1_{g^{-1}}) = \alpha_g(\alpha_{g^{-1}h}(x1_{h^{-1}g})1_{g^{-1}}) \\ &= \alpha_h(x1_{h^{-1}})1_g = f_x(h)1_g.\end{aligned}$$

Daí, $f_x \in \mathcal{F}^G$ e a aplicação está bem-definida. Ademais, a recíproca é também verdadeira: se $f \in \mathcal{F}^G$, temos

$$[(1_g\delta_g)f](h) = \alpha_g(f(h^{-1}g)1_{g^{-1}}) = 1_g f(h),$$

para todo $g, h \in G$. Em particular, tomando $h = g$, obtemos

$$\alpha_g(f(1)1_{g^{-1}}) = 1_g f(g) = f(g).$$

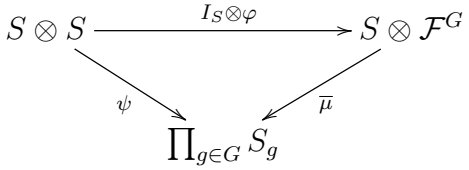
Denotando $x = f(1)$, temos

$$f(g) = \alpha_g(x1_{g^{-1}}) = f_x(g), \text{ para todo } g \in G,$$

ou seja, $f = f_x$, com $x = f(1)$. Assim, f é unicamente determinada por $f(1)$. Com isso, concluímos que a aplicação $\varphi : S \to \mathcal{F}^G$ é um isomorfismo de R-módulos á esquerda com inversa dada por

$$\begin{array}{rccc} \varphi^{-1}: & \mathcal{F}^G & \to & S \\ & f & \mapsto & f(1) \end{array}.$$

Logo, temos o seguinte diagrama:



Vejamos que o diagrama acima é comutativo. Para $x \otimes y \in S \otimes S$, temos

$$\begin{aligned}\overline{\mu} \circ (I_S \otimes \varphi)(x \otimes y) &= \overline{\mu}(x \otimes \varphi(y)) = \overline{\mu}(x \otimes f_y) \\ &= (xf_y(g))_{g\in G} = (x\alpha_g(y1_{g^{-1}}))_{g\in G} \\ &= \psi(x \otimes y).\end{aligned}$$

Portanto, ψ é um isomorfismo de S-módulos á esquerda.

$(iv) \Rightarrow (i)$ Por hipótese, temos que $S^\alpha = R$. Então, só resta mostrar que existem as coordenadas de Galois parciais. Para a segunda parte de (i), considere $(1_R, 0, \ldots, 0) \in \prod_{g\in G} S_g$, onde a primeira parte é correspondente ao elemento $g = 1$ em G. Como ψ é um isomorfismo, existe $w = \sum_{i=1}^n x_i \otimes y_i \in S \otimes S$ tal que $\psi(w) = (1_R, 0, \ldots, 0)$. Assim,

$$\psi(w) = \psi\left(\sum_{i=1}^n x_i \otimes y_i\right) = \left(\sum_{i=1}^n x_i\alpha_g(y_i 1_{g^{-1}})\right)_{g\in G} = (1_R, 0, \ldots, 0),$$

ou seja,

$$\left(\sum_{i=1}^n x_i\alpha_g(y_i 1_{g^{-1}})\right)_{g\in G} = \delta_{1,g}.$$

Logo, x_i, y_i são as coordenadas de Galois parciais de S. Portanto, o teorema está provado.

■

Teorema 3.28 *[11,* Teorema 4.2] *Seja α uma ação parcial de G sobre uma R-álgebra S. Se S é uma extensão de Galois α-parcial de R, então S é separável sobre R.*

Demonstração. Suponha que S é uma extensão de Galois α-parcial de R, ou seja, $S^\alpha = R$ e existem elementos $x_i, y_i \in S, 1 \leq i \leq n$, tais que $\sum_{i=1}^n x_i\alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g}$, para todo $g \in G$. Vamos mostrar que o elemento $e = \sum_{i=1}^n x_i \otimes y_i \in S \otimes S$ é o idempotente de separabilidade de S. Inicialmente, observe que

$$m_S(e) = m_S\left(\sum_{i=1}^n x_i\alpha_g(y_i 1_{g^{-1}})\right) = \sum_{i=1}^n x_i y_i = 1_S.$$

Além disso, para todo $x \in S$, temos

$$\begin{aligned}
\sum_{i=1}^n xx_i \otimes y_i &= \sum_{i=1}^n \left(\sum_{g\in G} \alpha_g(xx_i 1_{g^{-1}})\delta_{1,g}\right) \otimes y_i = \sum_{i=1}^n \left(\sum_{g\in G} \alpha_g(xx_i 1_{g^{-1}}) \sum_{j=1}^n x_j\alpha_g(y_j 1_{g^{-1}})\right) \otimes y_i \\
&= \sum_{i,j=1}^n \left(\sum_{g\in G} \alpha_g(xx_i y_j 1_{g^{-1}})\right) x_j \otimes y_i = \sum_{i,j=1}^n x_j tr_{S/R}(xx_i y_j) \otimes y_i \\
&= \sum_{i,j=1}^n x_j \otimes tr_{S/R}(xx_i y_j) y_i, \text{ pois } tr_{S/R}(xx_i y_j) \in S^\alpha = R \\
&= \sum_{j=1}^n x_j \otimes \sum_{i=1}^n \sum_{g\in G} \alpha_g(xx_i y_j 1_{g^{-1}}) 1_g y_i \\
&= \sum_{j=1}^n x_j \otimes \sum_{i=1}^n \sum_{g\in G} \alpha_g(xx_i y_j 1_{g^{-1}}) \alpha_{g^{-1}}(y_i 1_g) \\
&= \sum_{j=1}^n x_j \otimes \sum_{g\in G} \alpha_g\left(\sum_{i=1}^n x_i\alpha_{g^{-1}}(y_i 1_g) y_j x 1_{g^{-1}}\right) \\
&= \sum_{j=1}^n x_j \otimes \sum_{g\in G} \alpha_g(\delta_{1,g} y_j x 1_{g^{-1}}) = \sum_{j=1}^n x_j \otimes y_j x.
\end{aligned}$$

Logo, $e \in C_{S\otimes S}(S)$. Assim, e é o idempotente de separabilidade de S e portanto S é separável sobre R, pela Proposição 2.4. ∎

A próxima proposição mostra que a aplicação traço parcial é sobrejetora.

Proposição 3.29 *Seja S uma extensão α-parcial de Galois de R. Temos que:*

(i) Para qualquer $f \in Hom_R(S,R)$ existe $s = s(f) \in S$ tal que $f(y) = tr_{S/R}(sy)$, para todo $y \in S$.

(ii) Existe $c \in S$ com $tr_{S/R}(c) = 1$.

Demonstração.

(i) Suponha que S é uma extensão α-parcial de Galois de R. Então, pelo Teorema 3.27, $j : S \rtimes_\alpha G \to End_R(S)$ é um isomorfismo. Como $Hom_R(S,R) \subseteq End_R(S) \overset{j^{-1}}{\simeq} S \rtimes_\alpha G$, existe $w = \sum_{g\in G} a_g\delta_g \in S \rtimes_\alpha G$ tal que $f = j(w)$. Assim,

$$f(y) = j(w)(y) = \sum_{g\in G} a_g\alpha_g(y1_{g^{-1}}), \text{ para todo } y \in S.$$

Usando o Lema 3.23, temos

$$\begin{aligned}\alpha_h(f(y)1_{h^{-1}}) &= \alpha_h\left(\sum_{g\in G} a_g\alpha_g(y1_{g^{-1}})1_{h^{-1}}\right) = \sum_{g\in G}\alpha_h(a_g1_{h^{-1}})\alpha_h(\alpha_g(y1_{g^{-1}})1_{h^{-1}})\\ &= \sum_{g\in G}\alpha_h(a_g1_{h^{-1}})\alpha_{hg}(y1_{g^{-1}h^{-1}})1_h\\ &= \sum_{l\in G}\alpha_h(a_{h^{-1}l}1_{h^{-1}})\alpha_l(y1_{l^{-1}}),\end{aligned}$$

para todo $h \in G$, onde a última igualdade foi obtida fazendo $hg = l$.

Por outro lado, já que $f(y) \in R = S^\alpha$, temos $\alpha_h(f(y)1_{h^{-1}}) = f(y)1_h$. Então,

$$\sum_{l\in G}\alpha_h(a_{h^{-1}l}1_{h^{-1}})\alpha_l(y1_{l^{-1}}) = \sum_{l\in G} a_l\alpha_l(y1_{l^{-1}})1_h,$$

e isto implica que

$$j\left(\sum_{l\in G}\alpha_h(a_{h^{-1}l}1_{h^{-1}})1_l\delta_l\right)(y) = j\left(\sum_{l\in G} a_l1_h\delta_l\right)(y),$$

para todo $y \in S$ e $h \in G$. Como j é um isomorfismo, temos $\sum_{l\in G}\alpha_h(a_{h^{-1}l}1_{h^{-1}})1_l\delta_l = \sum_{l\in G} a_l1_h\delta_l$ e portanto $\alpha_h(\alpha_{h^{-1}l}1_{h^{-1}}) = a_l\delta_l$, para todo $g,h \in G$. Em particular, para $l = h$, temos

$$\alpha_h(a_11_{h^{-1}}) = a_h1_h = a_h, \text{ para todo } h \in G.$$

Para todo $y \in S$, temos

$$f(y) = \sum_{g\in G} = a_g\alpha_g(y1_{g^{-1}}) = \sum_{g\in G} \alpha_g(a_1 1_{g^{-1}})\alpha_g(y1_{g^{-1}}) = \sum_{g\in G}(a_1 y 1_{g^{-1}}) = tr_{S/R}(a_1 y).$$

(ii) Pelo Teorema 3.27, segue que S é um R-módulo projetivo e finitamente gerado. Sendo S também fiel, pelo Corolário 1.52, temos que S é um R-progerador e, em particular, S é um R-gerador. Então, existem $y_i \in S$ e $f_i \in Hom_R(S, R), 1 \leq i \leq n$, com $\sum_{i=1}^{n} f_i(y_i) = 1$. Usando o item (i), existem $x_i \in S$ tais que $f_i(y) = tr_{S/R}(x_i y)$, para todo $y \in S$. Assim,

$$\begin{aligned} 1 &= \sum_{i=1}^{n} f_i(y_i) = \sum_{i=1}^{n} tr_{S/R}(x_i y_i) \\ &= tr_{S/R}\left(\sum_{i=1}^{n} x_i y_i\right) = tr_{S/R}(c), \end{aligned}$$

onde $c = \sum_{i=1}^{n} x_i y_i \in S$. ∎

Capítulo 4

Quando um produto cruzado parcial por uma ação parcial torcida é Azumaya?

Sejam R um anel e G um grupo. Neste capítulo, discutiremos as condições necessárias e suficientes para que o produto cruzado parcial $S = R \rtimes_{\alpha,\omega} G$ por uma ação parcial torcida $\alpha = (\{D_g\}_{g\in G}, \{\alpha_g\}_{g\in G}, \{w_{g,h}\}_{(g,h)\in G\times G})$ de um grupo finito G sobre um anel R seja Azumaya, de acordo com [21].

De agora em diante, vamos supor que para cada $g \in G$, D_g é um ideal de R gerado por um idempotente central 1_g de R, ou seja, $D_g = 1_g R$. Como 1_g é idempotente, então $D_g = D_g^2$, para todo $g \in G$. Além disso, sendo $D_h = 1_h R$, onde $1_h \in R$ é um idempotente central, segue que $D_g \cdot D_h = 1_g 1_h R = 1_h 1_g R = D_h \cdot D_g$, mostrando que $D_g \cdot D_h = D_h \cdot D_g$, para quaisquer $g, h \in G$. Sabendo que para cada $g \in G$, D_g é uma álgebra com unidade, temos que D_g é isomorfo a $\mathcal{M}(D_g)$, pela Proposição 3.8. Assim, assumindo que cada ideal D_g é gerado por um idempotente central, podemos reescrever a Definição 3.15 da seguinte forma:

Definição 4.1 *Uma ação parcial torcida α de G em R é uma tripla*

$$\alpha = (\{D_g\}_{g\in G}, \{\alpha_g\}_{g\in G}, \{w_{g,h}\}_{(g,h)\in G\times G}),$$

onde para todo $g \in G$, D_g é um ideal de R gerado por um idempotente central 1_g de R, $\alpha_g : D_{g^{-1}} \to D_g$ é um isomorfismo de anéis, e para todo $(g,h) \in G \times G$, $w_{g,h}$ é um elemento invertível de $D_g \cdot D_{gh}$, satisfazendo as seguintes condições, para quaisquer $g, h, l \in G$:

(i) $D_1 = R$ *e* α_1 *é a aplicação identidade* I_R *de* R*;*
(ii) $\alpha_g(D_{g^{-1}} \cdot D_h) = D_g \cdot D_{gh}$*;*
(iii) $\alpha_g \circ \alpha_h(a) = w_{g,h}\alpha_{gh}(a)w_{g,h}^{-1}, \forall a \in D_{h^{-1}} \cdot D_{h^{-1}g^{-1}}$*;*
(iv) $w_{1,g} = w_{g,1} = 1_g$*;*
(v) $\alpha_g(aw_{h,l})w_{g,hl} = \alpha_g(a)w_{g,h}w_{gh,l}, \forall a \in D_{g^{-1}} \cdot D_h \cdot D_{hl}$.

Dizemos que α é *global* se $D_g = R$, para todo $g \in G$.

Note que se $w_{g,h} = 1_g 1_{gh}$, para todo $g, h \in G$, temos apenas a noção de ação parcial apresentada na Definição 3.1. De fato, já que os itens (i) e (ii) são satisfeitos, basta verificarmos se (iii) ocorre. Para $r \in D_{h^{-1}} \cdot D_{(gh)^{-1}}$, temos que:

$$\alpha_g \circ \alpha_h(r) = w_{g,h}\alpha_{gh}(r)w_{g,h}^{-1} = 1_g 1_{gh}\alpha_{gh}(r)1_g 1_{gh} = 1_g 1_{gh}\alpha_{gh}(r).$$

Observe que $\alpha_{gh}(r) \in \alpha_{gh}(D_{h^{-1}} \cdot D_{(gh)^{-1}}) = D_g \cdot D_{gh}$. Como $1_g 1_{gh}$ é a unidade de $D_g \cdot D_{gh}$ e $\alpha_g(r) \in D_g \cdot D_{gh}$, então $\alpha_g \circ \alpha_h(r) = \alpha_{gh}(r), \forall r \in D_{h^{-1}} \cdot D_{(gh)^{-1}}$.

Observe que, para todo $g \in G$,

$$\alpha_g(w_{g^{-1},g}) = w_{g,g^{-1}}. \tag{4.1}$$

De fato, pela condições (iv) e (v), para todo $g \in G$, temos:

$$\alpha_g(w_{g^{-1},g}) = \alpha_g(w_{g^{-1},g}1_{g^{-1}})w_{g,1} = 1_g w_{g,g^{-1}}w_{1,g} = w_{g,g^{-1}}1_g = w_{g,g^{-1}}.$$

Como cada α_g é um homomorfismo de álgebras, então

$$\alpha_g(w_{g^{-1},g}^{-1}) = \alpha_g(w_{g^{-1},g})^{-1},$$

para todo $g \in G$.

Ademais, para todo $g \in G$,

$$\alpha_g^{-1}(a) = w_{g^{-1},g}^{-1}\alpha_{g^{-1}}(a)w_{g^{-1},g},$$

para todo $a \in D_g$. Pela condição (iii) e por (4.1), para todo $a \in D_g$, temos:

$$\begin{aligned}\alpha_g(w_{g^{-1},g}^{-1}\alpha_{g^{-1}}(a)w_{g^{-1},g}) &= \alpha_g(w_{g^{-1},g}^{-1})\alpha_g(\alpha_{g^{-1}}(a))\alpha_g(w_{g^{-1},g}) \\ &= \alpha_g(w_{g^{-1},g})^{-1}w_{g,g^{-1}}aw_{g,g^{-1}}^{-1}\alpha_g(w_{g^{-1},g}) \\ &= w_{g,g^{-1}}^{-1}w_{g,g^{-1}}aw_{g,g^{-1}}^{-1}w_{g,g^{-1}} = a.\end{aligned}$$

Analogamente, temos que $\alpha_g^{-1}(a) \circ \alpha_g(a) = a$, para todo $a \in D_{g^{-1}}$.

Sendo $\alpha = (\{D_g\}_{g\in G}, \{\alpha_g\}_{g\in G}, \{w_{g,h}\}_{(g,h)\in G\times G})$ uma ação parcial torcida de um grupo G em um anel R, onde para todo $g \in G$, D_g é um ideal de R, vamos considerar o produto cruzado parcial $R \rtimes_{\alpha,\omega} G$, onde agora a multiplicação é definida pela regra

$$(r_g\delta_g)(r_h\delta_h) = r_g\alpha_g(r_h 1_{g^{-1}})w_{g,h}\delta_{gh}.$$

De fato, veja que:

$$\begin{aligned}(r_g\delta_g)(r_h\delta_h) &= \alpha_g(\alpha_g^{-1}(r_g)r_h)w_{g,h}\delta_{gh} = \alpha_g(\alpha_g^{-1}(r_g)1_{g^{-1}}r_h)w_{g,h}\delta_{gh}\\ &= \alpha_g(\alpha_g^{-1}(r_g))\alpha_g(r_h 1_{g^{-1}})w_{g,h}\delta_{gh}\\ &= r_g\alpha_g(r_h 1_{g^{-1}})w_{g,h}\delta_{gh}.\end{aligned}$$

Temos que $R \rtimes_{\alpha,\omega} G$ é um anel com unidade $1_R\delta_1$. Além disso, a aplicação $R \to R \rtimes_{\alpha,\omega} G, r \mapsto r\delta_1$, é uma imersão que nos permite identificar R com $R\delta_1$ e portanto podemos ver $R \rtimes_{\alpha,\omega} G$ como uma extensão de anéis de R.

Tome $W = \{w_{g,h}\}_{(g,h)\in G\times G}$. Relembre da Seção 3.4.2 que o subanel dos invariantes de R segundo α é definido por

$$R^\alpha = \{r \in R \mid \alpha_g(r1_{g^{-1}}) = r1_g, \text{ para todo } g \in G\}.$$

Lema 4.2 *[5, Lema 2.1] Sejam R, G e α como acima e $r \in R$. Para todo $g \in G$, temos:*

(i) *Se $r \in R^\alpha$, então $\alpha_g(r1_{g^{-1}}) \in C_R(W)$.*

(ii) $\alpha_g(C_R(W)1_{g^{-1}}) \subseteq C_R(W)$.

(iii) $\alpha_g(C(R)1_{g^{-1}}) \subseteq C(R)$.

Demonstração.

(i) Suponha que $r \in R^\alpha$, ou seja, $\alpha_g(r1_{g^{-1}}) = r1_g$, para todo $g \in G$. Como $\alpha_g(r1_{g^{-1}}) \in D_g \subset R$, basta verificar que

$$\alpha_g(r1_{g^{-1}})w_{h,l} = w_{h,l}\alpha_g(r1_{g^{-1}}),$$

para todo $g, h, l \in G$. Veja que:

$$\begin{aligned}\alpha_g(r1_{g^{-1}})1_h 1_{hl} &= 1_g r1_h 1_{hl} = 1_g r1_h 1_h 1_{hl} = 1_g\alpha_h(r1_{h^{-1}})\alpha_h(1_l 1_{h^{-1}}), \text{ pelo Lema 3.23}\\ &= 1_g\alpha_h(r1_l 1_{h^{-1}}) = 1_g\alpha_h(\alpha_l(r1_{l^{-1}})1_{h^{-1}})\\ &= 1_g\alpha_h(\alpha_l(r1_{l^{-1}}1_{(hl)^{-1}})), \text{ pelo Lema 3.23}\end{aligned}$$

$$
\begin{aligned}
&= 1_g w_{h,l}\alpha_{hl}(r1_{l^{-1}}1_{(hl)^{-1}})w_{h,l}^{-1}\\
&= 1_g w_{h,l}\alpha_{hl}(r1_{(hl)^{-1}})\alpha_{hl}(1_{l^{-1}}1_{(hl)^{-1}})w_{h,l}^{-1}\\
&= 1_g w_{h,l}\alpha_{hl}(r1_{(hl)^{-1}})1_h 1_{hl} w_{h,l}^{-1}\\
&= 1_g w_{h,l}\alpha_{hl}(r1_{(hl)^{-1}})w_{h,l}^{-1}, \text{ pois } w_{h,l} \in D_h \cdot D_{hl}\\
&= 1_g w_{h,l} r 1_{hl} w_{h,l}^{-1}\\
&= 1_g w_{h,l} r w_{h,l}^{-1}, \text{ pois } w_{h,l} \in D_h \cdot D_{hl}\\
&= w_{h,l}1_g r w_{h,l}^{-1}\\
&= w_{h,l}\alpha_g(r1_{g^{-1}})w_{h,l}^{-1}.
\end{aligned}
$$

Logo,

$$\alpha_g(r1_{g^{-1}})1_h 1_{hl} = w_{h,l}\alpha_g(r1_{g^{-1}})w_{h,l}^{-1}, \tag{4.2}$$

para todo $g, h, l \in G$. Como $w_{h,l}$ é inversível em $D_h \cdot D_{hl}$, multiplicando ambos os lados de (4.2) por $w_{h,l}$, obtemos

$$\alpha_g(r1_{g^{-1}})1_h 1_{hl} w_{hl} = w_{h,l}\alpha_g(r1_{g^{-1}})w_{h,l}^{-1}w_{h,l}$$

e assim $\alpha_g(r1_{g^{-1}})w_{hl} = w_{h,l}\alpha_g(r1_{g^{-1}})1_h 1_{hl}$, para todo $g, h, l \in G$. Portanto, $\alpha_g(r1_{g^{-1}}) \in C_R(W)$, para todo $g \in G$.

(ii) Para todo $w_{h,l} \in W$ e $g \in G$, tome

$$s = w_{g^{-1},g}^{-1}\alpha_{g^{-1}}(w_{h,l}1_g)w_{g^{-1},g} = w_{g^{-1},g}^{-1}\alpha_{g^{-1}}(w_{h,l}1_g)w_{g^{-1},hl}w_{g^{-1},hl}^{-1}w_{g^{-1},g},$$

pois $\alpha_{g^{-1}}(w_{h,l}1_g) \in \alpha_{g^{-1}}(D_h \cdot D_{hl} \cdot D_g) = D_{g^{-1}} \cdot D_{g^{-1}h} \cdot D_{g^{-1}hl}$. Pela condição (v) da Definição 4.1, segue que

$$
\begin{aligned}
s &= w_{g^{-1},g}^{-1}\alpha_{g^{-1}}(1_g)w_{g^{-1},h}w_{g^{-1}h,l}w_{g^{-1},hl}^{-1}w_{g^{-1},g}\\
&= w_{g^{-1},g}^{-1}1_{g^{-1}}w_{g^{-1},h}w_{g^{-1}h,l}w_{g^{-1},hl}^{-1}w_{g^{-1},g}\\
&= w_{g^{-1},g}^{-1}w_{g^{-1},h}w_{g^{-1}h,l}w_{g^{-1},hl}^{-1}w_{g^{-1},g},
\end{aligned}
$$

pois $w_{g^{-1},h} \in D_{g^{-1}} \cdot D_{g^{-1}h}$. Daí, $s \in W$. Agora, observe que:

$$
\begin{aligned}
\alpha_g(s) &= \alpha_g(w_{g^{-1},g}^{-1}\alpha_{g^{-1}}(w_{h,l}1_g)w_{g^{-1},g})\\
&= \alpha_g(w_{g^{-1},g}^{-1})\alpha_g(\alpha_{g^{-1}}(w_{h,l}1_g))\alpha_g(w_{g^{-1},g})\\
&= \alpha_g(w_{g^{-1},g})^{-1}w_{g,g^{-1}}\alpha_{gg^{-1}}(w_{h,l}1_g)w_{g,g^{-1}}^{-1}w_{g,g^{-1}}\\
&= w_{g,g^{-1}}^{-1}w_{g,g^{-1}}w_{h,l}1_g 1_g\\
&= 1_g w_{h,l}1_g = w_{h,l}1_g.
\end{aligned}
$$

Se $r \in C_R(W)$, então $rs = sr$, já que $s \in W$. Assim, para todo $r \in C_R(W)$, temos

$$\begin{aligned}\alpha_g(r1_{g^{-1}})w_{h,l} &= \alpha_g(r1_{g^{-1}})w_{h,l}1_g = \alpha_g(r1_{g^{-1}})\alpha_g(s) = \alpha_g(rs1_{g^{-1}}) \\ &= \alpha_g(sr1_{g^{-1}}) = \alpha_g(s)\alpha_g(r1_{g^{-1}}) = w_{h,l}1_g\alpha_g(r1_{g^{-1}}) \\ &= w_{h,l}\alpha_g(r1_{g^{-1}}).\end{aligned}$$

Logo,

$$\alpha_g(C_R(W)1_{g^{-1}}) \subseteq C_R(W),$$

para todo $g \in G$.

(iii) Para todo $s \in R$ e $g \in G$, considere

$$s' = w^{-1}_{g^{-1},g}\alpha_{g^{-1}}(s1_g)w_{g^{-1},g}.$$

Utilizando um raciocínio análogo a demonstração do item (ii), encontramos

$$\alpha_g(s') = s1_g,$$

para todo $g \in G$. Para $r \in C(R)$, temos

$$\begin{aligned}\alpha_g(r1_{g^{-1}})s &= \alpha_g(r1_{g^{-1}})1_g s = \alpha_g(r1_{g^{-1}})\alpha_g(s') = \alpha_g(rs'1_{g^{-1}}) \\ &= \alpha_g(s'r1_{g^{-1}}) = \alpha_g(s')\alpha_g(r1_{g^{-1}}) = s1_g\alpha_g(r1_{g^{-1}}) \\ &= s\alpha_g(r1_{g^{-1}}).\end{aligned}$$

Como r e s foram tomados de forma arbitrária, concluímos que $\alpha_g(C(R)1_{g^{-1}}) \subseteq C(R)$, para todo $g \in G$. ∎

Corolário 4.3

(i) $\alpha|_{C_R(W)} = (\{C_R(W)1_g\}_{g\in G}, \{\alpha_g|_{C_R(W)1_{g^{-1}}}\}_{g\in G})$ *(respectivamente,* $\alpha|_{C(R)} = (\{C(R)1_g\}_{g\in G}$, $\{\alpha_g|_{C(R)1_{g^{-1}}}\}_{g\in G})$*) é uma ação parcial de* G *em* $C_R(W)$ *(respectivamente,* $C(R)$*).*

(ii) O subanel dos invariantes de R *segundo* α *é* $C_R(W) = \{r \in C_R(W) \mid \alpha_g(r1_{g^{-1}}) = r1_g$*, para todo* $g \in G\}$*.*

Demonstração.

(i) Basta mostrar que $\alpha'_g = \alpha_g|_{C_R(W)} : C_R(W)1_{g^{-1}} \to C_R(W)1_g$ é um isomorfismo. Para isso, é suficiente mostrar que

$$\alpha_g(C_R(W)1_{g^{-1}}) = C_R(W)1_g.$$

Pelo Lema 4.2, temos que $\alpha_g(C_R(W)1_{g^{-1}}) \subseteq C_R(W)$. Claramente, $\alpha_g(C_R(W)1_{g^{-1}}) \subseteq D_g$ e portanto $\alpha_g(C_R(W)1_{g^{-1}}) \subseteq C_R(W)1_g$. Para a inclusão contrária, considere $y \in C_R(W)1_g$, então $y \in C_R(W)$ e $y \in D_g$. Como $\alpha_g : D_{g^{-1}} \to D_g$ é um isomorfismo, então existe $x \in D_{g^{-1}}$ tal que $y = \alpha_g(x)$. Aplicando $\alpha_{g^{-1}}$ temos, pelo Lema 4.2, que

$$w_{g,g^{-1}} x w_{g,g^{-1}}^{-1} = \alpha_{g^{-1}}(y) \in C_R(W).$$

Assim, como $w_{g,g^{-1}}^{-1} \in D_1 = R$, segue

$$\begin{aligned} x &= w_{g,g^{-1}}^{-1} \alpha_{g^{-1}}(y) w_{g,g^{-1}} \\ &= \alpha_{g^{-1}}(y) w_{g,g^{-1}}^{-1} w_{g,g^{-1}} \\ &= \alpha_{g^{-1}}(y) \in C_R(W). \end{aligned}$$

Logo, $y = \alpha_g(x) \in \alpha_g(C_R(W)1_{g^{-1}})$. Portanto, vale a igualdade. Para
$\alpha' = (\{C(R)1_g\}, \{\alpha_g|_{C(R)1_{g^{-1}}}\})$ é análogo.
(ii) É imediato que $C_R(W)^\alpha \subseteq R^\alpha$, já que $C_R(W) \subseteq R$. Se $r \in R^\alpha$, então pelo Lema 4.2, temos que

$$r1_g = \alpha_g(r1_{g^{-1}}) \in C_R(W), \forall g \in G.$$

Em particular, para $g = 1$, temos que

$$r = r1_R = \alpha_1(r1_R) \in C_R(W).$$

Logo, $r \in C_R(W)^\alpha$. ∎

4.1 H-separabilidade

De agora em diante, $\alpha = (\{D_g\}_{g\in G}, \{\alpha_g\}_{g\in G}, \{w_{g,h}\}_{(g,h)\in G\times G},)$ sempre denotará uma ação parcial torcida de um grupo G sobre R e $S = R \rtimes_{\alpha,\omega} G$ será o correspondente produto cruzado parcial. Temos:

Observação 4.4 *Todo elemento em $S \otimes_R S$ pode ser representado de modo único na forma*

$$x = \sum_{g,h\in G} r_{g,h}\delta_g \otimes 1_h\delta_h, \text{ com } r_{g,h} \in D_g \cdot D_{gh}.$$

De fato, seja $x = \sum_{g,h\in G} r_g\delta_g \otimes r_h\delta_h \in S \otimes_R S$, com $r_g \in D_g$ e $r_h \in D_h$. Assim,

$$\begin{aligned} x &= \sum_{g,h\in G} r_g\delta_g \otimes r_h\delta_h = \sum_{g,h\in G} r_g\delta_g \otimes (r_h\delta_1)(1_h\delta_h) \\ &= \sum_{g,h\in G} (r_g\delta_g)(r_h\delta_1) \otimes 1_h\delta_h = \sum_{g,h\in G} r_g\alpha_g(r_h1_{g^{-1}})\delta_g \otimes 1_h\delta_h. \end{aligned}$$

Sendo $\alpha_g(r_h 1_{g^{-1}}) \in \alpha_g(D_h \cdot D_{g^{-1}}) = D_g \cdot D_{gh}$ *e considerando* $r_{g,h} = r_g \alpha_g(r_h 1_{g^{-1}}) \in D_g \cdot D_g \cdot D_{gh} = D_g \cdot D_{gh}$, *temos a expressão desejada para* $x \in S \otimes_R S$. *A unicidade decorre das propriedades do produto tensorial.*

Para cada par $(g, h) \in G \times G$, seja

$$\phi_{g,h} := \{r \in D_g \cdot D_{gh} \mid (rw_{g,h})\alpha_{gh}(s1_{(gh)^{-1}}) = s(rw_{g,h}), \text{ para todo } s \in R\}.$$

Veja que:

$$\begin{aligned}\phi_{1,g} &= \{r \in D_g \cdot D_g \mid (rw_{g,1})\alpha_g(s1_{g^{-1}}) = s(rw_{g,1}), \text{ para todo } s \in R\} \\ &= \{r \in D_g \mid (r1_g)\alpha_g(s1_{g^{-1}}) = s(r1_g), \text{ para todo } s \in R\} \\ &= \{r \in D_g \mid r\alpha_g(s1_{g^{-1}}) = sr, \text{ para todo } s \in R\}.\end{aligned}$$

Analogamente, $\phi_{g,1} = \{r \in D_g \mid r\alpha_g(s1_{g^{-1}}) = sr, \text{ para todo } s \in R\}$ para todo $g \in G$. Assim, vamos denotar simplesmente por $\phi_g = \phi_{1,g} = \phi_{g,1}$.

Definição 4.5 *Dizemos que a ação parcial torcida* α *de* G *sobre* R *é* ω*-externa em* R *se* $\phi_g = 0$, *para todo* $g \neq 1$.

Lema 4.6

(i) $C_S(R) = \sum_{g \in G} \phi_g \delta_g$.

(ii) São equivalentes:

(1) α *é* ω*-externa em* R;

(2) $C_S(R) \subseteq R$;

(3) $C_S(R) = C(R)$.

Neste caso, $C(S) = C(R)^\alpha$.

Demonstração.

(i) Seja $s = \sum_{g \in G} r_g \delta_g \in S$. Então, $s \in C_S(R)$ se, e somente se, para todo $r \in R$,

$$rs = sr. \tag{4.3}$$

Temos:

$$rs = \sum_{g \in G} r(r_g \delta_g) = \sum_{g \in G} r r_g \delta_g.$$

Por outro lado:

$$sr = \sum_{g \in G} (r_g \delta_g) r = \sum_{g \in G} r_g \alpha_g(r 1_{g^{-1}}) \delta_g.$$

Assim, a equação (4.3) ocorre se, e somente se, $rr_g = r_g\alpha_g(r1_{g^{-1}})$, para todo $g \in G$, ou, equivalentemente, $r_g \in \phi_g$, para todo $g \in G$.

(ii) (1) $\Rightarrow$ (2) Suponha que α é ω-externa em R. Seja $x \in C_S(R)$, com $x = \sum_{g\in G} r_g\delta_g$. Sendo $C_S(R) = \sum_{g\in G} \phi_g\delta_g$, pelo item (i), segue que $r_g \in \phi_g$, para todo $g \in G$. Como α é ω-externa em R, temos $\phi_g = 0$ para todo $1 \neq g \in G$. Logo, $x = r_1\delta_1 \in D_1 = R$ e daí $C_S(R) \subseteq R$.

(2) $\Rightarrow$ (3) Suponha que $C_S(R) \subseteq R$. Seja $x \in C_S(R)$. Então, $x \in S$ comuta com os elementos de R. Como $x \in C_S(R) \subseteq R$, segue que $x \in R$ e daí $x \in C(R)$. Reciprocamente, seja $x \in C(R)$. Como $R \subset S$, temos que $x \in C_S(R)$, provando a igualdade.

(3) $\Rightarrow$ (1) Suponha que $C_S(R) = C(R)$. Pelo item (i), $C_S(R) = \sum_{g\in G} \phi_g\delta_g$. Assim, $\sum_{g\in G} \phi_g\delta_g \subseteq R$. Ou seja, $\phi_g = 0$, para todo $1 \neq g \in G$. mostrando que α é ω-externa em R.

Agora, suponha que vale (1) e portanto todas as condições equivalentes de (ii). Vamos mostrar que $C(S) = C(R)^\alpha$. Se $r \in C(R)^\alpha$, então $r \in C(R)$ e $\alpha_g(r1_{g^{-1}}) = r1_g$, para todo $g \in G$. Observe que $r \in S$, já que $R \subset S$. Assim, só resta provar que r comuta com os elementos de S. Para todo $g \in G$ e $r_g \in D_g$, temos

$$\begin{aligned}(r_g\delta_g)r &= (r_g\delta_g)(r\delta_1) = r_g\alpha_g(r1_{g^{-1}})w_{g,1}\delta_g \\ &= r_g1_gr\delta_g = r_gr\delta_g \\ &= rr_g\delta_g = (r\delta_1)(r_g\delta_g) \\ &= r(r_g\delta_g).\end{aligned}$$

Dessa forma, $C(R)^\alpha \subseteq C(S)$. Reciprocamente, seja $x \in C(S) \subseteq C_S(R) = C(R)$. Como $x \in C(S)$, em particular,

$$x(1_g\delta_g) = (1_g\delta_g)x,$$

para todo $g \in G$. Veja que:

$$x(1_g\delta_g) = (x\delta_1)(1_g\delta_g) = x1_g\delta_g$$

e

$$(1_g\delta_g)x = (1_g\delta_g)(x\delta_1) = 1_g\alpha_g(x1_{g^{-1}})\delta_g = \alpha_g(x1_{g^{-1}})\delta_g.$$

Assim, $x1_g\delta_g = \alpha_g(x1_{g^{-1}})\delta_g$, o que implica em $x1_g = \alpha_g(x1_{g^{-1}})$, para todo $g \in G$. Portanto, $x \in C(R)^\alpha$.

■

Temos que $S = R \rtimes_{\alpha,\omega} G$ é um R-bimódulo cuja estrutura é definida por:

$$r(r_g\delta_g) = (r\delta_1)(r_g\delta_g) = rr_g\delta_g$$

e

$$(r_g\delta_g)r = (r_g\delta_g)(r\delta_1) = r_g\alpha_g(r1_{g^{-1}})\delta_g,$$

para todo $r \in R, r_g\delta_g \in S$.

Além disso, $S \otimes_R S$ é um S-bimódulo cuja estrutura é definida por:

$$(r_l\delta_l)(r_{g,h}\delta_g \otimes 1_h\delta_h) = (r_l\delta_l)(r_{g,h}\delta_g) \otimes 1_h\delta_h$$

e

$$(r_{g,h}\delta_g \otimes 1_h\delta_h)(r_l\delta_l) = r_{g,h}\delta_g \otimes (1_h\delta_h)(r_l\delta_l),$$

para todo $r_{g,h}\delta_g \otimes 1_h\delta_h \in S \otimes_R S$ e $r_l\delta_l \in S$.

Proposição 4.7

(i) $\sum_{g,h\in G} r_{g,h}\delta_g \otimes 1_h\delta_h \in C_{S\otimes_R S}(S)$ *se, e somente se,*

$$r_{g,h} \in \phi_{g,h} \quad e \quad \alpha_l(r_{l^{-1}g,h}1_{l^{-1}})w_{l,l^{-1}g} = r_{g,hl^{-1}}\alpha_g(w_{hl^{-1},l}1_{g^{-1}}),$$

para todo $g, h, l \in G$.

(ii) Se $\sum_{g,h\in G} r_{g,h}\delta_g \otimes 1_h\delta_h \in C_{S\otimes_R S}(S)$, *então* $r_{1,1} \in C(R)$ *e* $r_{g,g^{-1}} = \alpha_g(r_{1,1}1_{g^{-1}})w^{-1}_{g,g^{-1}}$, *para todo* $g \in G$.

(iii) Se G *é finito, então* $\sum_{g\in G} \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}} \in C_{S\otimes_R S}(S)$, *para qualquer* $r \in C(R)$.

(iv) Se G *é finito e* α *é* ω*-externa em* R, *então todo elemento em* $C_{S\otimes_R S}(S)$ *é do tipo descrito em (iii).*

Demonstração.

(*i*) Seja $x = \sum_{g,h\in G} r_{g,h}\delta_g \otimes 1_h\delta_h \in S \otimes_R S$, com $r_{g,h} \in D_g \cdot D_{gh}$.

Afirmação 4.8 $x \in C_{S\otimes_R S}(S)$ *se, e somente se,*

$$rx = xr \tag{4.4}$$

e

$$(1_g\delta_g)x = x(1_g\delta_g) \tag{4.5}$$

para todo $r \in R$ *e* $g \in G$.

De fato, se $x \in C_{S\otimes_R S}(S)$, então (4.4) e (4.5) ocorrem, já que x comuta com os elementos de S e, em particular, $R \subseteq S$. Reciprocamente, assuma que (4.4) e (4.5) valem. Como $x \in S \otimes_R S$, só resta verificar que x comuta com os elementos de S. Seja $s = \sum_{l\in G} r_l\delta_l \in S$. Uma vez que $S \otimes_R S$ é um (S, S)-bimódulo, segue que:

$$\begin{aligned}
xs &= x\left(\sum_{l\in G} r_l\delta_l\right) = x\left(\sum_{l\in G}(r_l\delta_1)(1_l\delta_l)\right)\\
&= \sum_{l\in G} x[(r_l\delta_1)(1_l\delta_l)] = \sum_{l\in G}[x(r_l\delta_1)](1_l\delta_l)\\
&= \sum_{l\in G}[(r_l\delta_1)x](1_l\delta_l), \text{ pela equação (4.4)}\\
&= \sum_{l\in G}(r_l\delta_1)[x(1_l\delta_l)]\\
&= \sum_{l\in G}(r_l\delta_1)[(1_l\delta_l)x], \text{ pela equação (4.5)}\\
&= \sum_{l\in G}[(r_l\delta_1)(1_l\delta_l)]x\\
&= \left(\sum_{l\in G} r_l\delta_l\right)x = sx.
\end{aligned}$$

Assim, $x \in C_{S\otimes_R S}(S)$, provando o resultado.

Por (4.4), temos:

$$\begin{aligned}
\sum_{g,h\in G} rr_{g,h}\delta_g \otimes 1_h\delta_h &= \sum_{g,h\in G} r_{g,h}\delta_g \otimes (1_h\delta_h)(r\delta_1)\\
&= \sum_{g,h\in G} r_{g,h}\delta_g \otimes 1_h\alpha_h(r1_{h^{-1}})w_{h,1}\delta_h\\
&= \sum_{g,h\in G} r_{g,h}\delta_g \otimes (\alpha_h(r1_{h^{-1}})\delta_1)(1_h\delta_h)\\
&= \sum_{g,h\in G} (r_{g,h}\delta_g)(\alpha_h(r1_{h^{-1}})\delta_1) \otimes 1_h\delta_h, \text{ pois } \alpha_h(r1_{h^{-1}})\delta_1 \in R\\
&= \sum_{g,h\in G} r_{g,h}\alpha_g(\alpha_h(r1_{h^{-1}})1_{g^{-1}})w_{g,1}\delta_g \otimes 1_h\delta_h\\
&= \sum_{g,h\in G} r_{g,h}\alpha_g \circ \alpha_h(r1_{h^{-1}}1_{(gh)^{-1}})\delta_g \otimes 1_h\delta_h, \text{ pelo Lema 3.23}\\
&= \sum_{g,h\in G} r_{g,h}w_{g,h}\alpha_{gh}(r1_{h^{-1}}1_{(gh)^{-1}})w_{g,h}^{-1}\delta_g \otimes 1_h\delta_h\\
&= \sum_{g,h\in G} r_{g,h}w_{g,h}\alpha_{gh}(r1_{(gh)^{-1}})\alpha_{gh}(1_{h^{-1}}1_{(gh)^{-1}})w_{g,h}^{-1}\delta_g \otimes 1_h\delta_h\\
&= \sum_{g,h\in G} r_{g,h}w_{g,h}\alpha_{gh}(r1_{(gh)^{-1}})1_{gh}1_gw_{g,h}^{-1}\delta_g \otimes 1_h\delta_h\\
&= \sum_{g,h\in G} r_{g,h}w_{g,h}\alpha_{gh}(r1_{(gh)^{-1}})w_{g,h}^{-1}\delta_g \otimes 1_h\delta_h,
\end{aligned}$$

pois $w_{g,h} \in D_g \cdot D_{gh}$. Assim, $rr_{g,h} = r_{g,h}w_{g,h}\alpha_{gh}(r1_{(gh)^{-1}})w_{g,h}^{-1}$, para $r \in R$ e $g, h \in G$. Já que $w_{g,h}$ é inversível em $D_g \cdot D_{gh}$, segue que

$$rr_{g,h}w_{g,h} = r_{g,h}w_{g,h}\alpha_{gh}(r1_{(gh)^{-1}}),$$

para todo $r \in R$ e $g, h \in G$ e isso é equivalente a dizer que $r_{g,h} \in \phi_{g,h}$.

Agora, note que para todo $l \in G$, temos

$$\begin{aligned}
(1_l\delta_l)x &= \sum_{g,h\in G} (1_l\delta_l)(r_{g,h}\delta_g) \otimes 1_h\delta_h \\
&= \sum_{g,h\in G} 1_l\alpha_l(r_{g,h}1_{l^{-1}})w_{l,g}\delta_{lg} \otimes 1_h\delta_h, \quad (\text{tome } lg = k) \\
&= \sum_{k,h\in G} \alpha_l(r_{l^{-1}k,h}1_{l^{-1}})w_{l,l^{-1}k}\delta_k \otimes 1_h\delta_h, \quad (\text{tome } g = k) \\
&= \sum_{g,h\in G} \alpha_l(r_{l^{-1}g,h}1_{l^{-1}})w_{l,l^{-1}g}\delta_g \otimes 1_h\delta_h
\end{aligned}$$

e

$$\begin{aligned}
x(1_l\delta_l) &= \sum_{g,h\in G} r_{g,h}\delta_g \otimes (1_h\delta_h)(1_l\delta_l) \\
&= \sum_{g,h\in G} r_{g,h}\delta_g \otimes 1_h\alpha_h(1_l1_{h^{-1}})w_{h,l}\delta_{hl} \\
&= \sum_{g,h\in G} r_{g,h}\delta_g \otimes 1_h1_{hl}w_{h,l}\delta_{hl} \\
&= \sum_{g,h\in G} r_{g,h}\delta_g \otimes w_{h,l}\delta_{hl}, \text{ pois } w_{h,l} \in D_h \cdot D_{hl} \\
&= \sum_{g,h\in G} r_{g,h}\delta_g \otimes (w_{h,l}\delta_1)(1_{hl}\delta_{hl}) \\
&= \sum_{g,h\in G} (r_{g,h}\delta_g)(w_{h,l}\delta_1) \otimes 1_{hl}\delta_{hl}, \text{ pois } w_{h,l}\delta_1 \in R \\
&= \sum_{g,h\in G} r_{g,h}\alpha_g(w_{h,l}1_{g^{-1}})w_{g,1}\delta_g \otimes 1_{hl}\delta_{hl} \quad (\text{tome } hl = k) \\
&= \sum_{g,k\in G} r_{g,kl^{-1}}\alpha_g(w_{kl^{-1},l}1_{g^{-1}})\delta_g \otimes 1_k\delta_k \quad (\text{tome } h = k) \\
&= \sum_{g,h\in G} r_{g,hl^{-1}}\alpha_g(w_{hl^{-1},l}1_{g^{-1}})\delta_g \otimes 1_h\delta_h.
\end{aligned}$$

Portanto, segue de (4.5) que

$$\sum_{g,h\in G} \alpha_l(r_{l^{-1}g,h}1_{l^{-1}})w_{l,l^{-1}g}\delta_g \otimes 1_h\delta_h = \sum_{g,h\in G} r_{g,hl^{-1}}\alpha_g(w_{hl^{-1},l}1_{g^{-1}})\delta_g \otimes 1_h\delta_h,$$

o que significa que

$$\alpha_l(r_{l^{-1}g,h}1_{l^{-1}})w_{l,l^{-1}g} = r_{g,hl^{-1}}\alpha_g(w_{hl^{-1},l}1_{g^{-1}}), \tag{4.6}$$

para todo $g, h, l \in G$.

(ii) Suponha que $\sum_{g,h\in G} r_{g,h}\delta_g \otimes 1_h\delta_h \in C_{S\otimes_R S}(S)$. Por (i), $r_{g,h} \in \phi_{g,h}$ e

$$\alpha_l(r_{l^{-1}g,h}1_{l^{-1}})w_{l,l^{-1}g} = r_{g,hl^{-1}}\alpha_g(w_{hl^{-1},l}1_{g^{-1}}), \tag{4.7}$$

para todo $g, h, l \in G$. Para $g = h = 1$, temos que $r_{1,1} \in \phi_1 = C(R)$, pois:

$$\phi_1 = \{r \in D_1 \mid r\alpha_1(s) = sr, \text{ para todo } s \in R\} = \{r \in R \mid rs = sr, \text{ para todo } s \in R\} = C(R).$$

Além disso, tomando $g = l$ e $h = 1$ em (4.7), temos

$$\alpha_g(r_{1,1}1_{g^{-1}}) = r_{g,g^{-1}}\alpha_g(w_{g^{-1},g}1_{g^{-1}}) = r_{g,g^{-1}}w_{g,g^{-1}},$$

para todo $g \in G$. Como $w_{g,g^{-1}}$ é um elemento inversível de D_g e $r_{g,g^{-1}} \in D_g$, obtemos que $\alpha_g(r_{1,1}1_{g^{-1}})w^{-1}_{g,g^{-1}} = r_{g,g^{-1}}$, para todo $g \in G$.

(iii) Seja $x = \sum_{g\in G} \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}} \in S \otimes_R S$, com $r \in C(R)$. Para verificar que $x \in C_{S\otimes_R S}(S)$, basta verificar que

$$r'x = xr'$$

e

$$(1_g\delta_g)x = x(1_g\delta_g),$$

para todo $r' \in R$ e $g \in G$. Veja que:

$$\begin{aligned}
xr' &= \sum_{g\in G} \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes (1_{g^{-1}}\delta_{g^{-1}})(r'\delta_1) = \sum_{g\in G} \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\alpha_{g^{-1}}(r'1_g)w_{g^{-1},1}\delta_{g^{-1}} \\
&= \sum_{g\in G} \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes ((\alpha_{g^{-1}}(r'1_g)\delta_1)(1_{g^{-1}}\delta_{g^{-1}})) \\
&= \sum_{g\in G} \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g\alpha_{g^{-1}}(r'1_g)\delta_1 \otimes 1_{g^{-1}}\delta_{g^{-1}}, \text{ pois } \alpha_{g^{-1}}(r1_g)\delta_1 \in R \\
&= \sum_{g\in G} \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\alpha_g(\alpha_{g^{-1}}(r'1_g))w_{g,1}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}} \\
&= \sum_{g\in G} \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}w_{g,g^{-1}}\alpha_1(r'1_g)w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}}, \text{ pela Definição 4.1 } (iii) \\
&= \sum_{g\in G} \alpha_g(r1_{g^{-1}})r'w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}} \\
&= \sum_{g\in G} r'\alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}}, \text{ pelo Lema 4.2 } (iii) \\
&= r'x.
\end{aligned}$$

Agora, note que para todo $l \in G$, temos

$$\begin{aligned}
(1_l\delta_l)x &= \sum_{g\in G}(1_l\delta_l)\alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}} \\
&= \sum_{g\in G} 1_l\alpha_l(\alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}1_{l^{-1}})w_{l,g}\delta_{lg} \otimes 1_{g^{-1}}\delta_{g^{-1}}, \quad (\text{tome } lg = k) \\
&= \sum_{k\in G} \alpha_l(\alpha_{l^{-1}k}(r1_{k^{-1}l})w^{-1}_{l^{-1}k,k^{-1}l}1_{l^{-1}})w_{l,l^{-1}k}\delta_k \otimes 1_{k^{-1}l}\delta_{k^{-1}l}, \quad (\text{tome } k = g) \\
&= \sum_{g\in G} \alpha_l(\alpha_{l^{-1}g}(r1_{g^{-1}l})w^{-1}_{l^{-1}g,g^{-1}l}1_{l^{-1}})w_{l,l^{-1}g}\delta_g \otimes 1_{g^{-1}l}\delta_{g^{-1}l}
\end{aligned}$$

e

$$\begin{aligned}
x(1_l\delta_l) &= \sum_{g\in G}\alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes (1_{g^{-1}}\delta_{g^{-1}})(1_l\delta_l) \\
&= \sum_{g\in G}\alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\alpha_{g^{-1}}(1_l1_g)w_{g^{-1},l}\delta_{g^{-1}l} \\
&= \sum_{g\in G}\alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}1_{g^{-1}}1_{g^{-1}l}w_{g^{-1},l}\delta_{g^{-1}l} \\
&= \sum_{g\in G}\alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g w_{g^{-1},l}\delta_1 \otimes 1_{g^{-1}l}\delta_{g^{-1}l} \\
&= \sum_{g\in G}\alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\alpha_g(w_{g^{-1},l}1_{g^{-1}})w_{g,1}\delta_g \otimes 1_{g^{-1}l}\delta_{g^{-1}l}.
\end{aligned}$$

Assim, $(1_l\delta_l)x = x(1_l\delta_l)$ se, e somente se,

$$\alpha_l(\alpha_{l^{-1}g}(r1_{g^{-1}l})w^{-1}_{l^{-1}g,g^{-1}l}1_{l^{-1}})w_{l,l^{-1}g} = \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\alpha_g(w_{g^{-1},l}1_{g^{-1}}),$$

para todo $l \in G$. Vejamos que isso ocorre. Das propriedades (iii) e (v) da Definição 4.1, para todo $g, l \in G$, temos:

$$\begin{aligned}
\alpha_l(\alpha_{l^{-1}g}(r1_{g^{-1}l})w^{-1}_{l^{-1}g,g^{-1}l}1_{l^{-1}})w_{l,l^{-1}g} &= \alpha_l(\alpha_{l^{-1}g}(r1_{g^{-1}l})1_{l^{-1}})\alpha_l(w^{-1}_{l^{-1}g,g^{-1}l}1_{l^{-1}})w_{l,l^{-1}g} \\
&= w_{l,l^{-1}g}\alpha_g(r1_{g^{-1}l}1_{g^{-1}})w^{-1}_{l,l^{-1}g}(\alpha_l(1_{l^{-1}})w_{l,l^{-1}g}w_{g,g^{-1}l})^{-1}w_{l,l^{-1}g} \\
&= w_{l,l^{-1}g}\alpha_g(r1_{g^{-1}})\alpha_g(1_{g^{-1}}1_{g^{-1}l})w^{-1}_{l,l^{-1}g}w^{-1}_{g,g^{-1}l}w^{-1}_{l,l^{-1}g}w_{l,l^{-1}g} \\
&= w_{l,l^{-1}g}\alpha_g(r1_{g^{-1}})1_l1_gw^{-1}_{l,l^{-1}g}w^{-1}_{g,g^{-1}l}1_l1_g \\
&= w_{l,l^{-1}g}\alpha_g(r1_{g^{-1}})w^{-1}_{l,l^{-1}g}w^{-1}_{g,g^{-1}l}, \text{ pois } w_{g,g^{-1}l} \in D_g \cdot D_l \\
&= w_{l,l^{-1}g}w^{-1}_{l,l^{-1}g}\alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}l}, \text{ pois } \alpha_g(r1_{g^{-1}}) \in C(R) \\
&= \alpha_g(r1_{g^{-1}})w_{g,g^{-1}l}, \text{ pois } w_{g,g^{-1}l} \in D_g \cdot D_l \\
&= \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}w_{g,g^{-1}}w_{g,g^{-1}l} \\
&= \alpha_g(r1_{g^{-1}})w^{-1}_{g,g^{-1}}\alpha_g(w_{g^{-1},l}1_{g^{-1}}).
\end{aligned}$$

Logo, temos o resultado desejado.

(iv) Suponha que G é finito e α é ω-externa em R. Seja $x = \sum_{g,h\in G} r_{g,h}\delta_g \otimes 1_h\delta_h \in C_{S\otimes_R S}(S)$. Pelo item (i), temos que $r_{g,h} \in \phi_{g,h}$. Isso significa que

$$(r_{g,h}w_{g,h})\alpha_{gh}(s1_{(gh)^{-1}}) = s(r_{g,h}w_{g,h}), \text{ para todo } s \in R.$$

Como $\phi_{gh} = \{r \in D_{gh} \mid r\alpha_{gh}(s1_{(gh)^{-1}}) = sr, \text{ para todo } s \in R\}$, segue que $r_{g,h}w_{g,h} \in \phi_{gh}$. Pelo item (i) do Lema 4.6, sabemos que $C_S(R) = \sum_{g\in G} \phi_g\delta_g$. Logo, $r_{g,h}w_{g,h}\delta_{gh} \in C_S(R) = C(R)$, pelo item (ii) do mesmo Lema, já que α é ω-externa. Assim, $r_{g,h} = 0$ para todo $g, h \in G$ tal que $gh \neq 1$ e, consequentemente, $x = \sum_{g\in G} r_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}}$. Por (ii), sabemos que $r_{1,1} \in C(R)$ e $r_{g,g^{-1}} = \alpha_g(r_{1,1}1_{g^{-1}})w^{-1}_{g,g^{-1}}$, para todo $g \in G$. Logo, $x = \alpha_g(r_{1,1}1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}}$. Tomando $r_{1,1} = r \in C(R)$, obtemos o resultado desejado.

■

Corolário 4.9 *Considere as seguintes afirmações:*

(i) $C_S(R)$ *é um anel comutativo;*

(ii) $C_S(R) = C(R)$*;*

(iii) $C_S(R) \subseteq R$*;*

(iv) $C_S(C(R)) = R$*;*

(v) α *é* ω*-externa em* R*.*

Então, $(ii) \Rightarrow (i), (ii) \Leftrightarrow (iii) \Leftrightarrow (v)$*, e* $(iv) \Rightarrow (v)$*. Se em adição* $C_S(C_S(R)) = R$*, então* $(i) \Rightarrow (ii) \Rightarrow (iv)$ *e, em particular, neste caso as condições são equivalentes.*

Demonstração.

$(ii) \Rightarrow (i)$ Temos que $C_S(R)$ é um subanel de S e assim $C_S(R)$ é por si um anel (com as mesmas operações de S). Como $C(R)$ é comutativo e $C_S(R) = C(R)$, então $C_S(R)$ é um anel comutativo.

$(ii) \Leftrightarrow (iii) \Leftrightarrow (v)$ Pelo item (ii) do Lema 4.6.

$(iv) \Rightarrow (v)$ Suponha que $C_S(C(R)) = R$. Queremos mostrar que α é ω-externa em R. Como $C_S(R) \subseteq C_S(C(R)) = R$, então $C_S(R) \subseteq R$. Pelo item (i) do Lema 4.6, sabemos que $C_S(R) = \sum_{g\in G} \phi_g\delta_g$. Daí, $\phi_g = 0$ para todo $1 \neq g \in G$, mostrando que α é ω-externa em R.

Assuma agora que $C_S(C_S(R)) = R$. Vejamos que:

$(i) \Rightarrow (ii)$ Sendo $C_S(R)$ um anel comutativo, então

$$C_S(R) \subseteq C_S(C_S(R)) = R.$$

Logo,

$$C_S(R) = \{x \in S; xr = rx, \text{ para todo } r \in R\} = C(R).$$

$(ii) \Rightarrow (iv)$ Supondo que $C_S(R) = C(R)$, temos

$$C_S(C(R)) = C_S(C_S(R)) = R.$$

■

Observação 4.10 *Se S é H-separável sobre R, então as afirmações do Corolário 4.9 são equivalentes. De fato, observe que R é um somando direto de S como R-bimódulo, já que o produto cruzado parcial S é a soma direta $\oplus_{g\in G} D_g\delta_g$ e $R = R\delta_1 = D_1\delta_1$. O resultado segue pela Proposição 2.47.*

Teorema 4.11 *Suponha que G é finito. Então, $C(R)$ é uma extensão de Galois α-parcial de $C(R)^\alpha$ se, e somente se, S é uma extensão H-separável de R e qualquer uma das condições equivalentes do Corolário 4.9 é válida.*

Demonstração.

($\Rightarrow$) Suponha que G é finito e $C(R)$ é uma extensão de Galois α-parcial de $C(R)^\alpha$. Então, pela Definição 3.25, existem elementos $x_i, y_i \in C(R)$, com $i = 1, 2, \ldots, m$, tais que

$$\sum_{i=1}^{m} x_i\alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g} = \begin{cases} 1_R, & \text{se} \quad g = 1 \\ 0, & \text{se} \quad g \neq 1 \end{cases}.$$

Temos que o conjunto

$$\left\{ x_i, z_i = \sum_{g\in G} \alpha_g(y_i 1_{g^{-1}}) w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}} \mid 1 \leq i \leq m \right\}$$

é um sistema H-separável de S sobre R. De fato, observe que $x_i \in C(R) \subseteq C_S(R)$. Como $y_i \in C(R)$, pelo item (iii) da Proposição 4.7, segue que $z_i \in C_{S\otimes_R S}(S)$, para todo $i = 1, 2, \ldots, m$. Veja que:

$$\begin{aligned} \sum_{i=1}^{m} x_i z_i &= \sum_{g\in G}\sum_{i=1}^{m} x_i\alpha_g(y_i 1_{g^{-1}}) w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}} \\ &= \sum_{g\in G} \delta_{1,g} w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}} \\ &= 1_R 1_R\delta_1 \otimes 1_R\delta_1 \\ &= 1_R\delta_1 \otimes 1_R\delta_1 = 1_S \otimes 1_S. \end{aligned}$$

Assim, S é uma extensão H-separável de R, pelo Teorema 2.44.

Agora, mostraremos que α é ω-externa em R. Seja $r \in \phi_g$, ou seja, $r \in D_g$ e $r\alpha_g(s1_{g^{-1}}) = sr$, para todo $s \in R$. Para todo $1 \neq g \in G$ e $r \in \phi_g$, temos

$$\begin{aligned}
r = r1_R &= r\left(\sum_{i=1}^{m} x_i y_i\right) \\
&= r\left(\sum_{i=1}^{m} x_i(y_i - \alpha_g(y_i 1_{g^{-1}}))\right), \text{ pois } g \neq 1 \text{ e } x_i\alpha_g(y_i 1_{g^{-1}}) = 0 \\
&= \sum_{i=1}^{m} rx_i y_i - rx_i\alpha_g(y_i 1_{g^{-1}}) \\
&= \sum_{i=1}^{m} x_i y_i r - x_i r\alpha_g(y_i 1_{g^{-1}}), \text{ pois } x_i, y_i \in C(R) \\
&= \sum_{i=1}^{m} x_i(y_i r - r\alpha_g(y_i 1_{g^{-1}})) \\
&= \sum_{i=1}^{m} x_i(y_i r - y_i r), \text{ pois } r \in \phi_g \\
&= 0.
\end{aligned}$$

Logo, $\phi_g = 0$ para todo $1 \neq g \in G$ e portanto α é ω-externa em R.

($\Leftarrow$) Suponha que S é uma extensão H-separável de R e qualquer uma das condições equivalentes do Corolário 4.9 é válida. Sendo S uma extensão H-separável de R, pelo Teorema 2.44, existem elementos $x_i \in C_S(R)$ e $y_i \in C_{S\otimes_R S}(S)$, $1 \leq i \leq m$, tais que

$$\sum_{i=1}^{m} x_i y_i = 1_S \otimes 1_S.$$

Pelo Corolário 4.9 (ii), temos que $C_S(R) = C(R)$. Assim, $x_i \in C(R)$. Além disso, pelo mesmo Corolário, sabemos que α é ω-externa em R. Considerando que G é finito, α é ω-externa em R e $y_i \in C_{S\otimes_R S}(S)$, então pelo item (iv) da Proposição 4.7, $y_i = \sum_{g\in G} \alpha_g(r_i 1_{g^{-1}})w^{-1}_{g,g^{-1}}\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}}$, para $r_i \in C(R)$. Temos que $\{x_i, r_i \mid 1 \leq i \leq m\}$ é o sistema de coordenadas de Galois parcial de $C(R)$ sobre $C(R)^\alpha$. De fato, veja que:

$$1_R\delta_1 \otimes 1_R\delta_1 = 1_S \otimes 1_S = \sum_{i=1}^{m} x_i y_i = \sum_{g\in G}\left(\sum_{i=1}^{m} x_i\alpha_g(r_i 1_{g^{-1}})w^{-1}_{g,g^{-1}}\right)\delta_g \otimes 1_{g^{-1}}\delta_{g^{-1}}.$$

Para $g = 1$, temos

$$\sum_{g\in G} x_i r_i 1_R\delta_1 \otimes 1_R\delta_1 = 1_R\delta_1 \otimes 1_R\delta_1.$$

E assim $\sum_{g\in G} x_i r_i = 1_R$. Para todo $1 \neq g \in G$, devemos ter $\sum_{i=1}^{m} x_i\alpha_g(r_i 1_{g^{-1}})w_{g,g^{-1}} = 0$. Como $w_{g,g^{-1}}$ é um elemento inversível em D_g, então $\sum_{i=1}^{m} x_i\alpha_g(r_i 1_{g^{-1}}) = 0$.

Portanto, $\sum_{i=1}^{m} x_i r_i = 1_R$ e $\sum_{i=1}^{m} x_i\alpha_g(r_i 1_{g^{-1}}) = 0$ para todo $1 \neq g \in G$. ∎

4.2 Propriedade de Azumaya

Nesta seção, R, G, α são considerados como na anterior, ou seja, R é um anel, G é um grupo, $\alpha = (\{D_g\}_{g\in G}, \{\alpha_g\}_{g\in G}, \{w_{g,h}\}_{(g,h)\in G\times G})$ é uma ação parcial torcida de G em R, e $S = R \rtimes_{\alpha,\omega} G$ é o correspondente produto cruzado parcial.

A primeira proposição é, de fato, uma consequência imediata da Proposição 2.51.

Proposição 4.12 *As seguintes afirmações são equivalentes:*

(i) S *é Azumaya e* $C(S) \subseteq R$*;*

(ii) S *é uma extensão H-separável de* R *e* R *é uma extensão separável de* $C(R)^\alpha$*.*

Demonstração.

$(i) \Leftrightarrow (ii)$ Como $R \simeq R\delta_1 = D_1\delta_1$ e $S = \bigoplus_{g\in G} D_g\delta_g$, então R é um somando direto de S e S é um R-bimódulo livre de base G, e pela Observação 1.40, um R-módulo projetivo. Além disso, temos que $C(S) \cap R = C(R)^\alpha$. De fato, seja $x \in C(S) \cap R$. Já que $C(S) \subseteq C_S(R)$, segue que $x \in C_S(R)$, ou seja, x comuta com os elementos de R, logo $x \in C(R)$. Ademais, para todo $g \in G$, temos $x(1_g\delta_g) = (1_g\delta_g)x$ e assim

$$x1_g\delta_g = \alpha_g(x1_{g^{-1}})\delta_g.$$

Logo, $x \in C(R)^\alpha$. Por outro lado, considere $x \in C(R)^\alpha$, então $x \in C(R)$ e $\alpha_g(x1_{g^{-1}}) = x1_g$. Em particular, $x \in R$. Para $s = \sum_{g\in G} r_g\delta_g \in S$, temos

$$\begin{aligned} sx &= \sum_{g\in G}(r_g\delta_g)(x\delta_1) = \sum_{g\in G} r_g\alpha_g(x1_{g^{-1}})\delta_g = \sum_{g\in G} r_gx1_g\delta_g \\ &= \sum_{g\in G} xr_g\delta_g = (x\delta_1)\sum_{g\in G} r_g\delta_g = xs. \end{aligned}$$

Como s foi tomado de forma arbitrária em S, então $x \in C(S)$ e portanto $x \in C(S) \cap R$, provando a igualdade. Portanto, o resultado segue da Proposição 2.51. ∎

Para os nossos próximos resultados, vamos supor que G é finito. Note que se substituirmos $C(S) \subseteq R$ por $C_S(R) \subseteq R$ na condição (i) da Proposição 4.12, obtemos mais. Antes de provarmos isso, vejamos o seguinte resultado.

Lema 4.13 *[14,* Proposição 2.5*]* *Sejam* A *um anel,* B *e* T *subanéis de* A *tais que* $B \supseteq T$*. Se* A *é uma extensão separável de* T*, então* A *é uma extensão separável de* B*.*

Demonstração. Suponha que A é uma extensão separável de T. Então, existe um elemento $x = \sum_i a_i \otimes b_i \in C_{A\otimes_T A}(A)$ tal que $\sum_i a_i b_i = 1$. Defina $\varphi : A \otimes_T A \to A \otimes_B A$ por $\varphi\big(\sum_i \alpha_i \otimes_T \beta_i\big) = \sum_i \alpha_i \otimes_B \beta_i$. Considere $\sum_i \alpha_i \otimes \beta_i \in A \otimes_T A$ e $a \in A$. Temos:

$$\varphi\Big(a\sum_i \alpha_i \otimes \beta_i\Big) = \varphi\Big(\sum_i a\alpha_i \otimes \beta_i\Big) = \sum_i a\alpha_i \otimes \beta_i = a\sum_i \alpha_i \otimes \beta_i = a\varphi\Big(\sum_i \alpha_i \otimes \beta_i\Big).$$

Analogamente, mostra-se que $\varphi\big(\big(\sum_i \alpha_i \otimes \beta_i\big)a\big) = \varphi\big(\sum_i \alpha_i \otimes \beta_i\big)a$. Assim, φ é um homomorfismo de A-bimódulos. Além disso, $\varphi(x) \in A \otimes_B A$ satisfaz as condições de separabilidade de A sobre B. De fato, para todo $a \in A$, temos

$$\begin{aligned} a\varphi(x) &= \varphi(ax), \text{ pois } \varphi \text{ é um homomorfismo de } A\text{-bimódulos;} \\ &= \varphi(xa), \text{ pois } x \in C_{A\otimes_T A}(A); \\ &= \varphi(x)a, \text{ pois } \varphi \text{ é um homomorfismo de } A\text{-bimódulos.} \end{aligned}$$

Logo, $\varphi(x) \in C_{A\otimes_B A}(A)$. Como $\sum_i a_i b_i = 1$, por hipótese, temos que A é uma extensão separável de B. ∎

Proposição 4.14 *As seguintes afirmações são equivalentes:*

(i) S *é Azumaya e* $C_S(R) \subseteq R$*;*

(ii) S *é uma extensão H-separável de* R*,* R *é uma extensão separável de* $C(R)^\alpha$ *e* α *é* ω*-externa em* R*;*

(iii) R *é Azumaya e* $C(R)$ *é uma extensão de Galois* α*-parcial de* $C(R)^\alpha$*.*

Demonstração.

$(i) \Leftrightarrow (ii)$ Note que $C(S) \subseteq C_S(R)$. Pela Proposição 4.12, S é Azumaya e $C(S) \subseteq C_S(R) \subseteq R$ se, e somente se, S é uma extensão H-separável de R e R é uma extensão separável de $C(R)^\alpha$. Pelo Lema 4.6 (ii), $C_S(R) \subseteq R$ se, e somente se, α é ω-externa em R.

$(ii) \Rightarrow (iii)$ Como S é uma extensão H-separável de R e α é ω-externa em R, pelo Teorema 4.11, $C(R)$ é uma extensão de Galois α-parcial de $C(R)^\alpha$. Além disso, temos que $C(R)$ e $C(R)^\alpha$ são subanéis de R tais que $C(R) \supseteq C(R)^\alpha$. Sendo R uma extensão separável de $C(R)^\alpha$, segue pelo Lema 4.13 que R é separável sobre $C(R)$ e portanto R é Azumaya.

$(iii) \Rightarrow (ii)$ Como $C(R)$ é uma extensão de Galois α-parcial de $C(R)^\alpha$, pelo Teorema 4.11, S é uma extensão H-separável de R e α é ω-externa em R. Além disso, $C(R)$ é separável sobre $C(R)^\alpha$, pelo Teorema 3.28. Já que R é separável sobre $C(R)$ e $C(R)$

é separável sobre $C(R)^\alpha$, pela transitividade da separabilidade (Proposição 2.15), temos que R é separável sobre $C(R)^\alpha$. ■

Se supormos que R é comutativo e α é ω-externa em R, então temos as seguintes equivalências.

Proposição 4.15 *Suponha que R é comutativo e α é ω-externa em R. Então, as seguintes afirmações são equivalentes:*

(i) S é Azumaya;

(ii) S é uma extensão H-separável de R;

(iii) R é uma extensão de Galois α-parcial de R^α.

Demonstração.

$(i) \Rightarrow (ii)$ Suponha que S é Azumaya. Como α é ω-externa em R, então pelo Lema 4.6 (ii), $C_S(R) \subseteq R$. Pela Proposição 4.12, temos que S é uma extensão H-separável de R.

$(ii) \Rightarrow (i)$ Suponha que S é uma extensão H-separável de R. Pela Proposição 2.48, temos que $C_S(R)$ é uma extensão separável de $C(S)$. Como α é ω-externa em R, pelo Lema 4.6 (ii), então $C_S(R) = C(R)$ e $C(S) = C(R)^\alpha$. Logo, $C(R)$ é uma extensão separável de $C(R)^\alpha$. Como R é comutativo, $R = C(R)$ e daí R é uma extensão separável de $C(R)^\alpha$. Aplicando a Proposição 4.12, temos que S é Azumaya.

$(ii) \Leftrightarrow (iii)$ Observe que $C(R) = R$ e α é ω-externa em R. Logo, o resultado segue pelo Teorema 4.11. ■

Vamos considerar R como um (S, R^α)-bimódulo com a estrutura natural, ou seja, $r_g\delta_g \cdot r = r_g\alpha_g(r1_{g^{-1}})$ e $r \cdot r' = rr'$, para todo $r_g \in D_g, r \in R$ e $r' \in R^\alpha$.

Lema 4.16 *[20,* Proposição 5.1.2] *A aplicação $\theta : R^\alpha \to End_S(R)$, definida por $\theta(a) = \theta_a$, onde $\theta_a(x) = xa$,para todo $x \in R$, é um isomorfismo de anéis.*

Demonstração. Defina $\theta : R^\alpha \to End_S(R)$, tomando para cada $a \in R^\alpha$, $\theta_a : R \to R$, onde $\theta_a(x) = xa$, para todo $x \in R$ (multiplicação à direita). Para ver que $\theta_a \in End_S(R)$, é suficiente verificar que θ_a é S-linear à esquerda. Para $r_g \in D_g$ e $r \in R$, temos:

$$\begin{aligned}
\theta_a((r_g\delta_g)r) = \theta_a(r_g\alpha_g(r1_{g^{-1}})) &= r_g\alpha_g(r1_{g^{-1}})a \\
&= r_g\alpha_g(r1_{g^{-1}})1_g a \\
&= r_g\alpha_g(r1_{g^{-1}})\alpha_g(a1_{g^{-1}}), \text{ pois } a \in R^\alpha \\
&= r_g\alpha_g(ra1_{g^{-1}}) \\
&= (r_g\delta_g)(ra) = (r_g\delta_g)\theta_a(r).
\end{aligned}$$

Assim, $\theta_a \in End_S(R)$, o que mostra que a aplicação θ está bem-definida. É fácil ver que θ é um homomorfismo de anéis. Defina

$$\begin{array}{rccc} \theta': & End_S(R) & \to & R^\alpha \\ & f & \mapsto & f(1_R) \end{array}.$$

Vejamos que θ' está bem-definida, ou seja, $f(1_R) \in R^\alpha$. Como f é S-linear à esquerda, temos:

$$\begin{aligned} \alpha_g(f(1_R)1_{g^{-1}}) &= (1_g\delta_g)(f(1_R)) = f((1_g\delta_g)1_R) \\ &= f(1_g\alpha_g(1_R1_{g^{-1}})) \\ &= f(1_g\alpha_g(1_{g^{-1}})) \\ &= f(\alpha_g((1_{g^{-1}})\delta_1)1_R) \\ &= (\alpha_g((1_{g^{-1}})\delta_1)f(1_R) \\ &= (1_g\delta_1)(f(1_R)) = 1_gf(1_R). \end{aligned}$$

Logo, $f(1_R) \in R^\alpha$. Para $f \in End_S(R), r \in R$ e $a \in R^\alpha$, temos:

$$\begin{aligned} \theta \circ \theta'(f)(r) &= \theta(\theta'(f))(r) = \theta(f(1_R))(r) \\ &= \theta_{f(1_R)}(r) = rf(1_R) = (r\delta_1)f(1_R) \\ &= f((r\delta_1)1_R) = f(r1_R) = f(r). \end{aligned}$$

Assim, $\theta \circ \theta' = I_{End_S(R)}$. Por outro lado,

$$\theta' \circ \theta(a) = \theta'(\theta(a)) = \theta(a)(1_R) = \theta_a(1_R) = 1_Ra = a.$$

Assim, $\theta' \circ \theta = I_{R^\alpha}$. Ou seja, θ' é a inversa de θ. Portanto, $R^\alpha \backsimeq End_S(R)$. ∎

Na última proposição, considerando o anel de grupo skew parcial, consegue-se determinar o centro de S.

Proposição 4.17 *Suponha que R é comutativo e $w_{g,h} = 1_g1_{gh}$ para todo $g, h \in G$. Então, as seguintes afirmações são equivalentes:*

(i) S é Azumaya com centro R^α;

(ii) S é uma extensão H-separável de R;

(iii) R é uma extensão de Galois α-parcial de R^α.

Demonstração.

$(i) \Rightarrow (ii)$ Como $R \simeq R\delta_1 = D_1\delta_1$ e $S = \bigoplus_{g\in G} D_g\delta_g$, então R é um somando direto de S e S é um R-bimódulo livre de base G, e pela Observação 1.40, um R-módulo projetivo. Como G é finito, S é um R-módulo projetivo e finitamente gerado. Além disso, sendo S Azumaya e $S \supset R \supset R^\alpha$, segue que S é uma extensão H-separável de R, pelo Teorema 2.49.

$(ii) \Rightarrow (iii)$ Suponha que S é uma extensão H-separável de R. Sabemos que R é um S-módulo á esquerda com unidade 1_R. Como ${}_RR$ é um gerador, então pela Proposição 2.50, ${}_SR$ também é um gerador. Pelo Lema 4.16, vimos que $R^\alpha \backsimeq End_S(R)$. Como R é um gerador para a categoria dos S-módulos à esquerda, pela Proposição B.5, concluímos que R é um R^α-módulo projetivo e finitamente gerado e a aplicação $\varphi : S \to End_{R^\alpha}(R)$ dada por $\varphi(r_g\delta_g)(r) = r_g\alpha_g(r1_{g^{-1}})$, para todo $g \in G, r_g \in D_g$ e $r \in R$, é um isomorfismo. Agora, vamos verificar que φ é um isomorfismo de anéis e R^α-módulos. Sejam $r_g \in D_g, r' \in R^\alpha$ e $r \in R$. Temos:

$$\begin{aligned}\varphi((r')(r_g\delta_g))(r) &= \varphi((r'\delta_1)(r_g\delta_g))(r) = \varphi(rr_g\delta_g)(r)\\ &= r'r_g\alpha_g(r1_{g^{-1}}) = r'\varphi(r_g\delta_g)(r).\end{aligned}$$

Ou seja, φ é R^α-linear. Por outro lado, considerando $r_g \in D_g, r_h \in D_h$ e $r \in R$, temos:

$$\begin{aligned}[\varphi(r_g\delta_g)\varphi(r_h\delta_h)](r) &= \varphi(r_g\delta_g)(r_h\alpha_h(r1_{h^{-1}})) = r_g\alpha_g(r_h\alpha_h(r1_{h^{-1}})1_{g^{-1}})\\ &= r_g\alpha_g(r_h1_{g^{-1}})\alpha_g(\alpha_h(r1_{h^{-1}})1_{g^{-1}}) = r_g\alpha_g(r_h1_{g^{-1}})\alpha_g(\alpha_h(r1_{h^{-1}}1_{(gh)^{-1}}))\\ &= r_g\alpha_g(r_h1_{g^{-1}})\alpha_{gh}(r1_{h^{-1}}1_{(gh)^{-1}}) = r_g\alpha_g(r_h1_{g^{-1}})\alpha_{gh}(r1_{(gh)^{-1}})\alpha_{gh}(1_{h^{-1}}1_{(gh)^{-1}})\\ &= r_g\alpha_g(r_h1_{g^{-1}})\alpha_{gh}(r1_{(gh)^{-1}}) = \varphi(r_g\alpha_g(r_h1_{g^{-1}})\delta_{gh})(r)\\ &= \varphi((r_g\delta_g)(r_h\delta_h))(r).\end{aligned}$$

Logo, φ é um isomorfismo de anéis e também de R^α-módulos. Portanto, pelo Teorema 3.27 (ii), R é uma extensão de Galois α-parcial de R^α.

$(iii) \Rightarrow (i)$ Suponha que R é uma extensão de Galois α-parcial de R^α. Pelo Teorema 3.27 (ii), R é um R^α-módulo projetivo e finitamente gerado e $S \backsimeq End_{R^\alpha}(R)$. Como R é comutativo e R é um R^α-módulo fiel, então R é um R^α-progerador (Corolário 1.52). Logo, pela Proposição 2.27, $S = End_{R^\alpha}(R)$ é Azumaya de centro R^α.

■

Apêndice A

Categoria e Funtores de módulos: funtor produto tensorial e funtor Hom

Seja R um anel. Vamos denotar por ${}_R\mathcal{M}$ a categoria dos R-módulos à esquerda, isto é, os objetos são os R-módulos à esquerda e os morfismos são todos os homomorfismos de R-módulos à esquerda. O produto é a composição de aplicações. Da mesma forma, $\mathcal{M}_R$ denotará a categoria de todos os R-módulos à direita e R-homomorfismos.

Para qualquer anel R, denotamos por R^o o anel cujo grupo abeliano é o mesmo que o de R, mas cuja a multiplicação é dada por $a * b = ba$, onde ba é o produto em R. R^o é chamado de anel oposto de R. Claramente um R-módulo à esquerda M pode ser dado uma estrutura de R^o à direita definindo

$$m \cdot r = rm, \quad \forall r \in R, m \in M.$$

Em particular, se R é um anel comutativo, então $R = R^o$ e qualquer R-módulo pode ser considerado como um R-módulo à direita e à esquerda. Consequentemente, quando R é comutativo, temos ${}_R\mathcal{M} = \mathcal{M}_R$.

Agora, vejamos as duas definições a seguir: funtor covariante e funtor exato.

Definição A.1 *Um funtor covariante de uma categoria de módulos $\mathcal{C}$ em uma categoria de módulos $\mathcal{D}$ é uma correspondência F que associa para todo módulo M em $\mathcal{C}$ um módulo $F(M)$ em $\mathcal{D}$ e que associa para todo homomorfismo $f : M \to N$ em $\mathcal{C}$ um homomorfismo $F(f) : F(M) \to F(N)$ tal que para todo M em $\mathcal{C}$*

(i) $F(I_M) = I_{F(M)}$;

(ii) se f, g são homomorfismos em $\mathcal{C}$ tal que fg está definida, então $F(fg) = F(f)F(g)$.

Definição A.2 *Um funtor F de uma categoria $\mathcal{C}$ para uma categoria $\mathcal{D}$ é dito exato à esquerda se para toda sequência exata de módulos e aplicações*

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0 \tag{A.1}$$

em $\mathcal{C}$,

$$0 \longrightarrow F(L) \longrightarrow F(M) \longrightarrow F(N)$$

é exata em $\mathcal{D}$. Analogamente, F é dito exato à direita se (A.1) sempre fornece uma sequência

$$F(L) \longrightarrow F(M) \longrightarrow F(N) \longrightarrow 0$$

exata em $\mathcal{D}$.

Um funtor é dito exato se é exato à esquerda e à direita.

Estamos interessados nos funtores produto tensorial e o conjunto de todos os homomorfismos de um módulo fixo em outro módulo. Agora, vamos ver as principais propriedades desses conceitos.

A.0.1 Funtor produto tensorial

O conceito de produto tensorial de módulos é uma generalização de um antigo conceito de espaços vetoriais que tem desempenhado papel importante há bastante tempo em vários ramos da matemática, como geometria diferencial e teoria da representação, de acordo com [19].

Seja R um anel. Dado um R-módulo à direita M e um R-módulo à esquerda N, vamos formar o produto tensorial $M \otimes_R N$, considerando o grupo abeliano livre $\mathbb{Z}^{M\times N}$ indexado pelo produto cartesiano $M \times N$ e então fazendo o quociente pelo subgrupo $\mathcal{R}$ gerado por todos os elementos da forma:

$$b_{(m+m',n)} - b_{(m,n)} - b_{(m',n)}, \tag{A.2}$$

$$b_{(m,n+n')} - b_{(m,n)} - b_{m,n'}, \tag{A.3}$$

$$b_{(m\cdot r,n)} - b_{(m,r\cdot n)}, \tag{A.4}$$

onde $m, m' \in M, n, n' \in N$ e $r \in R$ e $b_{(m,n)}$ denota o elemento da base de $\mathbb{Z}^{M\times N}$ determinado por (m, n). Vamos denotar a classe

$$b_{(m,n)} + \mathcal{R} = m \otimes n.$$

Como os elementos (A.2), (A.3) e (A.4) pertencem a $\mathcal{R}$, temos que as classes satisfazem

$$(m + m') \otimes n = m \otimes n + m' \otimes n,$$
$$a \otimes (n + n') = a \otimes n + a \otimes n',$$
$$(m \cdot r) \otimes n = m \otimes r \cdot n,$$

para todo $m, m' \in M, n, n' \in N$ e $r \in R$.

Observa-se que um elemento típico de $M \otimes_R N$ é da forma

$$\sum_{i=1}^{k} m_i \otimes n_i$$

e que não necessariamente pode ser representado por um monômio $m \otimes n$.

Sejam M um R-módulo à direita e N um R-módulo à esquerda. $M \otimes_R N$ satisfaz uma propriedade que se G é um grupo abeliano e $f : M \times N \to G$ é uma aplicação R-balanceada, ou seja,

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

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

(iii) $f(m \cdot r, n) = f(m, r \cdot n)$,

para todo $m, m' \in M, n, n' \in N$ e $r \in R$, então existe um único homomorfismo $f^* : M \otimes_R N \to G$ com $f^*(m \otimes n) = f(m, n)$, para todo $m \in M$ e $n \in N$. Essa propriedade é conhecida como Propriedade Universal do produto tensorial e será usada para provar a boa definição de determinadas aplicações.

Sejam R e S anéis. Dizemos que um grupo abeliano M é um (R, S)-bimódulo à esquerda se M é um R-módulo à esquerda e um S-módulo à esquerda tal que

$$r \cdot (s \cdot m) = s \cdot (r \cdot m),$$

para $r \in R, s \in S$ e $m \in M$. Vamos denotar por ${}_{R-S}\mathcal{M}$ a categoria de todos os (R, S)-bimódulos à esquerda, onde os morfismos da categoria são aplicações que são R-homomorfismos e S-homomorfismos. Analogamente, definimos a categoria $\mathcal{M}_{R-S}$ de (R, S)-bimódulos à direita e a categoria ${}_R\mathcal{M}_S$ de (R, S)-bimódulos (R-módulo à esquerda e S-módulo à direita).

Até agora, $M \otimes_R N$ tem apenas uma estrutura de grupo abeliano. Entretanto, sobre certas condições, podemos dar a $M \otimes_R N$ uma estrutura de módulo. Por exemplo, se $N \in {}_R\mathcal{M}_S$, então $M \otimes_R N$ torna-se um S-módulo à direita através da operação

$$\left(\sum_{i=1}^{k} m_i \otimes n_i\right) \cdot s = \sum_{i=1}^{k} m_i \otimes (n_i s).$$

Observe que esta operação está bem definida, pois N tem uma estrutura de S-módulo à direita. O mesmo pode ser feito se $M \in {}_S\mathcal{M}_R$, $M \in \mathcal{M}_{R-S}$ e $N \in {}_{R-S}\mathcal{M}$. Em particular, vemos que se R é comutativo, então todo R-módulo é visto como um $(R-R)$-bimódulo (de todas as maneiras possíveis) e assim $M \otimes_R N$ tem uma estrutura de R-módulo.

A seguir, trazemos algumas propriedades do produto tensorial, que podem ser encontradas em [9].

(a) Para qualquer anel R e quaisquer R-módulos à direita M e à esquerda N, $M \otimes_R N \simeq N \otimes_{R^o} M$ sobre a aplicação $m \otimes n \mapsto n \otimes m$. Se R é comutativo, então $M \otimes_R N \simeq N \otimes_R M$ como um R-módulo.

(b) (Associatividade) Para quaisquer anéis R e S e $L \in \mathcal{M}_R, M \in {}_R\mathcal{M}_S$ e $N \in {}_S M$, temos

$$(L \otimes_R M) \otimes_S N \simeq L \otimes_R (M \otimes_S N)$$

sob a aplicação $(l \otimes m) \otimes n \mapsto l \otimes (m \otimes n)$, onde $L \otimes_R M$ é um S-módulo e $M \otimes_S N$ é um R-módulo devido a estrutura de bimódulo de M.

(c) Para qualquer anel R e qualquer $M \in {}_R\mathcal{M}$, $R \otimes_R M \simeq M$ sobre a aplicação $r \otimes m \mapsto rm$. Da mesma forma, para $M \in \mathcal{M}_R$, $M \otimes_R R \simeq M$.

(d) Para $M, M' \in \mathcal{M}_R, N, N' \in {}_R\mathcal{M}, f \in Hom_R(M, M')$ e $g \in Hom_R(N, N')$ existe um homomorfismo $f \otimes g \in Hom_R(M \otimes_R N, M' \otimes_R N')$ dado por

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n).$$

(e) Sejam $\{M_i\}_{i \in I}$ uma coleção de R-módulos à direita e $\{N_j\}_{j \in J}$ uma coleção de R-módulos à esquerda. Então, temos

$$\bigoplus_{i \in I} M_i \otimes \bigoplus_{j \in J} N_j \simeq \bigoplus_{i,j} (M_i \otimes N_j).$$

Dado $M \in {}_R\mathcal{M}$, podemos definir um funtor $(\quad) \otimes_R M : \mathcal{M}_R \to {}_{\mathbb{Z}}\mathcal{M}$ por:

(i) Dado $N \in \mathcal{M}_R$, temos $N \otimes_R M \in {}_{\mathbb{Z}}\mathcal{M}$.

(ii) Sejam $N, N' \in \mathcal{M}_R$ e $f \in Hom_R(N, N')$, então

$$\begin{array}{rccc} f \otimes m : & N \otimes_R M & \to & N' \otimes_R M \\ & n \otimes m & \mapsto & f(n) \otimes m \end{array}.$$

A.0.2 Funtor Hom

Seja R um anel e M e N R-módulos. Vamos denotar por $Hom_R(M, N)$ o conjunto de todas as funções $f : M \to N$ tais que

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

(ii) $f(r \cdot m) = r \cdot f(m)$,

para todo $m, m' \in M$ e $r \in R$. Temos que $Hom_R(M, N)$ tem uma estrutura de grupo abeliano sob a operação

$$(f + g)(m) = f(m) + g(m),$$

para todo $f, g \in Hom_R(M, N)$ e $m \in M$.

Além disso, se M ou N é um bimódulo, por exemplo $M \in {}_R\mathcal{M}_S$, então $Hom_R(M, N)$ pode ser dotado com uma estrutura de S-módulo pela operação

$$(s \cdot f)(m) = f(m \cdot s),$$

para todo $s \in S$, $m \in M$ e $f \in Hom_R(M, N)$. Quando R é comutativo, todo R-módulo pode ser considerado como um (R, R)-bimódulo, então $Hom_R(M, N)$ torna-se um R-módulo. Quando $M = N$ a composição de funções de elementos de $Hom_R(M, M)$ serve como uma multiplicação sobre a qual $Hom_R(M, M)$ torna-se um anel. Assim, quando R é comutativo, $Hom_R(M, M)$ tem uma estrutura de R-álgebras.

Para qualquer R-módulo fixado M e qualquer homomorfismo f de um R-módulo N para um R-módulo N' temos a aplicação $Hom_R(I_M, f) : Hom_R(M, N) \to Hom_R(M, N')$ dada por

$$Hom_R(I_M, f)(g) = fgI_M = fg.$$

É imediato verificar que $Hom_R(M, \quad)$ pode ser visto como um funtor de ${}_R\mathcal{M}$ para ${}_{\mathbb{Z}}\mathcal{M}$. As seguintes propriedades fundamentais de $Hom_R(M, \quad)$ são facilmente verificadas e podem ser vistas em [9].

Proposição A.3 *Temos as seguintes propriedades:*

(a) $Hom_R(M, \quad)$ *é um funtor exato à esquerda e é exato se, e somente se,* M *é* R*-projetivo.*

(b) Para $M_1, M_2, \ldots, M_n, N_1, N_2, \ldots, N_k$ R*-módulos, temos*

$$Hom_R\left(\bigoplus_{i=1}^{n} M_i, \bigoplus_{j=1}^{k} N_j\right) = \bigoplus_{i,j} Hom_R(M_i, N_j).$$

(c) $Hom_R(M, R) \simeq M$ *sobre a aplicação* $f \mapsto f(1)$.

Apêndice B

Teoria de Morita

Sejam $\mathcal{C}$ e $\mathcal{D}$ categorias de módulos e suponha que temos dois funtores T e T' de $\mathcal{C}$ em $\mathcal{D}$. Dizemos que T e T' são naturalmente equivalentes se para todo módulo M em $\mathcal{C}$ existe um isomorfismo φ_M em $Hom_{\mathcal{D}}(T(M), T'(M'))$ tal que para todo par de módulos M e N em $\mathcal{C}$ e qualquer $f \in Hom_{\mathcal{C}}(M, N)$ o diagrama

$$\begin{array}{ccc} T(M) & \xrightarrow{T(f)} & T(N) \\ {\scriptstyle \varphi_M}\downarrow & & \downarrow{\scriptstyle \varphi_N} \\ T'(M) & \xrightarrow[T'(f)]{} & T'(N) \end{array}$$

comuta. Vamos denotar por $I_{\mathcal{C}}$ o funtor identidade sobre a categoria $\mathcal{C}$ definido por $I_{\mathcal{C}}(M) = M$ e $I_{\mathcal{C}}(f) = f$, para módulos M e aplicações f.

Dizemos que duas categorias $\mathcal{C}$ e $\mathcal{D}$ são *equivalentes* se existem funtores $F : \mathcal{C} \to \mathcal{D}$ e $G : \mathcal{D} \to \mathcal{C}$ tal que $F \circ G$ é naturalmente equivalente a $I_{\mathcal{D}}$ e $G \circ F$ é naturalmente equivalente a $I_{\mathcal{C}}$. Dizemos que F e G são inversos equivalentes.

Vamos mostrar que $\mathcal{M}_R$ e ${}_S\mathcal{M}$ são categorias equivalentes quando S é o anel de endomorfismos de algum R-progerador. Essa equivalência e suas consequências são conhecidas como Teoremas de Morita e dizemos que R e S são Morita equivalentes.

Antes disso, vejamos o seguinte resultado geral de categorias.

Proposição B.1 *Sejam $\mathcal{C}$ e $\mathcal{D}$ categorias equivalentes de módulos com inversas equivalentes $F : \mathcal{C} \to \mathcal{D}$ e $G : \mathcal{D} \to \mathcal{C}$. Então, para quaisquer objetos L e L' em $\mathcal{C}$, o homomorfismo*

$$\begin{array}{ccc} Hom_{\mathcal{C}}(L, L') & \to & Hom_{\mathcal{D}}(F(L), F(L')) \\ g & \mapsto & F(g) \end{array}$$

é injetor e sobrejetor.

Demonstração. [9, Proposição 3.1]. ∎

Para qualquer anel R e qualquer R-módulo M, seja $M^* = Hom_R(M, R)$ e $S = End_R(M)$. Como R é um (R, R)-bimódulo, então M^* é um R-módulo à direita sob a operação

$$(f \cdot r)(m) = f(m)r.$$

Além disso, M é um S-módulo à esquerda com a operação

$$s \cdot m = s(m).$$

Sobre essas operações M é um (R, S)-bimódulo à esquerda e assim M^* torna-se um S-módulo à direita sobre a operação

$$(f \cdot s)(m) = f(s(m)).$$

Assim, M^* é um (R, S)-bimódulo à direita. Logo, podemos formar $M^* \otimes_R M$ e $M^* \otimes_S M$. Além disso, $M^* \otimes_R M$ é um (S, S)-bimódulo, onde

$$s \cdot (f \otimes m) = f \otimes s \cdot m = f \otimes s(m) \quad \text{e} \quad (f \otimes m) \cdot s = fs \otimes m.$$

Analogamente, temos que $M^* \otimes_S M$ é um (R, R)-bimódulo, onde:

$$r \cdot (f \otimes m) = f \otimes rm \quad \text{e} \quad (f \otimes m) \otimes r = f \cdot r \otimes m.$$

Seja θ_R a aplicação de $M^* \otimes_R M$ para S dada por $\theta_R(\sum_i f_i \otimes m_i)(m) = \sum_i f_i(m)m_i$. Vejamos que θ_R é um S-homomorfismo de módulos à direita e à esquerda. De fato, sejam $s \in S$ e $x = \sum_i f_i \otimes m_i \in M^* \otimes_R M$, então para todo $m \in M$,

$$\theta_R\Big(s \cdot \sum_i f_i \otimes m_i\Big)(m) = \theta_R\Big(\sum_i f_i \otimes s(m_i)\Big)(m) = \sum_i f_i(m)s(m_i).$$

Por outro lado,

$$s \cdot \theta_R\Big(\sum_i f_i \otimes m_i\Big)(m) = s \cdot \Big(\sum_i f_i(m)m_i\Big) = s\Big(\sum_i f_i(m)m_i\Big) = \sum_i f_i(m)s(m_i),$$

pois s é R-linear à esquerda. Logo, θ_R é um homomorfismo de S-módulos à esquerda. Além disso, para todo $m \in M$

$$\theta_R\Big(\sum_i f_i \otimes m_i \cdot s\Big)(m) = \theta_R\Big(\sum_i f_i s \otimes m_i\Big)(m) = \sum_i^n f_i(s(m))m_i.$$

Por outro lado,

$$\left[\theta_R\left(\sum_i f_i \otimes m_i\right)\cdot s\right](m) = \theta_R\left(\sum_i f_i \otimes m_i\right)(s(m)) = \sum_i f_i(s(m))m_i.$$

Logo, θ_R é um homomorfismo de S-módulos à direita.

Considere agora θ_S a aplicação de $M^* \otimes_S M$ para R dada por

$$\theta_S\left(\sum_i f_i \otimes m_i\right) = \sum_i f_i(m_i).$$

Temos que θ_S é um R-homomorfismo de módulos à direita e à esquerda. De fato, sejam $r \in R$ e $f_i \otimes m_i \in M^* \otimes_S M$, então

$$\begin{aligned}\theta_S\left(r \cdot \sum_i f_i \otimes m_i\right) &= \theta_S\left(\sum_i f_i \otimes rm_i\right) = \sum_i f_i(rm_i)\\ &= r\sum_i f_i(m_i) = r\theta_S\left(\sum_i f_i \otimes m_i\right).\end{aligned}$$

Isso mostra que θ_S é um R-homomorfismo de módulos à esquerda. Agora, veja que:

$$\begin{aligned}\theta_S\left(\sum_i f_i \otimes m_i \cdot r\right) &= \theta_S\left(\sum_i f_i \cdot r \otimes m_i\right) = \sum_i (f_i \cdot r)(rm_i)\\ &= \sum_i f_i(m_i)r = \theta_S\left(\sum_i f_i \otimes m_i\right)r.\end{aligned}$$

Logo, θ_S é um R-homomorfismo de módulos à direita. Ademais, a imagem do homomorfismo θ_S é o ideal traço $\mathcal{T}_R(M)$.

Lema B.2 *(i) θ_R é sobrejetor se, e somente se, M é finitamente gerado e projetivo. Se θ_R é sobrejetor, então θ_R é injetor.*

(ii) θ_S é sobrejetor se, e somente se, M é um gerador. Se θ_S é sobrejetor, então θ_S é injetor.

Demonstração. [9, Lema 3.2]. ∎

Como visto acima, para qualquer R-módulo M, podemos ver M como um (R,S)-bimódulo à esquerda e $M^* = Hom_R(M,R)$ como um (R,S)-bimódulo à direita, onde $S = End_R(M)$. Assim, para qualquer R-módulo à direita L, $L \otimes_R M$ tem uma estrutura de S-módulo à esquerda, e para qualquer S-módulo à esquerda N, $M^* \otimes_S N$ tem uma estrutura de R-módulo à direita. Assim, temos funtores $(\quad) \otimes_R M : \mathcal{M}_R \to {}_S\mathcal{M}$ e $M^* \otimes (\quad) : {}_S\mathcal{M} \to \mathcal{M}_R$.

Proposição B.3 *Sejam R um anel qualquer e M um R-progerador. Se $S = End_R(M)$ e $M^* = Hom_R(M, R)$, então*

$$(\quad) \otimes_R M : \mathcal{M}_R \to {}_S\mathcal{M} \quad e \quad M^* \otimes_S (\quad) : {}_S\mathcal{M} \to \mathcal{M}_R$$

são inversas equivalentes.

Demonstração. Seja L um objeto de $\mathcal{M}_R$. Pelas propriedades do produto tensorial e pelo Lema B.2 (b) temos

$$\begin{aligned} M^* \otimes_S (L \otimes_R M) &\simeq M^* \otimes_S (M \otimes_{R^o} L) \simeq (M^* \otimes_S M) \otimes_{R^o} L \\ &\simeq R \otimes_{R^o} L \simeq L \otimes_R R \simeq L, \end{aligned}$$

onde o isomorfismo é dado por

$$f \otimes (l \otimes m) \mapsto l \cdot \theta_S(f \otimes m) = lf(m).$$

Isso permite verificar que a composição dos funtores $(\quad)\otimes_R M$ e $M^*\otimes_S(\quad)$ é naturalmente equivalente ao funtor identidade sobre $\mathcal{M}_R$.

Analogamente, pelo Lema B.2 (a), para qualquer S-módulo à esquerda N, temos

$$\begin{aligned} (M^* \otimes_S N) \otimes_R M &\simeq (N \otimes_{S^o} M^*) \otimes_R M \simeq N \otimes_{S^o} (M^* \otimes_R M) \\ &\simeq N \otimes_{S^o} S \simeq S \otimes_S N \simeq N, \end{aligned}$$

sobre a aplicação $(f \otimes n) \otimes m \mapsto \theta_R(f \otimes m)n$. Novamente, isso nos dá que $M^* \otimes_S (\quad)$ e $(\quad) \otimes_R M$ é naturalmente equivalente ao funtor identidade ${}_S\mathcal{M}$. Portanto, $M^* \otimes_S (\quad)$ e $(\quad) \otimes_R M$ são inversas equivalentes. ∎

Corolário B.4 *Com a notação da proposição anterior, temos:*

(i) $R \simeq Hom_S(M, M)$ *(como anéis) sobre a aplicação que associa um elemento $r \in R$ ao endomorfismo de M induzido pela multiplicação por escalar.*

(ii) $M^* \simeq Hom_S(M, S)$ *(como S-módulos à direita) sobre a aplicação que associa a um elemento $f \in M^*$ o homomorfismo $\theta_R(f \otimes (\quad))$ de M em S.*

(iii) $M \simeq Hom_R(M^*, R) \simeq M^{**}$ *(como R-módulos à esquerda) sobre a aplicação que associa um elemento $m \in M$ um elemento em M^{**} que leva $f \in M^*$ a $f(m)$.*

(iv) $S^o \simeq Hom_R(M^*, M^*)$ *(como anéis) sobre a aplicação que associa um elemento $s \in S^o$ a um homomorfismo de M^* em M^* dado por $f \mapsto fs$.*

(v) M *é um S-progerador.*

(vi) M^* *é um* R*-progerador.*

(vii) M^* *é um* S*-progerador.*

Demonstração. [9, Proposição 3.3]. ■

Proposição B.5 *Sejam* M *um* A*-módulo à direita e* $B = End_A(M)$ *e consideremos de modo natural,* M *como um* B*-módulo à esquerda. Então as seguintes afirmações são equivalentes:*

(i) M *é um gerador para a categoria dos* A*-módulos à direita;*

(ii) M *é um* B*-módulo à esquerda, projetivo e finitamente gerado e* $A \simeq End_B(M)$*.*

Demonstração. [20, Teorema 1.5.32]. ■

Referências Bibliográficas

[1] Alfaro, Ricardo, and George Szeto. *Skew group rings which are Azumaya.* Communications in Algebra 23.6 (1995): 2255-2261. 4

[2] Auslander, Maurice, and David A. Buchsbaum. *On ramification theory in noetherian rings.* American Journal of Mathematics 81.3 (1959): 749-765. 2

[3] Auslander, Maurice, and Oscar Goldman. *The Brauer group of a commutative ring.* Transactions of the American Mathematical Society 97.3 (1960): 367-409. 1, 2

[4] Azumaya, Gorô. *On maximally central algebras.* Nagoya mathematical journal 2 (1951): 119-150. 2

[5] Bagio, Dirceu, Joao Lazzarin, and Antonio Paques. *Crossed products by twisted partial actions: separability, semisimplicity, and Frobenius properties.* Communications in Algebra 38.2 (2010): 496-508. 90

[6] Cartan, Henri, and Samuel Eilenberg. *Homological algebra.* Vol. 28. Princeton university press (1999). 22

[7] Carvalho, Paula AAB. *ON THE AZUMAYA LOCUS OF SOME CROSSED PRODUCTS#.* Communications in Algebra® 33.1 (2005): 51-72. 4, 56

[8] Chase, Stephen Urban, David K. Harrison, and Alex Rosenberg. *Galois theory and cohomology of commutative rings.* Vol. 52. American Mathematical Soc. (1969). 2

[9] De Meyer, Frank, and Edward Ingraham. *Separable algebras over commutative rings.* Vol. 181. Springer (2006). 1, 2, 3, 5, 23, 24, 35, 36, 38, 39, 40, 112, 113, 116, 117, 119

[10] Dokuchaev, Michael, and Ruy Exel. *Associativity of crossed products by partial actions, enveloping actions and partial representations.* Transactions of the American Mathematical Society 357.5 (2005): 1931-1952. 2, 57, 62, 64, 65, 66, 67

[11] Dokuchaev, Michael, Miguel Ferrero, and Antonio Paques. *Partial actions and Galois theory.* Journal of Pure and Applied Algebra 208.1 (2007): 77-87. 2, 57, 85

[12] Dokuchaev, Michael, R. Exel, and J. J. Simón. *Crossed products by twisted partial actions and graded algebras.* Journal of Algebra 320.8 (2008): 3278-3310. 2, 3, 57, 69, 70

[13] Exel, Ruy. *Twisted partial actions: a classification of regular C*-algebraic bundles.* Proceedings of the London Mathematical Society 74.2 (1997): 417-443. 2

[14] Hirata, Kazuhiko, and Kozo Sugano. *On semisimple extensions and separable extensions over non commutative rings.* Journal of the Mathematical Society of Japan 18.4 (1966): 360-373. 104

[15] Hirata, Kazuhiko. *Separable extensions and centralizers of rings.* Nagoya Mathematical Journal 35 (1969): 31-45. 52

[16] Hirata, Kazuhiko. *Some types of separable extensions of rings.* Nagoya Mathematical Journal 33 (1968): 107-115. 3, 24, 42, 47, 52

[17] Hungerford, Thomas W. *Algebra.* Vol. 73. Springer Science & Business Media (2012). 19

[18] Ikehata, Shûichi. *Note on Azumaya algebras and H-separable extensions.* Mathematical Journal of Okayama University 23.1 (1981): 17-18. 24, 54, 56

[19] Jacobson, Nathan. *Basic algebra ii, 2a edição.* (2009). 110

[20] Lazzarin, João Roberto. *Ações Parciais de Grupos sobre Anéis: o Skew Anel de Grupo Parcial e o Subanel dos Invariantes.* PhD thesis, UFRGS, Brazil (2006). 106, 119

[21] Paques, Antonio, and Alveri Sant'Ana. *When is a crossed product by a twisted partial action Azumaya?.* Communications in Algebra ® 38.3 (2010): 1093-1103. 3, 4, 88

[22] Paques, Antonio. *Teoría de Galois sobre anillos conmutativos.* Universidad Los Andes (1999). 74

[23] Polcino Milies, Francisco César. *Anéis e módulos* (2018). 5, 6, 9, 10, 11, 12, 17

[24] Sugano, Kozo. *Note on semisimple extensions and separable extensions* (1967): 265-270. 3, 24, 49, 54

[25] Sugano, Kozo. *On centralizers in separable extensions* (1970): 29-40. 54

[26] Sugano, Kozo. *Separable extensions and Frobenius extensions* (1970): 291-299. 3, 53