Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

EXTENSÕES GALOIS-AZUMAYA-HOPF PARCIAIS

por

Daiane Silva de Freitas

Porto Alegre, 17 de setembro de 2010.

Tese submetida por Daiane Silva de Freitas[1] como requisito parcial para a obtenção do grau de Doutor em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:

Prof. Dr. Antonio Paques

Banca Examinadora:

Prof. Dr. Antonio Paques (IM-UFRGS)

Prof. Dr. Miguel Ferrero (IM-UFRGS)

Prof. Dr. Alveri Sant'Ana (IM-UFRGS)

Prof. Dr. Francisco César Polcino Milies (IME-USP)

Prof. Dr. Michael Dokuchaev (IME-USP)

[1]Bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq

Agradecimentos

Agradeço, em primeiro lugar, ao meu esposo Alexsandro, companheiro e amigo, por ser meu maior incentivador, por sempre acreditar em mim e pelo ombro amigo com o qual sempre pude contar. Deixo aqui o meu muito obrigada, à você o grande amor da minha vida.

Agradeço aos meus pais, Tania e Nedilande, por terem propiciado as condições e os incentivos necessários para que mais este resultado fosse atingido e pelo carinho e apoio a mim dedicados. Também agradeço às minhas irmãs, Nadja e Dafne, pelo apoio e compreensão.

Agradeço aos meus tios, Soraida e Irno, bem como minha vó, Wilma, pela hospitalidade e carinho com o qual me acolheram.

Agradeço em especial ao meu orientador Antonio Paques, à quem tenho grande apreço e consideração, pela orientação, amizade e carinho.

Por fim agradeço aos amigos e colegas, Adriana, Bárbara, Alexandre, Luciane, Daiana, Saradia, Thaísa, Carolina, Diego, Rosane, Cinthya e todos os outros que estiveram presentes.

Resumo

Nesta tese apresentamos condições necessárias e suficientes para que o skew anel de grupo parcial, $R *_\alpha G$, e o produto smash parcial, $A\#_\alpha H$, sejam separáveis sobre seus respectivos centros em termos de separabilidade, Hirata-separabilidade e condições de Galois. Além disso, estabelecemos correspondências de Galois para extensões Galois-Azumaya-Hopf parciais.

Abstract

In this thesis we present sufficient and necessary conditions for the partial skew group ring, $R*_\alpha G$, and the partial smash product, $A\#_\alpha H$, to be separable over their respective centers in terms of separability, Hirata-separability and Galois conditions. Furthermore, we establish Galois correspondences for partial Galois-Azumaya-Hopf extensions.

Conteúdo

Introdução

Sejam R uma álgebra sobre um anel comutativo $\mathbf{k}$ e G um grupo finito. Em [15] DeMeyer e Janusz determinaram, no caso em que $\mathbf{k}$ é um corpo, quando o anel do grupo $R[G]$ é Azumaya, isto é, quando $R[G]$ é uma extensão separável de seu próprio centro. Motivados por esse trabalho Szeto e Wong [35] deram um passo à frente e estudaram o caso do anel do grupo torcido $R^t[G]$. O caso do skew anel do grupo $R * G$, quando R é comutativo, foi considerado por Ikehata [23]. Posteriormente Alfaro e Szeto [2] estenderam os resultados de Ikehata ao contexto de anéis não necessariamente comutativos. Os resultados em [2] foram considerados por Carvalho [8] para produtos cruzados não torcidos, também denotados por $R*G$, por Paques e Sant'Ana [32] para produtos cruzados torcidos parciais $R *_\alpha G$, onde α denota uma ação parcial torcida de G sobre R, e por Ouyang [30], em sua tese de PhD, para produtos smash $R\#H$, onde H é uma álgebra de Hopf de dimensão finita e R é um H-módulo álgebra à esquerda.

Num contexto puramente algébrico, a noção de ação parcial (resp. parcial torcida) de grupos foi introduzida na literatura pela primeira vez por Dokuchaev e Exel [16] (resp. Dokuchaev, Exel e Simón [17]).

O principal resultado de Alfaro e Szeto em [2], considerado em [8], [30] e [32] para contextos mais gerais, é o seguinte

Teorema *Sejam R um anel, G um grupo finito agindo sobre R por automorfismos, $A = R*G$ o correspondente skew anel do grupo e $C(R)$ (resp. $C(A)$) o centro de R (resp. A). Então, as seguintes afirmações são equivalentes:*

(1) *A é Azumaya e $C(A) \subseteq R$.*

(2) *A é Hirata-separável sobre R e R é separável sobre $C(A)$.*

(3) *R é uma extensão de Galois de R^G e R^G é uma $C(A)$-álgebra de Azumaya.*

Na realidade, as três afirmações do teorema acima são ainda equivalentes a uma quarta:

(4) *$C_R(R^G)$ é uma extensão de Galois de $C(A)$ e R^G é uma $C(A)$-álgebra de Azumaya,*

onde $C_T(S)$ denota o centralizador de S em T, para qualquer extensão de anéis $S \subseteq T$.

Dessas equivalências decorre também que

$$\begin{aligned} C(A) = C(R^G) &= C(R)^G \quad \text{e} \\ A \simeq R^G \otimes_{C(A)} (C_R(R^G) * G) &\simeq R^G \otimes_{C(A)} \mathrm{End}_{C(A)}(C_R(R^G)). \end{aligned}$$

Nos principais resultados em [32] a hipótese $C(A) \subseteq R$ foi substituída por $C_A(R) \subseteq R$. No capítulo 2 desta tese nós retomamos a hipótese $C(A) \subseteq R$ e estendemos os resultados acima listados ao contexto de ações parciais de grupos (veja Teoremas 2.1.1, 2.1.2), bem como analizamos o que ocorre com $C_A(R)$ nesse contexto (veja Teorema 2.1.3).

Motivados por seus resultados acima descritos, Alfaro e Szeto introduziram em [3] a noção de extensão Galois-Azumaya.

Dados um anel R e um grupo finito G agindo sobre R por automorfismos, R é dito ser uma extensão Galois-Azumaya de R^G se:

(i) *R é uma extensão de Galois de R^G e*

(ii) R^G *é uma* $C(R)^G$*-álgebra de Azumaya.*

Em particular, de acordo com o teorema acima, se R é uma extensão Galois-Azumaya de R^G então $A = R * G$ é Azumaya e $C(A) = C(R)^G = C(R^G)$.

Além disso, Alfaro e Szeto também provaram em [3] a existência de correspondências de Galois entre subálgebras separáveis de R e subálgebras separáveis de R^G, generalizando, em particular, um similar resultado de DeMeyer [13] no contexto de álgebras de Galois centrais.

Esses resultados foram estendidos por Paques, Rodrigues e Sant'Ana [31] ao contexto de ações parciais de grupos e por Ouyang [30] ao contexto de ações de álgebras de Hopf.

No capítulo 3 desta tese nós estendemos os resultados de Alfaro e Szeto em [3, 2] ao contexto de ações parciais de álgebras de Hopf. Ações parciais de álgebras de Hopf foram introduzidas pela primeira vez na literatura por Caenepeel e Janssen [7], generalizando, em particular, alguns dos resultados de Dokuchaev, Ferrero e Paques [18] para ações parciais de grupos.

Esta tese está organizada da seguinte forma:

No capítulo 1 apresentamos as noções preliminares e os resultados pertinentes, constantes da literatura, que serão utilizados nos demais capítulos. O leitor familiarizado com essa literatura, poderá passar diretamente aos capítulos seguintes.

No capítulo 2 apresentamos condições necessárias e suficientes que permitem decidir quando um skew anel de grupo parcial $A = R *_\alpha G$ é Azumaya, em termos de separabilidade, Hirata-separabilidade e condições de Galois (veja Teorema 2.1.2). Também estendemos a ação parcial α de G sobre R a uma ação parcial α^* de G sobre o centralizador $\Delta = C_A(R)$, via automorfismos internos parciais (veja Proposição 2.2.1), bem como obtivemos um teorema similar ao Teorema 2.1.2 para o skew anel de grupo parcial $\Lambda = \Delta *_{\alpha^*} G$ (veja Teorema 2.1.3). Em particular, se $\Delta \subseteq R$ então α^* coincide com a restrição de α a Δ.

No capítulo 3 começamos por apresentar um teorema-definição para extensões Galois-Hopf parciais (veja Teorema 3.1.6) generalizando teoremas similares existentes na literatura (veja em particular [9, Theorem 1.3], [28, Theorem 8.3.3], [18, Theorem 4.1] [19, Theorem 3.1]e [5, Section 4]). Este teorema é de crucial importância para os demais resultados do capítulo, quais sejam, o Teorema 3.2.3, do qual extraímos a noção de extensão Galois-Azumaya-Hopf parcial, e os Teoremas 3.3.3 e 3.3.4, que falam das correspondências de Galois para tais extensões.

Por fim, gostaríamos de fazer uma rápida observação sobre o título da tese **Extensões Galois-Azumaya-Hopf Parciais**, tendo em vista que no capítulo 2 tratamos de extensões Galois-Azumaya no contexto de ação parcial de grupos. Na realidade as ações parciais de um grupo finito G sobre um anel R estão em correspondência um a um com as ações parciais da correspondente álgebra de Hopf $R[G]$. Este resultado é devido a Caenepeel e Janssen [7]. Portanto, uma extensão Galois-Azumaya parcial é um caso particular de extensão Galois-Azumaya-Hopf parcial.

Capítulo 1

Pré Requisitos

Neste capítulo daremos as definições e os resultados principais usados no trabalho. Estes resultados já são conhecidos e estão publicados nas referências mencionadas.

Neste trabalho todos anéis são associativos, unitários e não necessariamente comutativos, exceto nos casos explicitamente mencionados. Todo subanel B de um anel A é unitário com a mesma unidade de A.

1.1 Separabilidade e Hirata-separabilidade

Definição 1.1.1. Seja A um anel e $B \subseteq A$ um subanel com mesma unidade. A extensão $A \supseteq B$ é dita uma extensão separável se o homomorfismo de A-bimódulos cinde

$$\mu : A \otimes_B A \to A, \quad a \otimes b \mapsto ab.$$

Em particular, se $B = C(A)$ (o centro de A), então A é dito uma extensão Azumaya de B (ou simplesmente Azumaya sobre B ou B-álgebra de Azumaya ou ainda separável e central).

Dado um (A,A)-bimódulo V e B um subanel de A, definimos o *centralizador* de B em V como o conjunto $C_V(B) = \{v \in V : bv = vb, \forall b \in B\}$. Em particular, se V tem também uma estrutura de anel compatível com a estrutura de bimódulo então $C_V(B)$ é um subanel de V.

Uma extensão $A \supseteq B$ é dita Hirata-separável (ou simplesmente H-separável) se existem $v_i \in C_A(B)$ e $d_i \in C_{A\otimes_B A}(A)$, $1 \leq i \leq n$, tais que $\sum_i v_i d_i = 1 \otimes 1$. O conjunto $\{v_i, d_i\}$ é dito um sistema de Hirata (ou H-sistema) de A sobre B.

Proposição 1.1.2. [30, Proposition 2.1] *Sejam $A \supseteq B$ uma extensão de anéis. Então as seguintes afirmações são equivalentes:*

(1) A é uma extensão separável de B.

(2) A é um A-bimódulo somando direto de $A \otimes_B A$.

(3) Existe um elemento $e = \sum_i a_i \otimes b_i \in A \otimes_B A$ tal que $\sum_i x a_i \otimes b_i = \sum_i a_i \otimes b_i x$ e $\sum_i a_i b_i = 1_A$ para todo $x \in A$, tal elemento é dito idempotente de separabilidade.

Teorema 1.1.3. [14, Theorem 2.3.8] *Seja R um anel comutativo. Então, uma R-álgebra A é separável se e somente se A é separável sobre seu centro $C(A)$ e $C(A)$ é separávvel sobre R.*

Definição 1.1.4. Sejam R um anel e A um R-módulo à esquerda (à direita). Diremos que A é um *gerador* para a categoria dos R-módulos à esquerda se para qualquer R-módulo à esquerda (à direita) M existem um conjunto $\Lambda \neq \emptyset$ e um homomorfismo de R-módulos sobrejetor $\Phi : \oplus_{\lambda\in\Lambda} A_\lambda \to M$ (onde $A_\lambda = A$), ou seja, todo R-módulo à esquerda (à direita) M é um quociente de $\oplus_{\lambda\in\Lambda} A_\lambda$.

Diremos que A é um *progerador* para a categoria dos R-módulos à esquerda (à direita) se A for projetivo finitamente gerado e gerador.

O resultado a seguir nos fornece uma definição equivalente para progerador.

Proposição 1.1.5. [14, Corolary 1.1.10] *Seja R um anel comutativo. Então, um R-módulo M é um R-progerador se e somente se M é projetivo finitamente gerado e fiel.*

Proposição 1.1.6. [14, Proposition 2.3.3] *Sejam R um anel comutativo, A e B R-álgebras separáveis e centrais. Então $A \otimes_R B$ é uma R-álgebra separável e central.*

Vamos denotar por A^{op} a álgebra oposta de A, ou seja o produto em A^{op} é dado por $a^{op}b^{op} = (ba)^{op}$.

Teorema 1.1.7. [14, Theorem 2.3.4] *Sejam R um anel comutativo e A uma R-álgebra. As seguintes afirmações são equivalentes:*

(1) A é Azumaya sobre R.

(2) A é $A \otimes A^{op}$-progerador e A é R-central.

(3) A é um R-progerador e $A \otimes A^{op} \backsimeq End_R(A)$.

Teorema 1.1.8. [14, Theorem 2.4.1] *Sejam R um anel comutativo e E qualquer R-progerador. Então $A = End_R(E)$ é Azumaya sobre R.*

Teorema 1.1.9. [14, Theorem 2.4.4] *Sejam R um anel comutativo e A uma R-álgebra de Azumaya. Suponha que B e C são subálgebras tais que a aplicação $B \otimes_R C \to A$ dada por $b \otimes c \mapsto bc$ é um isomorfismo de R-álgebras. Então B e C são R-álgebras de Azumaya $C_A(B) = C$ e $C_A(C) = B$.*

Teorema 1.1.10. [14, Theorem 2.5.1] *Sejam R um anel comutativo e A uma R-álgebra de Azumaya. Então para qualquer R-álgebra comutativa S, $A \otimes_R S$ é uma S-álgebra de Azumaya.*

Teorema 1.1.11. [36, Theorem 18.8] *Sejam R um anel, A um R-módulo à esquerda e $S = End({}_RA)$. Então as seguintes afirmações são equivalentes:*

(1) A é um gerador para a categoria dos R-módulos à esquerda.

(2) A é um S-módulo à direita projetivo finitamente gerado e $R \backsimeq End(A_S)$.

O teorema a seguir é conhecido como o Teorema do Centralizador para álgebras de Azumaya.

Teorema 1.1.12. [14, Theorem 2.4.3] *Sejam R um anel comutativo e A uma R-álgebra de Azumaya. Suponha B qualquer subálgebra separável de A contendo R. Então $C_A(B)$ é uma subálgebra separável de A e $C_A(C_A(B)) = B$. Se B for Azumaya sobre R então $C_A(B)$ também o é e a aplicação de R-álgebras $B \otimes_R C_A(B) \to A$ dada por $b \otimes a \to bc$ é um isomorfismo.*

Proposição 1.1.13. [33, Propositon 1.3] *Sejam A uma extensão Hirata-separável de B tal que B é um somando direto de A como B-bimódulo e $\Delta = C_A(B)$. Então, Δ é separável sobre $C = C(A)$ e $C_A(\Delta) = B$.*

Lema 1.1.14. [23, Lemma] *Sejam A uma extensão Hirata-separável de B e M um A-módulo à esquerda. Se M é um gerador como B-módulo à esquerda, então M é um gerador como A-módulo à esquerda.*

Teorema 1.1.15. [21, Theorem 2.2] *Se A é uma extensão Hirata-separável de B então, A é uma extensão separável sobre B.*

Teorema 1.1.16. [33, Corollary 1.1] *Uma extensão A é de Azumaya sobre B se e somente se A é uma extensão Hirata-separável sobre B e B é um B-somando direto de A.*

Teorema 1.1.17. [23, Theorem 1] *Sejam A uma C-álgebra Azumaya (respectivamente, separável) e $A \supseteq B \supseteq C$. Se A é projetivo finitamente gerado como B-módulo então A é Hirata-separável sobre B (respectivamente, separável).*

Teorema 1.1.18. [33, Proposition 1.2] *Se A é uma extensão H-separável de B tal que B é um B-somando direto de A, então $C_A(C_A(B)) = B$.*

Teorema 1.1.19. [29, Theorem 1] *Sejam A uma $C(A)$-álgebra de Azumaya, B uma $C(A)$-subálgebra e $\Delta = C_A(B)$.*

(1) B é uma $C(A)$-álgebra separável se e somente se B é isomorfo a algum somando direto de uma soma direta finita de cópias de A como (A, B)-bimódulos. Neste caso, $A \supseteq B$ é uma extensão H-separável com $C_A(\Delta) = B$ e A é um B-módulo à esquerda projetivo finitamente gerado.

(2) B é uma $C(A)$-álgebra de Azumaya se e somente se A é isomorfo a algum somando direto de uma soma direta finita de cópias de B como (A, B)-bimódulos.

Lema 1.1.20. [29, Lemma 1] *Sejam $A \supseteq B$ uma extensão H-separável e $\Delta = C_A(B)$.*

(1) Se B é um A-módulo projetivo finitamente gerado, então $C_A(\Delta) = B$.

(2) Se B é isomorfo a algum somando direto de uma soma direta finita de cópias de A como (A, B)-bimódulos, então Δ é uma $C(A)$-álgebra separável.

Proposição 1.1.21. [22, Proposition 2.5] *Sejam S um anel , B e R subanéis de S tais que $B \supseteq R$. Se S é uma extensão separável de B e B é uma extensão separável de R, então S é uma extensão separável de R.*

1.2 Ação parcial de grupos

Sejam $\mathbf{k}$ um anel comutativo com unidade $1_{\mathbf{k}}$, R uma $\mathbf{k}$-álgebra com unidade 1_R e G um grupo com elemento identidade e. As definições correspondentes à ação parcial de grupo foram extraídas de [16].

Definição 1.2.1. Uma ação parcial α de G sobre R é um par

$$\alpha = (\{D_g\}_{g\in G}, \{\alpha_g\}_{g\in G}),$$

onde para cada $g \in G$, D_g é um ideal de R e $\alpha_g : D_{g^{-1}} \to D_g$ é um isomorfismo de $\mathbf{k}-$álgebras, satisfazendo as seguintes condições:

(i) $D_e = R$ e $\alpha_e = id_R$.

(ii) $\alpha_g \left(D_{g^{-1}} \cap D_h\right) = D_g \cap D_{gh}$, $\forall g, h \in G$.

(iii) $\alpha_g \left(\alpha_h \left(x\right)\right) = \alpha_{gh} \left(x\right)$, $\forall x \in D_{h^{-1}} \cap D_{(gh)^{-1}}$, $\forall g, h \in G$.

Dizemos que a ação parcial α possui uma *ação envolvente* (ou *globalização*) se existe um anel T e uma ação global de G em T, por automorfismos β_g $(g \in G)$, tais que R pode ser visto como um ideal de T e as seguintes condições valem:

(i) $T = \sum_{g\in G} \beta_g(R)$,

(ii) $D_g = R \cap \beta_g(R), \forall g \in G$,

(iii) $\alpha_g(r) = \beta_g(r), \forall g \in G, r \in D_{g^{-1}}$.

Para nossa proposta vamos assumir que cada ideal D_g possui unidade 1_g. Em particular cada 1_g é um idempotente central de R, o que é equivalente a dizer que α possui envolvente, conforme resultado a seguir.

Teorema 1.2.2. [16, Theorem 4.5] *Seja R um anel com unidade. Então uma ação parcial α de um grupo G sobre R possui uma ação global envolvente β se, e somente se, cada ideal $D_g(g \in G)$ é um anel com unidade. Além disso, se β existe, ela é única a menos de equivalências.*

Observação 1.2.3. Notemos que $D_g = R1_g = 1_gR$ e $D_g \cap D_h = 1_g1_hR$, para todo $g, h \in G$. Em [16], encontramos duas identidades muito usadas

$$\alpha_g(1_{g^{-1}}1_h) = 1_g1_{gh} \quad e \quad 1_g = \beta_g(1_R)1_R.$$

Definição 1.2.4. Definimos o *skew anel de grupo parcial* da seguinte forma

$$R *_\alpha G = \{\sum_{g \in G} r_g\delta_g : r_g \in D_g\} = \oplus_{g \in G} D_g\delta_g.$$

O produto em $R *_\alpha G$ é definido por

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

$R *_\alpha G$ é um anel com unidade $1_R\delta_1$, o qual é uma extensão de R via inclusão

$$R \hookrightarrow R *_\alpha G, r \mapsto r\delta_1.$$

Em [18] foi introduzido o conceito de subanel dos elementos invariantes de R pela ação α como sendo

$$R^\alpha = \{r \in R : \alpha_g(r1_{g^{-1}}) = r1_g, \forall g \in G\}.$$

Definimos a aplicação traço parcial e denotamos por t_α a aplicação $t_\alpha : R \to R$ dada por $t_\alpha(r) = \sum_g \alpha_g(r1_{g^{-1}})$. É claro que $t_\alpha(r) \in R^\alpha$.

Observação 1.2.5. $R *_\alpha G$ é um R-módulo à esquerda projetivo finitamente gerado. De fato, como $R *_\alpha G = \oplus D_g\delta_g$, existe $1_g \in D_g$ tal que $R = D_g \oplus R(1 - 1_g)$. Logo, cada D_g é um R-módulo projetivo finitamente gerado, o que implica que $\oplus D_g\delta_g$ é um R-módulo projetivo finitamente gerado.

Definição 1.2.6. Sejam G um grupo finito e α uma ação parcial de G sobre R. Diremos que R é uma extensão Galois parcial de R^α com ação α (ou simplesmente, extensão α-Galois parcial) se existirem elementos $x_i, y_i \in R$, $1 \leq i \leq n$, tais que $\sum_i x_i \alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g} 1_g$, para todo $g \in G$.

O teorema a seguir foi demonstrado em [18], a seguir apresentamos uma outra demonstração deste fato.

Teorema 1.2.7. *Seja α uma ação parcial de um grupo finito G sobre R. Se R é uma extensão α-Galois parcial de R^α então R é uma extensão separável de R^α.*

Demonstração. Sejam $x_i, y_i \in R$ com $1 \leq i \leq n$ tais que $\sum_{i=1}^{n} x_i \alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g} 1_R$. Considere a aplicação $tr_\alpha \in Hom_{R^\alpha}(R, R^\alpha)$ dada por $tr_\alpha(x) = \sum_{g \in G} \alpha_g(x 1_{g^{-1}})$ e o elemento $e = \sum_{j=1}^{n} x_j \otimes y_j \in R \otimes_{R^\alpha} R$. Então, $\sum_{j=1}^{n} x_j y_j = 1_R$ e para qualquer x em R temos

$$\begin{aligned} xe &= \sum_{j=1}^{n} x x_j \otimes y_j \\ &= \sum_{j=1}^{n} \sum_{k=1}^{n} x_k t_\alpha(y_k x x_j) \otimes y_j \\ &= \sum_{k=1}^{n} \sum_{j=1}^{n} x_k \otimes tr_\alpha(y_k x x_j) y_j \\ &= \sum_{k=1}^{n} x_k \otimes y_k x = ex, \end{aligned}$$

donde segue que e é um idempotente de separabilidade. Portanto, R é uma extensão separável de R^α. $\square$

Proposição 1.2.8. [6, Proposition 3.1] *Considere G um grupo finito e α uma ação parcial do grupo G sobre o anel R. Então $R *_\alpha G$ é uma extensão separável de R se e somente se $1_R \in t_\alpha(C(R))$.*

Teorema 1.2.9. [19, Theorem 3.1] *Seja* $S = R*_\alpha G$. *As seguintes afirmações são equivalentes:*

(1) R *é uma extensão* α*-Galois parcial de* R^α.

(2) R *é um* R^α*-módulo à direita projetivo finitamente gerado e* $\phi : S \to End(R_{R^\alpha})$ *definido por* $\phi(a\delta_g)(x) = a\alpha_g(x1_{g^{-1}})$*, é um isomorfismo de anéis.*

(3) $RtR = S$*, onde* $t = \sum_{h\in G} 1_h\delta_h$.

(4) A aplicação $\Gamma' : ({}_R R_{R^\alpha}) \otimes_S ({}_{R^\alpha} R_S) \to S$ *definida por* $\Gamma'(x \otimes y) = \sum_{g\in G} x\alpha_g(y1_{g^{-1}})\delta_g$ *é sobrejetora.*

(5) R *é um gerador para a categoria dos* S*-módulos à esquerda.*

Definição 1.2.10. Dado um subconjunto não vazio X de R, dizemos que X é α-invariante se $\alpha_g(X1_{g^{-1}}) = X1_g$, para todo $g \in G$.

Proposição 1.2.11. *Sejam* α *uma ação parcial de um grupo* G *em um anel* R *e* X *um subconjunto* α*-invariante de* R. *Então:*

(1) $C_R(X)$ *é* α*-invariante.*

(2) Em particular, se X *é subanel de* R *então* $(\{X_g = X1_g\}_{g\in G}, \{\alpha_g|_{X_{g^{-1}}}\}_{g\in G})$ *é uma ação parcial de* G *sobre* X.

Demonstração. (1) Seja $r \in C_R(X)$. Então, $rx = xr$ para todo $x \in X$. Com isso,

$$\begin{aligned} \alpha_g(r1_{g^{-1}})x &= \alpha_g(r1_{g^{-1}})\alpha_g(\alpha_{g^{-1}}(x1_g)) = \alpha_g(r\alpha_{g^{-1}}(x1_g)1_{g^{-1}}) \\ &= \alpha_g(\alpha_{g^{-1}}(x1_g)r) = \alpha_g(\alpha_{g^{-1}}(x1_g))\alpha_g(r1_{g^{-1}}) = x\alpha_g(r1_{g^{-1}}). \end{aligned}$$

(2) Comecemos por observar que X_g é um ideal de X, pois $1_R \in X$ e portanto, para qualquer $g \in G$ temos $1_g = \alpha_g(1_R 1_{g^{-1}}) \in X$ por hipótese. As

propriedades da Definição 1.2.1 são trivialmente satisfeitas. $\square$

1.3 Álgebra de Hopf

Nesta seção introduzimos os conceitos necessários para definir um H-módulo álgebra, um H-comódulo álgebra (onde H denotará um álgebra de Hopf) bem como resultados relacionados. Estes conceitos e resultados são amplamente conhecidos e podem ser encontrados nos livros [12] e [28].

Seja $\mathbf{k}$ um corpo. Denotaremos o produto tensorial sobre $\mathbf{k}$ por simplesmente $\otimes$.

Definição 1.3.1. Uma $\mathbf{k}$-álgebra de Hopf é uma quádrupla $(H, \Delta_H, \varepsilon_H, S_H)$, onde:

(i) H é uma $\mathbf{k}$-álgebra.

(ii) $\Delta_H : H \to H \otimes H$ e $\varepsilon_H : H \to \mathbf{k}$ são homorfismos de $\mathbf{k}$-álgebras que satisfazem as seguintes condições:

- $(\Delta_H \otimes id_H) \circ \Delta_H = (id_H \otimes \Delta_H) \circ \Delta_H$.
- $(\varepsilon_H \otimes id_H) \circ \Delta_H = 1_{\mathbf{k}} \otimes id_H$ e $(id_H \otimes \varepsilon_H) \circ \Delta_H = id_H \otimes 1_{\mathbf{k}}$.

(iii) $S_H : H \to H$ é um anti-homomorfismo de $\mathbf{k}$-álgebras, chamado antípoda, que satisfaz a seguinte condição:

$$\mu \circ (S_H \otimes id_H) \circ \Delta_H = 1_H \varepsilon_H = \mu \circ (id_H \otimes S_H) \circ \Delta_H,$$

onde $\mu : H \otimes H \to H$, é a multiplicação de H.

Para o que segue, H denotará uma álgebra de Hopf.

Definição 1.3.2. Uma $\mathbf{k}$-álgebra A é dita uma *H-módulo álgebra (à esquerda)* se:

(i) A é um H-módulo (à esquerda) via $h \otimes a \mapsto h \triangleright a$

(ii) $h \triangleright (ab) = \sum (h_1 \triangleright a)(h_2 \triangleright b)$, onde $\Delta_H(h) = \sum h_1 \otimes h_2$

(iii) $h \triangleright 1_A = \varepsilon_H(h) 1_A$

para todos $h \in H, a, b \in A$.

Definição 1.3.3. Seja A um H-módulo álgebra, definimos a *subálgebra dos invariantes* como

$$A^H = \{a \in A : h \triangleright a = \varepsilon_H(h)a, \forall h \in H\}.$$

Definição 1.3.4. Um $\mathbf{k}$-espaço vetorial M é dito um *H-comódulo (à direita)* se existe uma aplicação $\mathbf{k}$-linear $\rho : M \to M \otimes C$ dada por $\rho(m) = \sum m_{(0)} \otimes m_{(1)}$, a qual é dita coação, tal que os seguintes diagramas são comutativos:

$$\begin{tikzcd} M \arrow[r, "\rho"] \arrow[d, "\rho"'] & M \otimes C \arrow[d, "id_M \otimes \Delta"] \\ M \otimes C \arrow[r, "\rho \otimes id_C"'] & M \otimes C \otimes C \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "\rho"] \arrow[dr, "\simeq"'] & M \otimes C \arrow[d, "id_M \otimes \varepsilon_H"] \\ & M \otimes \mathbf{k} \end{tikzcd}$$

Definição 1.3.5. Uma álgebra A é dita uma *H-comódulo álgebra (à direita)* se:

(i) A é um H-comódulo (à direita) via $\rho : A \to A \otimes H, \quad a \mapsto \sum a_{(0)} \otimes a_{(1)}$

(ii) $\rho(ab) = \rho(a)\rho(b)$, ou seja, $\sum (ab)_{(0)} \otimes (ab)_{(1)} = \sum a_{(0)} b_{(0)} \otimes a_{(1)} b_{(1)}$

(iii) $\rho(1_A) = 1_A \otimes 1_H$

para todos $h \in H, a, b \in A$.

Definição 1.3.6. Seja A uma H-comódulo álgebra, definimos a *subálgebra dos coinvariantes* como

$$A^{coH} = \{a \in A : \rho(a) = a \otimes 1_H, \forall h \in H\}.$$

Observação 1.3.7. **(i)** Vamos denotar por H^* o dual da álgebra de Hopf H, ou seja, $H^* = Hom_{\mathbf{k}}(H, \mathbf{k})$, o qual tem uma estrutura de álgebra de Hopf (desde que H tenha dimensão finita). (Para detalhes ver [12, Proposition 4.2.11]).

(ii) Sejam A uma $\mathbf{k}$-álgebra e H uma álgebra de Hopf de dimensão finita. Então A é um H-módulo álgebra à esquerda se e somente se A é um H^*-comódulo álgebra à direita. Além disso, nesse caso $A^H = A^{coH^*}$.

A seguir introduzimos o conceito de integral em H, o qual será muito útil no desenvolvimento do capítulo 3.

Definição 1.3.8. Uma *integral* à esquerda em H é um elemento $t \in H$ tal que $ht = \varepsilon_H(h)t$, para todo $h \in H$. Denotamos o conjunto das integrais à esquerda por $\int_H^l$. Definimos de modo análogo integral à direita.

O seguinte resultado garante a existência de uma integral não nula para uma álgebra de Hopf de dimensão finita.

Proposição 1.3.9. [12, Corollary 5.2.6] *Seja H uma álgebra de Hopf de dimensão finita com antípoda S. Então $\int_H^l$ tem dimensão 1 e S é bijetiva.*

Para uma integral à esquerda $t \neq 0$, uma função *traço* à esquerda para H em A (onde A é um H-módulo álgebra à esquerda) é definida como a aplicação $\widehat{t} : A \to A$ dada por $\widehat{t}(a) = t \cdot a$.

Observemos que $\widehat{t}(a) \in A^H$ pois, $h \cdot (t \cdot a) = (ht) \cdot a = \varepsilon_H(h)t \cdot a$.

Para a definição e a proposição a seguir vamos assumir que H tem dimensão finita.

Definição 1.3.10. Seja A um H-comódulo álgebra à direita com estrutura dada por $\rho : A \to A \otimes H$. Então a extensão $A \supseteq A^{coH}$ é dita *H-Galois* à direita se a aplicação $\beta : A \otimes_{A^{coH}} A \to A \otimes H$ dada por $a \otimes b \mapsto (a \otimes 1_H)\rho(b)$ é uma bijeção.

Proposição 1.3.11. [10, Proposition 1.6] *Seja A uma extensão H^*-Galois. Então, A^H é um A^H-bimódulo somando direto de A se e somente se A tem um elemento $c \in C_A(A^H)$ de traço 1.*

Definição 1.3.12. Um **k**-espaço vetorial M é dito um *módulo de Hopf* à direita se M tem estrutura de H-módulo à direita (a ação de H em M será denotada por mh), e uma estrutura de H-comódulo à direita (a coação é dada por $\rho(m) = \sum m_{(0)} \otimes m_{(1)}$) e estas duas estruturas são compatíveis, ou seja, $\rho(mh) = \sum m_{(0)}h_1 \otimes m_{(1)}h_2$, $\forall m \in M, h \in H$.

O resultado a seguir é conhecido como o Teorema Fundamental para Módulos de Hopf.

Teorema 1.3.13. [12, Theorem 4.4.6] *Sejam H uma álgebra de Hopf e M um H-módulo de Hopf à direita. Então a aplicação $f : M^{coH} \otimes H \to M$ definida por $f(m \otimes h) = mh$, para todos $m \in M^{coH}$ e $h \in H$, é um isomorfismo de H-módulos de Hopf à direita.*

1.4 Extensões Galois-Hopf Parciais

Nesta seção trataremos de extensões de Hopf-Galois e para tal será necessário ver uma série de definições e resultados que se encontram nas referências [5] e [7].

Definição 1.4.1. Uma *ação parcial à esquerda de uma álgebra de Hopf* H numa álgebra A é uma aplicação $\alpha : H \otimes A \to A$, denotada por $\alpha(h \otimes a) = h \cdot a$, tal que

(i) $h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b)$,

(ii) $1_H \cdot a = a$,

(iii) $h \cdot (g \cdot a) = \sum (h_1 \cdot 1_A)(h_2 g \cdot a)$.

Neste caso dizemos que A é um H-*módulo álgebra parcial à esquerda*.

Definição 1.4.2. Uma *coação parcial à esquerda de uma álgebra de Hopf* H numa álgebra A é uma aplicação linear $\overline{\rho} : A \to H \otimes A$, denotada por $\overline{\rho}(a) = \sum a_{(0)} \otimes a_{(1)}$ tal que

(i) $\overline{\rho}(ab) = \overline{\rho}(a)\overline{\rho}(b)$, $\forall a, b \in A$,

(ii) $(id_A \otimes \varepsilon)\overline{\rho}(a) = a$, $\forall a \in A$,

(iii) $(\overline{\rho} \otimes id_H)\overline{\rho}(a) = (\overline{\rho}(1_A) \otimes 1_H)((id_A \otimes \Delta_H)\overline{\rho}(a))$, $\forall a \in A$.

Neste caso dizemos que A é um H-*comódulo álgebra parcial à direita*.

Seja A um H-módulo álgebra parcial e considere o produto tensorial $A \otimes H$ com estrutura de álgebra associativa dada por

$$(a \otimes h)(b \otimes g) = \sum a(h_1 \cdot b) \otimes h_2 g.$$

Definimos o *produto smash parcial* como a álgebra

$$A \#_\alpha H = (A \otimes H)(1_A \otimes 1_H),$$

em outras palavras, o produto smash parcial é a subálgebra gerada pelos elementos da forma

$$a \#_\alpha h = \sum a(h_1 \cdot 1_A) \otimes h_2.$$

Frequentemente usaremos a seguinte notação

$$(a \#_\alpha h)(b \#_\alpha g) = \sum a(h_1 \cdot b) \#_\alpha h_2 g.$$

Note que os elementos de A podem ser vistos em $A \#_\alpha H$ pela aplicação $a \mapsto a \#_\alpha 1_H = a \otimes 1_H$, a qual é uma aplicação de álgebras.

Observação 1.4.3. **(i)** [7, Proposition 4.9] Sejam A uma álgebra e α uma ação parcial do grupo finito G em A. Considere a álgebra de Hopf $H = \mathbf{k}G$, onde $\Delta_H(g) = g \otimes g$, $S_H(g) = g^{-1}$ e $\varepsilon_H(g) = 1_H$. Então, A é um H-módulo álgebra parcial. De fato, note que a ação parcial α induz naturalmente a seguinte aplicação $\mathbf{k}$-linear $\cdot : H \otimes A \to A$, $g \otimes a \mapsto g \cdot a := \alpha_g(a1_{g^{-1}})$ para todo $a \in A$ e para todo $g \in G$, a qual satisfaz as seguintes condições (as quais decorrem da definição de ação parcial de grupos.):

- $g \cdot (ab) = (g \cdot a)(g \cdot b)$,
- $1_H \cdot a = a$,
- $h \cdot (g \cdot a) = (h \cdot 1_A)(h \cdot a)$, para todo $a \in A$ e $h, g \in G$.

A recíproca desta afirmação também vale, ou seja, se A é um $\mathbf{k}G$-módulo álgebra parcial então $\mathbf{k}G$ induz naturalmente uma ação parcial do grupo G na álgebra A via $\alpha_g(a1_{g^{-1}}) = g \cdot a$. Novamente as condições da definição de ação parcial de grupos decorrem da definição de ação parcial de álgebras de Hopf.

(ii) Ainda nas condições do item **(i)** temos que $A *_\alpha G = A \#_\alpha H$. Basta considerar a aplicação

$$\begin{aligned} \gamma : A *_\alpha G &\to A\#_\alpha H \\ \sum_g a_g \delta_g &\mapsto \sum_g a_g \#_\alpha g = \sum_g a_g (g \cdot 1_A) \otimes g = \sum_g a_g \otimes g, \end{aligned}$$

a qual é um isomorfismo de $\mathbf{k}$-álgebras.

(iii) Seja M um $A\#_\alpha H$-módulo à esquerda. Notemos que neste caso M é um A-módulo à esquerda via identificação de A como subálgebra de $A\#_\alpha H$.

Contudo, a ação de $A\#_\alpha H$ em M não induz uma ação de H sobre M pois H não se identifica como subálgebra de $A\#_\alpha H$. Por esta razão denotaremos por $M^{\underline{H}}$ o $\mathbf{k}$-subespaço vetorial dos elementos invariantes de M pela ação de $A\#_\alpha H$, isto é,

$$M^{\underline{H}} = \{m \in M : h \cdot m = (h \cdot 1_A)m, \forall h \in H\}.$$

Observemos também que A é um $A\#_\alpha H$-módulo à esquerda via ação $(a\#_\alpha h) \triangleright b = a(h \cdot b)$ e neste caso se $h \cdot 1_A \in C(A)$, para todo $h \in H$ então

$$A^{\underline{H}} = \{a \in A : h \cdot a = (h \cdot 1_A)a, \forall h \in H\},$$

é uma $\mathbf{k}$-subálgebra de A, a qual é dita $\mathbf{k}$-subálgebra dos elementos invariantes.

(iv) Seja A um H-comódulo álgebra parcial à direita, definimos o $\mathbf{k}$-subespaço vetorial dos elementos invariantes de A pela coação $\overline{\rho}$ de H por

$$A^{\underline{coH}} = \{a \in A : \overline{\rho}(a) = a\overline{\rho}(1_A)\}.$$

(v) Definimos a função *traço parcial* como a aplicação $\widehat{t_\alpha} : A \to A$ dada por $\widehat{t_\alpha}(a) = t \cdot a$, onde $t \in \int_H^l$. Note que $\widehat{t_\alpha}(a) \in A^{\underline{H}}$.

Lema 1.4.4. [5, Proposition 6] *Sejam H uma álgebra de Hopf de dimensão finita e A um H-módulo álgebra parcial. Então, $(A^{\underline{H}})^{op} \backsimeq End_{A\#_\alpha H}(A)$ como anéis.*

Observação 1.4.5. Dada uma coação parcial $\overline{\rho} : A \to A \otimes H$, podemos definir uma estrutura de (A, A)-bimódulo em $A \otimes H$: a estrutura de A-módulo à esquerda é dada pela multiplicação e a estrutura de A-módulo à direita é dada por $(a \otimes h)b = \sum ab_{(0)} \otimes hb_{(1)}$.

Para o que segue, vamos considerar um (A, A)-sub-bimódulo de $A \otimes H$ definido por

$$\underline{A \otimes H} = (A \otimes H)1_A = \{\sum a1_{A_{(0)}} \otimes h1_{A_{(1)}} : a \in A, h \in H\},$$

onde $\sum 1_{A_{(0)}} \otimes 1_{A_{(1)}} = \overline{\rho}(1_A)$

Definição 1.4.6. Seja A um H-comódulo álgebra parcial à direita com estrutura dada por $\overline{\rho} : A \to A \otimes H$. Então a extensão $A \supseteq A^{\underline{coH}}$ é dita *H-Galois parcial* à direita se a aplicação $\beta : A \otimes_{A^{\underline{coH}}} A \to \underline{A \otimes H}$ dada por $a \otimes b \mapsto (a \otimes 1_H)\overline{\rho}(b) = \sum ab_{(0)} \otimes b_{(1)}$ é uma bijeção.

Observação 1.4.7. Se H é uma álgebra de Hopf de dimensão finita e A é um H-módulo álgebra parcial à esquerda, então a ação parcial de H em A induz uma coação parcial à direita de H^* em A do seguinte modo: $\overline{\rho}(a) = \sum(h_i \cdot a) \otimes h_i^*$, onde $\{h_i\}$ é uma base de H sobre $\mathbf{k}$ e $\{h_i^*\}$ é a base dual. Reciprocamente, se A é um H^*-comódulo álgebra parcial à direita, então a coação $\overline{\rho}$ induz uma ação parcial à esquerda de H em A do seguinte modo $h \cdot a = \sum a_{(0)}a_{(1)}(h)$, onde $\overline{\rho}(a) = \sum a_{(0)} \otimes a_{(1)}$.

Proposição 1.4.8. [7, Proposition 4.6] *Seja H uma álgebra de Hopf de dimensão finita e A uma $\mathbf{k}$-álgebra. Então A é um H-módulo álgebra parcial à esquerda se e somente se A é um H^*-comódulo álgebra parcial à direita.*

Lema 1.4.9. [5, Lemma 3] *Se H é uma álgebra de Hopf de dimensão finita, A é um H-módulo álgebra parcial à esquerda e $\overline{\rho} : A \to A \otimes H^*$ é a estrutura de H^*-comódulo álgebra parcial à direita induzida em A, então $A^{\underline{H}} = A^{\underline{coH^*}}$.*

Este resultado nos diz que quando H é uma álgebra de Hopf de dimensão finita, podemos considerar no H-módulo álgebra parcial à esquerda A a estrutura induzida, por esta ação, de H^*-comódulo álgebra parcial à direita e como $A^{\underline{H}} = A^{\underline{coH^*}}$, obtemos uma definição equivalente à Definição 1.4.6, onde a aplicação $\beta : A \otimes_{A^{\underline{H}}} A \to \underline{A \otimes H^*}$ é uma bijeção.

Teorema 1.4.10. [5, Theorem 2] *Sejam H uma álgebra de Hopf de dimensão finita, $0 \neq t \in \int_H^l$ e A um H-módulo álgebra parcial à esquerda tal que a aplicação $\beta : A \otimes_{A^{\underline{H}}} A \to \underline{A \otimes H^*}$ é sobrejetora. Então:*

(1) Existem $a_1, ..., a_n$ e $b_1, ..., b_n$ em A tais que $\phi_i : A \to A^{\underline{H}}$ dada por $\phi_i(a) = t \cdot b_i a$ é uma aplicação de $A^{\underline{H}}$-módulos, e $a = \sum_i a_i \phi_i(a)$ para cada $a \in A$; assim $\{a_i\}$ é uma base projetiva de A sobre $A^{\underline{H}}$ e A é projetivo finitamente gerado como $A^{\underline{H}}$-módulo à direita.

(2) β é uma bijeção.

A seguir veremos o conceito de ação envolvente para uma ação parcial de uma álgebra de Hopf H em uma álgebra A.

Definição 1.4.11. Sejam A e B H-módulo álgebras parciais. Dizemos que um morfismo de álgebras $\beta : A \to B$ é um *morfismo de H-módulo álgebras parciais* se $\beta(h \cdot a) = h \cdot \beta(a)$ para todo $h \in H$ e para todo $a \in A$. Se β é um isomorfismo dizemos que as *ações parciais são equivalentes*.

Definição 1.4.12. Sejam B um H-módulo álgebra (com ação denotada por $h \triangleright a$) e A um ideal à direita de B com unidade 1_A. Dizemos que a ação parcial induzida em A (isto é, $h \cdot a = 1_A(h \triangleright a)$) é *admissível* se $B = H \triangleright A$.

Definição 1.4.13. Seja A um H-módulo álgebra parcial. Uma *ação envolvente* para A é um par (B, β), onde

(i) B é um H-módulo álgebra (não necessariamente unitária).

(ii) A aplicação $\beta : A \to B$ é um monomorfismo de álgebras.

(iii) A subálgebra $\beta(A)$ é um ideal à direita em B.

(iv) A ação parcial em A é equivalente à ação parcial induzida em $\beta(A)$.

(v) A ação parcial induzida em $\beta(A)$ é admissível.

O resultado a seguir garante a existência de uma ação envolvente para o H-módulo álgebra parcial A.

Teorema 1.4.14. [4, Theorem 1] *Sejam A um H-módulo álgebra parcial e $\beta : A \to Hom_{\boldsymbol{k}}(H, A)$ a aplicação dada por $\beta(a)(h) = h \cdot a$ e $B = H \triangleright \beta(A)$, então (B, β) é uma ação envolvente para A.*

Capítulo 2

Quando o Skew Anel de Grupo parcial é Azumaya

Em todo este capítulo R denotará um anel unitário, G um grupo finito e $\alpha = (\{D_g\}_{g \in G}, \{\alpha_g\}_{g \in G})$ uma ação parcial de G sobre R que possui uma envolvente (T, β).

Sempre que necessário, usaremos a identificação de R em $R *_\alpha G$, via $r \mapsto r\delta_1$. Denotaremos por A o skew anel de grupo parcial $R *_\alpha G$, por B o skew anel de grupo $T * G$ e por Δ o centralizador $C_A(R)$ de R em A.

O nosso propósito neste capítulo é apresentar condições necessárias e suficientes para que A seja uma álgebra separável sobre seu centro, o qual denotaremos por $C(A)$, em termos de Hirata-separabilidade, separabilidade e condições de Galois parciais.

Veremos também como estender α a uma ação parcial α^* de G sobre Δ, bem como obter informações sobre a condição de ser Azumaya para $\Lambda = \Delta *_{\alpha^*} G$.

2.1 Os Teoremas

Nesta seção apresentamos os teoremas principais deste capítulo.

Teorema 2.1.1. *As seguintes afirmações são equivalentes:*

(1) A é uma álgebra de Azumaya e $C(A) \subseteq R$.

(2) A é H-separável sobre R e R é separável sobre $C(R)^\alpha$.

(3) R é uma extensão de Galois parcial sobre R^α e R^α é Azumaya sobre $C(A)$.

(4) $C_R(R^\alpha)$ é uma extensão α-Galois parcial de $C(A)$ e R^α é Azumaya sobre $C(A)$.

Teorema 2.1.2. *Assuma que A é Azumaya e $C(A) \subseteq R$, então:*

(1) $A \simeq R^\alpha \otimes_{C(A)} (E *_\alpha G)$, com $E = C_R(R^\alpha)$.

(2) R^α e $E *_\alpha G$ são $C(A)$-álgebras de Azumaya.

(3) E é uma extensão α-Galois parcial de $C(A)$.

Teorema 2.1.3. *As seguintes afirmações são equivalentes:*

(1) Δ é uma extensão α^*-Galois parcial de $C(A)$.

(2) Λ é H-separável sobre Δ.

(3) A é H-separável sobre R e $C_\Lambda(C_\Lambda(\Delta)) = \Delta$.

(4) Λ é uma $C(A)$-álgebra de Azumaya.

Para a demonstração destes teoremas necessitamos de vários outros resultados preliminares, os quais trataremos na seção a seguir.

2.2 Resultados Auxiliares

Começaremos por apresentar a ação parcial α^* de G sobre Δ, a qual é construída a partir de automorfismos internos de B induzidos pela ação β de G sobre T.

Recordemos que a existência da ação β como envolvente da ação parcial α é equivalente a dizer (pelo Teorema 1.2.2) que cada ideal D_g é um anel unitário, cujo elemento identidade será denotado por 1_g e neste caso o anel T é um anel unitário.

Proposição 2.2.1. *Nas condições estabelelecidas acima, temos:*

(1) β *induz sobre* B *uma ação* β^* *de* G *por automorfismos internos, isto é,* $\beta^* : G \to Aut(B), \quad g \mapsto \beta^*_g$*, com* $\beta^*_g(t\delta_h) = (1_T\delta_g)(t\delta_h)(1_T\delta_{g^{-1}}) = \beta_g(t)\delta_{ghg^{-1}}$ *para todos* $t \in T, \quad g, h \in G$.

(2) $\beta^*_g(1_{g^{-1}}) = 1_g$, $\beta^*_g(1_{g^{-1}}1_h) = 1_g1_{gh}$ *e* $1_R\beta^*_g(r) = \alpha_g(r1_{g^{-1}})$*, para todo* $h, g \in G$ *e* $r \in R$.

(3) $C_B(T)$ *é* β^**-invariante (isto é,* $\beta^*_g(C_B(T)) = C_B(T)$*, para todo* $g \in G$*) e portanto* β^* *induz, por restrição, uma ação de* G *sobre* $C_B(T)$.

(4) $C_B(T)1_R = \Delta$.

(5) $\alpha^* := (\{\Delta_g = \Delta 1_g\}_{g\in G}, \{\alpha^*_g = \beta^*_g|_{\Delta_{g^{-1}}}\}_{g\in G})$ *é uma ação parcial de* G *sobre* Δ.

(6) $(C_B(T), \beta^*|_{C_B(T)})$ *é uma envolvente de* (Δ, α^*).

(7) $\Delta^{\alpha^*} := \{a \in \Delta | \alpha^*_g(a1_{g^{-1}}) = a1_g, \quad \forall g \in G\} = C(A)$.

Demonstração. (1) Basta observar que $\beta^* : G \to Aut(B)$ é homomorfismo de grupos. De fato, para todo $g, h, l \in G$ e $t \in T$ temos

$$\begin{aligned}
\beta^*(gh)(t\delta_l) &= \beta^*_{gh}(t\delta_l) = \beta_{gh}(t)\delta_{ghl(gh)^{-1}} = \beta_g(\beta_h(t))\delta_{g(hlh^{-1})g^{-1}} \\
&= \beta^*_g(\beta_h(t)\delta_{hlh^{-1}}) = \beta^*_g(\beta^*_h(t\delta_l)) = \beta^*_g \circ \beta^*_h(t\delta_l)
\end{aligned}$$

(2) Para todo $r \in R$ e $g, h \in G$ temos

$$\begin{aligned}
\beta^*_g(1_{g^{-1}}) &= \beta^*_g(1_{g^{-1}}\delta_1) = \beta_g(1_R\beta_{g^{-1}}(1_R))\delta_1 = \beta_g(1_R)1_R\delta_1 \\
&= \alpha_g(1_{g^{-1}})\delta_1 = 1_g\delta_1 = 1_g.
\end{aligned}$$

$$\begin{aligned}
\beta^*_g(1_{g^{-1}}1_h) &= \beta^*_g(1_R\beta_{g^{-1}}(1_R)\beta_h(1_R)\delta_1) = \beta_g(1_R\beta_{g^{-1}}(1_R)\beta_h(1_R))\delta_1 \\
&= \beta_g(1_R)1_R\beta_{gh}(1_R)\delta_1) = \alpha_g(1_R1_{g^{-1}})\alpha_{gh}(1_R1_{(gh)^{-1}})\delta_1 \\
&= 1_g1_{gh}\delta_1 = 1_g1_{gh}. \\
1_R\beta^*_g(r) &= 1_R\beta^*_g(r\delta_1) = 1_R\beta_g(r)\delta_1 = \alpha_g(r1_{g^{-1}})\delta_1 = \alpha_g(r1_{g^{-1}}).
\end{aligned}$$

(3) Dados $b \in C_B(T)$, $\quad g \in G$, $\quad t \in T$ temos

$$\begin{aligned}
\beta^*_g(b)t &= (1_T\delta_g)b(1_T\delta_{g^{-1}})(t\delta_1) = (1_T\delta_g)b\beta_{g^{-1}}(t)\delta_{g^{-1}} \\
&= (1_T\delta_g)(\beta_{g^{-1}}(t)\delta_1)b\delta_{g^{-1}} = \beta_g(\beta_{g^{-1}}(t))(1_T\delta_g)b\delta_{g^{-1}} = t\beta^*_g(b),
\end{aligned}$$

ou seja, $\beta^*_g(b) \in C_B(T)$.

(4) Note que:

$$\begin{aligned}
1_RB1_R &= 1_R(\oplus_{g\in G}T\delta_g)1_R = \oplus_{g\in G}(T1_R\delta_g)(1_R\delta_1) \\
&= \oplus_{g\in G}T1_R\beta_g(1_R)\delta_g = \oplus_{g\in G}T1_g\delta_g = \oplus_{g\in G}D_g\delta_g = A.
\end{aligned}$$

Então, $C_B(T)1_R = 1_RC_B(T)1_R = C_{1_RB1_R}(T) = C_A(T) \subseteq C_A(R) = \Delta$. Reciprocamente, dado $a \in \Delta$, existe $b \in B$ tal que $a = 1_Rb1_R$. Logo,

$a \in B$, $\quad a1_R = 1_R a = a$ e para todo $t \in T$, temos $at = (a1_R)t = a(1_R t) = (1_R t)a = t(1_R a) = ta$, ou seja, $a \in C_B(T)1_R$.

(5) Comecemos por observar que $\alpha_g^*(\Delta_{g^{-1}}) = \beta_g^*(\Delta 1_{g^{-1}}) = \beta_g^*(C_B(T)1_{g^{-1}})$ $= \beta_g^*(C_B(T))\beta_g^*(1_{g^{-1}}) = C_B(T)1_g = \Delta 1_g = \Delta_g$, e como 1_g é idempotente central em Δ, temos que Δ_g é um ideal de Δ. Além disso, é imediato verificar que $(\alpha_g^*)^{-1} = \alpha_{g^{-1}}^*$. Portanto, $\alpha_g^* : \Delta_{g^{-1}} \to \Delta_g$ é isomorfismo de anéis. Vejamos agora que α^* satisfaz os axiomas que caracterizam uma ação parcial. De fato,

(i) $\Delta_1 = \Delta 1_R = C_B(T)1_R = \Delta$ e $\alpha_1^* = \beta_1^*|_\Delta = id_\Delta$.

(ii) $\alpha_g^*(\Delta_{g^{-1}} \cap \Delta_h) = \alpha_g^*(\Delta_{g^{-1}} 1_{g^{-1}} 1_h) = \alpha_g^*(\Delta_{g^{-1}})\alpha_g^*(1_{g^{-1}} 1_h)$ $= \Delta_g \beta_g^*(1_{g^{-1}} 1_h) = \Delta_g 1_g 1_{gh} = \Delta_g \cap \Delta_{gh}$.

(iii) $\alpha_g^* \circ \alpha_h^*(a) = \alpha_g^*(\beta_h^*(a)) = \beta_g^*(\beta_h^*(a)) = \beta_{gh}^*(a) = \alpha_{gh}^*(a)$, para todo $a \in \Delta_{h^{-1}} \cap \Delta_{(gh)^{-1}}$.

(6) Se $G = \{g_1 = 1, g_2, ..., g_n\}$, $e_1^* = 1_A$ e $e_i^* = (1_B - 1_A)(1_B - \beta_{g_2}^*(1_A))...$ $(1_B - \beta_{g_{i-1}}^*(1_A))\beta_{g_i}^*(1_A)$, para todo $i \geq 2$, é imediato verificar que $e_i^* = e_i\delta_1$ e $e_i^* \in \beta_{g_i}^*(\Delta)$ com $e_1 = 1_R$ e $e_i = (1_T - 1_R)(1_T - \beta_{g_2}(1_R))...(1_T - \beta_{g_{i-1}}(1_R))\beta_{g_i}(1_R)$, para todo $i \geq 2$. Então, $1_B = 1_T\delta_1 = \sum_i \beta_{g_i}(1_R)e_i\delta_1$ $= \sum_i (\beta_{g_i}(1_R)\delta_1)(e_i\delta_1) = \sum_i \beta_{g_i}^*(1_A)e_i^* \in \sum_i \beta_{g_i}^*(\Delta)$. Do item 4, segue que Δ, e portanto $\sum_i \beta_{g_i}^*(\Delta)$, são ideais de $C_B(T)$. Consequentemente, $C_B(T) = \sum_i \beta_{g_i}^*(\Delta)$. Finalmente,

$$\begin{aligned}
\Delta \cap \beta_g^*(\Delta) &= C_B(T)1_R \cap \beta_g^*(C_B(T)1_R) = C_B(T) \cap \beta_g^*(C_B(T))\beta_g^*(1_R) \\
&= C_B(T)1_R \cap C_B(T)\beta_g^*(1_R) = C_B(T)1_R\beta_g^*(1_R) \\
&= C_B(T)\alpha_g(1_R 1_{g^{-1}}) = C_B(T)1_g = \Delta 1_g = \Delta_g.
\end{aligned}$$

(7) Primeiramente observemos que para todo $a \in \Delta_{g^{-1}} = \Delta 1_{g^{-1}} = 1_{g^{-1}}\Delta$

temos:

$$\begin{aligned}
(1_g\delta_g)a(1_{g^{-1}}\delta_{g^{-1}}) &= (1_T\alpha_g(1_{g^{-1}})\delta_g)a(1_{g^{-1}}1_T\delta_{g^{-1}})\\
&= (1_T\delta_g)(1_{g^{-1}}a1_{g^{-1}})(1_T\delta_{g^{-1}}) = \beta_g^*(a) = \alpha_g^*(a),
\end{aligned}$$

para todo $g \in G$. Agora, seja $a \in \Delta^{\alpha^*}$. Então $a(r\delta_1) = (r\delta_1)a$ e $a1_g = \alpha_g^*(a1_{g^{-1}}) = (1_g\delta_g)a(1_{g^{-1}}\delta_{g^{-1}})$ para todo $r \in R$ e $g \in G$. Dessas igualdades obtemos:

$$\begin{aligned}
a(r_g\delta_g) &= (a1_g)(r_g\delta_g) = (1_g\delta_g)a(1_{g^{-1}}\delta_{g^{-1}})(r_g\delta_g)\\
&= (1_g\delta_g)a(\alpha_{g^{-1}}(r_g)\delta_1) = (1_g\delta_g)(\alpha_{g^{-1}}(r_g)\delta_1)a\\
&= (\alpha_g(\alpha_{g^{-1}}(r_g))\delta_g)a = (r_g\delta_g)a,
\end{aligned}$$

ou seja, $a \in C(A)$. Reciprocamente, como $C(A) \subseteq \Delta$ resta-nos verificar que que os elementos de $C(A)$ são fixos pela ação α^*. Mas, para todo $a \in C(A)$, temos

$$\begin{aligned}
\alpha_g^*(a1_{g^{-1}}) &= (1_g\delta_g)a(1_{g^{-1}}\delta_{g^{-1}}) = (1_g\delta_g(1_{g^{-1}}\delta_{g^{-1}}))a\\
&= (1_g\delta_1)a = 1_g a,
\end{aligned}$$

ou seja, $C(A) \subseteq \Delta^{\alpha^*}$. □

A partir de agora denotaremos por Λ o skew anel de grupo parcial $\Delta *_{\alpha^*} G$.

Proposição 2.2.2. *Se Δ é uma extensão α^*-Galois parcial de Δ^{α^*}, então*

(1) A é H-separável sobre R.

(2) $C(A) = C(R)^\alpha$.

(3) $C_\Lambda(C_\Lambda(\Delta)) = \Delta$.

(4) $C(\Lambda) = C(\Delta)^{\alpha^*}$.

Demonstração. (1) Assuma que Δ é uma extensão α^*-Galois parcial sobre $C(A)$, logo existem $a_i, b_i \in \Delta, 1 \leq i \leq n$ tais que para todo $g \in G$,

$$\sum_i a_i \alpha_g^*(1_{g^{-1}} b_i) = \delta_{1,g} 1_g.$$

Considere os seguintes elementos em A:

$$x_{ig} = \alpha_g^*(b_i 1_{g^{-1}})\delta_g \quad e \quad y_{ig} = 1_{g^{-1}}\delta_{g^{-1}}.$$

Vamos verificar que $\sum_{g\in G} x_{ig} \otimes y_{ig} \in C_{A\otimes_R A}(A)$ e que $\sum_i a_i(\sum_{g\in G} x_{ig} \otimes y_{ig})$ $= 1_A \otimes 1_A$. De fato, para $r_h\delta_h \in A$

$$\begin{aligned}
r_h\delta_h(\sum_{g\in G} x_{ig} \otimes y_{ig}) &= \sum_{g\in G} r_h\delta_h 1_g\delta_g b_i \otimes 1_{g^{-1}}\delta_{g^{-1}} \\
&= \sum_{g\in G} r_h\alpha_h(1_g 1_{h^{-1}})\delta_{hg} b_i \otimes 1_{g^{-1}}\delta_{g^{-1}} \\
&= \sum_{g\in G} r_h 1_{hg}\delta_{hg} b_i \otimes 1_{g^{-1}}\delta_{g^{-1}} \\
&= \sum_{k\in G} r_h 1_k\delta_k b_i \otimes 1_{k^{-1}h}\delta_{k^{-1}h} \\
&= \sum_{k\in G} 1_k\delta_k \alpha_{k^{-1}}(r_h 1_k) b_i \otimes 1_{k^{-1}h}\delta_{k^{-1}h} \\
&= \sum_{k\in G} 1_k\delta_k b_i \alpha_{k^{-1}}(r_h 1_k) \otimes 1_{k^{-1}h}\delta_{k^{-1}h} \\
&= \sum_{k\in G} 1_k\delta_k b_i \otimes \alpha_{k^{-1}}(r_h 1_k)\alpha_{k^{-1}}(1_k 1_h)\delta_{k^{-1}h} \\
&= \sum_{k\in G} 1_k\delta_k b_i \otimes \alpha_{k^{-1}}(r_h 1_k)\delta_{k^{-1}h} \\
&= \sum_{k\in G} x_{ik} \otimes 1_{k^{-1}}\delta_{k^{-1}} r_h\delta_h \\
&= (\sum_{k\in G} x_{ik} \otimes y_{ik}) r_h\delta_h.
\end{aligned}$$

Além disso,

$$\begin{aligned}
\sum_i a_i(\sum_{g\in G} x_{ig}\otimes y_{ig}) &= \sum_{i,g} a_i(1_g\delta_g b_i\otimes 1_{g^{-1}}\delta_{g^{-1}})\\
&= \sum_{i,g} a_i 1_g\delta_g b_i 1_{g^{-1}}\otimes 1_{g^{-1}}\delta_{g^{-1}}\\
&= \sum_{i,g} a_i\alpha_g^*(1_{g^{-1}}b_i 1_{g^{-1}})1_g\delta_g\otimes 1_{g^{-1}}\delta_{g^{-1}}\\
&= \sum_{g\in G}(\sum_i a_i\alpha_g^*(1_{g^{-1}}b_i 1_{g^{-1}}))1_g\delta_g\otimes 1_{g^{-1}}\delta_{g^{-1}}\\
&= \sum_{g\in G}\delta_{1,g}1_A 1_g\delta_g\otimes 1_{g^{-1}}\delta_{g^{-1}}\\
&= 1_R\delta_1\otimes 1_R\delta_1 = 1_A\otimes 1_A.
\end{aligned}$$

Logo $\{a_i, \sum_{g\in G} x_{ig}\otimes y_{ig}\}$ forma um H-sistema para A sobre R e portanto A é H-separável sobre R .

(2) É imediato que $C(R)^\alpha \subseteq C(A)$. Por outro lado, observe que R é um somando direto de A como um R-módulo à esquerda e portanto decorre de (1) e do Teorema 1.1.18 que $C_A(\Delta) = R$. Assim temos que

$$C(A) \subseteq C_A(\Delta) = R$$

e portanto todo elemento $a \in C(A)$ satisfaz: $a \in R$, $ar = ra$ para todo $r \in R$ e $(a\delta_1)(1_g\delta_g) = (1_g\delta_g)(a\delta_1)$ para todo $g \in G$. Consequentemente temos $a \in C(R)$ e $\alpha_g(a1_{g^{-1}}) = a1_g$, ou seja $a \in C(R)^\alpha$.

(3) Lembre que $\Delta^{\alpha^*} = C(A)$. Como Δ é uma extensão α^*-Galois parcial de $C(A)$, então pelo Teorema 1.2.9 temos que Δ é $C(A)$-módulo projetivo finitamente gerado e $\Lambda \cong End_{C(A)}(\Delta)$. Logo, Δ é um $C(A)$-progerador e pelo Teorema 1.1.8 Λ é Azumaya sobre $C(A)$. Além disso, segue do Teorema 1.2.7 que Δ é separável sobre $C(A)$. Portanto, pelo Teorema 1.1.19 temos $C_\Lambda(C_\Lambda(\Delta)) = \Delta$.

(4) Denotemos por Γ o centralizador $C_\Lambda(\Delta)$ e por α^{**} a ação parcial induzida pela ação parcial α^* em Γ. Então,

$$\begin{aligned} C(\Lambda) &= \Gamma^{\alpha^{**}} = C(\Gamma) \cap \Gamma^{\alpha^{**}} = C(\Gamma)^{\alpha^{**}} = (C_\Lambda(\Gamma) \cap \Gamma)^{\alpha^{**}} \\ &= (C_\Lambda(C_\Lambda(\Delta)) \cap \Gamma)^{\alpha^{**}} = (\Delta \cap \Gamma)^{\alpha^{**}} = C(\Delta)^{\alpha^*}. \end{aligned}$$

□

Proposição 2.2.3. *As seguintes afirmações são equivalentes:*

(1) Δ *é uma extensão* α^**-Galois parcial de* $C(A)$.

(2) Λ *é H-separável sobre* Δ.

Demonstração. (1) $\Rightarrow$ (2) Suponha que Δ é uma extensão α^*-Galois parcial de $\Delta^{\alpha^*} = C(A)$. Logo, Δ é um $C(A)$-módulo projetivo finitamente gerado e $\Lambda = End_{\Delta^{\alpha^*}}(\Delta)$ (pelo Teorema 1.2.9), o que implica que Λ é uma $C(A)$-álgebra Azumaya (pelo Teorema 1.1.8). Desde que Λ é um Δ-módulo projetivo finitamente gerado, decorre do Teorema 1.1.17 que Λ é H-separável sobre Δ.

(2) $\Rightarrow$ (1) Como Λ é H-separável sobre Δ e Δ é um gerador como Δ-módulo à esquerda, então pelo Lema 1.1.14, temos que Δ é um gerador como Λ-módulo à esquerda. Além disso, $C(A) = \Delta^{\alpha^*} \cong End({}_\Lambda\Delta)$ via homomorfismo de $C(A)^{\alpha^*}$-álgebras dado por $\theta(a)(x) = xa$, para todo $a \in \Delta^{\alpha^*}$ e $x \in \Delta$, cuja inversa é dada por $f \mapsto f(1_A)$ para todo $f \in End({}_\Lambda\Delta)$. Consequentemente, segue do Teorema 1.1.11 que Δ é um $C(A)$-módulo projetivo finitamente gerado e $\Lambda = End_{C(A)}(\Delta)$, o que significa que Δ é uma extensão α^*-Galois parcial de $C(A)$ (pelo Teorema 1.2.9). □

Proposição 2.2.4. *Se* A *é H-separável sobre* R *e* $C_\Lambda(C_\Lambda(\Delta)) = \Delta$ *então* Δ *é uma extensão* α^**-Galois parcial de* $C(A)$.

Demonstração. Demonstraremos este resultado em 5 etapas.

Etapa 1: *Λ é separável sobre Δ.*

Como H-separabilidade implica separabilidade (Teorema 1.1.15) temos que A é separável sobre R e portanto existe $r_0 \in C(R)$ tal que $tr_\alpha(r_0) = 1_R$ (Teorema 1.2.8). Por outro lado, como R é um somando direto de A como R-módulo à esquerda temos também que $C_A(\Delta) = R$ (pelo Teorema 1.1.18) donde segue que

$$C(R) = R \cap C_A(R) = R \cap \Delta = C_A(\Delta) \cap \Delta = C(\Delta).$$

Além disso, para todo $r \in C(R) = C(\Delta)$ temos

$$\begin{aligned} tr_{\alpha^*}(r\delta_1) &= \sum_{g \in G} \alpha_g^*((r\delta_1)1_{g^{-1}}) = \sum_{g \in G} \beta_g^*(r1_{g^{-1}}\delta_1) \\ &= \sum_{g \in G} \beta_g(r1_{g^{-1}})\delta_1 = \sum_{g \in G} \alpha_g(r1_{g^{-1}})\delta_1 = tr_\alpha(r)\delta_1. \end{aligned}$$

Em particular, $tr_{\alpha^*}(r_0\delta_1) = tr_\alpha(r_0)\delta_1 = 1_R\delta_1 = 1_A = 1_\Delta$. Novamente pelo Teorema 1.2.8 segue que Λ é separável sobre Δ.

Etapa 2: *Λ é separável sobre $C(A)$.*

Usando o fato de que R é um somando direto de A como (A, R)-bimódulos, segue do Lema 1.1.20 que Δ é separável sobre $C(A)$. Com isso, pelo Teorema 1.1.21, temos que Λ é separável sobre $C(A)$.

Etapa 3: *Λ é uma $C(A)$-álgebra de Azumaya.*

Resta apenas mostrar que que $C(\Lambda) = C(A)$.

Desde que $C_\Lambda(C_\Lambda(\Delta)) = \Delta$ obtemos, por um raciocínio idêntico ao utilizado na demonstração da Proposição 2.2.2(4), $C(\Lambda) = C(\Delta)^{\alpha^*}$. De $C(\Delta) = C(R)$ segue que $C(\Delta)^{\alpha^*} = C(R)^{\alpha^*}$. Mais ainda, como A é H-separável sobre R, por um raciocínio análogo ao utilizado na demonstração da Proposição 2.2.2(2) obtemos $C(A) = C(R)^\alpha$. Portanto, $C(\Lambda) = C(\Delta)^{\alpha^*} = C(R)^\alpha = C(A) = \Delta^{\alpha^*}$ e consequentemente, Λ é uma $C(A)$-álgebra de Azumaya.

Etapa 4: *Λ é H-separável sobre $C(A)$.*

Decorre imediatamente do fato que toda extensão de Azumaya é H-separável (Proposição 1.1.16) .

Etapa 5: *Δ é uma extensão α^*-Galois parcial de C(A).*

Comecemos por observar que, $\Lambda \supseteq \Delta \supseteq C(A)$, Λ é $C(A)$-álgebra de Azumaya e Λ é projetivo finitamente gerado como Δ-módulo à esquerda, logo pelo Teorema 1.1.17, segue que Λ é H-separável sobre Δ. Portanto, segue da Proposição 2.2.3 que, Δ é uma extensão α^*-Galois parcial de C(A). □

Lema 2.2.5. *$C(A) \subseteq R$ se e somente se $C(A) = C(R)^\alpha$.*

Demonstração. Suponha que $C(A) \subseteq R$. Tome $x \in C(A)$, então x comuta com qualquer elemento de R, bem como com qualquer elemento de G. Então $x \in C(R)$ e $x\delta_g = \delta_g x$ o que implica $x\delta_g = \alpha_g(x1_{g-1})\delta_g$, para todo $g \in G$, donde segue que $\alpha_g(x1_{g-1}) = x1_g$, ou seja $x \in C(R)^\alpha$. Agora, dado $r \in C(R)^\alpha$ temos $r \in C(R)$ e $\alpha_g(r1_{g-1}) = r1_g$, para todo $g \in G$. Seja $\sum_g r_g\delta_g \in A$, então

$$r(\sum_g r_g\delta_g) = \sum_g rr_g\delta_g = \sum_g r_g r\delta_g = \sum_g r_g\alpha_g(r1_{g^{-1}})\delta_g = (\sum_g r_g\delta_g)r.$$

Portanto, $r \in C(A)$. Logo, $C(R)^\alpha = C(A)$.

Reciprocamente, temos que $C(A) = C(R)^\alpha \subseteq R$. □

2.3 Demonstração dos Teoremas

Nesta seção apresentamos as respectivas demonstrações dos Teoremas 2.1.1, 2.1.2, 2.1.3.

Demonstração do Teorema 2.1.1:

(1) $\Rightarrow$ (2) Notemos que A é um R-módulo à esquerda projetivo finitamente gerado. Então, da hipótese sobre A e do Teorema 1.1.17 segue que A

é H-separável sobre R. Além disso R é um somando direto de A como (R, R)-bimódulo, o que implica pela Proposição 1.1.13 que $C_A(R)$ é separável sobre $C(A)$ e $C_A(C_A(R)) = R$. Consequentemente, pelo Teorema 1.1.12 temos que R é também separável sobre $C(A)$. Finalmente, $C(A) = C(R)^\alpha$ pelo Lema 2.2.5.

(2) $\Rightarrow$ (3) Procederemos por etapas.

Etapa 1: *A é uma álgebra de Azumaya e $C(A) = C(R)^\alpha$ (ou seja,* (2) $\Rightarrow$ (1)*).*

Comecemos por observar que extensões H-separáveis são, em particular, separáveis (Teorema 1.1.15). Logo, pela Proposição 1.1.21, segue que A é separável sobre $C(R)^\alpha$. Por outro lado, decorre da H-separabilidade de A sobre R, pelo mesmo raciocínio usado acima, que $C_A(C_A(R)) = R$ e consequentemente $C(A) \subseteq R$, ou seja, $C(A) = C(R)^\alpha$ pelo Lema 2.2.5.

Etapa 2: *$End_{C(R)^\alpha}(R)$ é uma $C(R)^\alpha$-álgebra de Azumaya.*

Decorre da etapa 1 e do Teorema 1.1.7 que A é um $C(R)^\alpha$-módulo projetivo finitamente gerado. Como R é um $C(R)^\alpha$-somando direto de A, segue que R também é projetivo finitamente gerado sobre $C(R)^\alpha$. Portanto $End_{C(R)^\alpha}(R)$ é uma $C(R)^\alpha$-álgebra de Azumaya pela Proposição 1.1.8.

Etapa 3: *$C_{End_{C(R)^\alpha}(R)}(A) = End_A(R) \simeq (R^\alpha)^{op}$ como $C(R)^\alpha$-álgebras.*

A primeira igualdade é imediata. Por $(R^\alpha)^{op}$ denotamos o anel oposto de R^α. Observemos que a aplicação $j : A \to End(R_{R^\alpha})$, $j(\sum_{g \in G} r_g \delta_g)(r) = \sum_{g \in G} r_g \alpha_g(r 1_{g^{-1}})$, é um homomorfismo de anéis e de R-módulos à esquerda. Em particular, R é um A-módulo à esquerda via j. Como R tem uma estrutura natural de $(R^\alpha)^{op}$-módulo à esquerda, via a mulplicação à direita, compatível com a estrutura de A-módulo à esquerda via j, segue que R é um $((R^\alpha)^{op}, A)$-bimódulo. Isto assegura que a aplicação $\theta : (R^\alpha)^{op} \to End_A(R)$, dada por $\theta(r)(x) = rx$, é um bem definido homomorfismo de $C(R)^\alpha$-álgebras. A inversa de θ é dada pela aplicação $f \mapsto f(1_R)$ para todo $f \in End_A(R)$.

Etapa 4: *R é uma extensão α-Galois parcial de R^α e R^α é uma álgebra de Azumaya e $C(R^\alpha) = C(R)^\alpha$.*

Desde que R é um gerador na categoria dos R-módulos à esquerda e A é H-separável sobre R, segue do Lema 1.1.14 que R é um gerador na categoria dos A-módulos à esquerda. Consequentemente decorre do Teorema 1.1.11 que R é um R^α-módulo à direita projetivo finitamente gerado e j é um isomorfismo, ou seja, R é uma extensão α-Galois parcial de R^α pelo Teorema 1.2.9. Já o fato de R^α ser uma álgebra de Azumaya e $C(R^\alpha) = C(R)^\alpha$ é uma consequência imediata das etapas 1,2 e 4 e do Teorema 1.1.12.

(3) $\Rightarrow$ (1) Pelo Teorema 1.2.9 temos que R é um R^α-módulo à direita projetivo finitamente gerado e $A \simeq End(R_{R^\alpha})$ como anéis e portanto como $C(R)^\alpha$-álgebras. Pelo Teorema 1.1.7 temos que R^α é um $C(R^\alpha)$-módulo projetivo finitamente gerado. E desde que $C(R^\alpha) = C(R)^\alpha$ temos então que R é um $C(R)^\alpha$-módulo projetivo finitamente gerado. Portanto $End_{C(R)^\alpha}$(R) é uma $C(R)^\alpha$-álgebra de Azumaya, conforme Proposição 1.1.8. Finalmente $End(R_{R^\alpha}) = C_{End_{C(R)^\alpha}(R)}(R^\alpha)$. De fato, basta observar que $End(R_{R^\alpha})$ é uma subálgebra de $End_{C(R)^\alpha}(R)$ e um (R^α, R^α)-bimódulo via as ações definidas por $xf : r \mapsto f(rx)$ e $fx : r \mapsto f(r)x$, para todo $f \in End(R_{R^\alpha})$, $x \in R^\alpha$ e $r \in R$. Portanto, pelo Teorema 1.1.12 segue que A é uma álgebra de Azumaya e $C(A) = C(R)^\alpha \subseteq R$.

(1) $\Rightarrow$ (4) Observemos que as afirmações anteriores são equivalentes, portanto, conforme será demonstrado a seguir, esta implicação decorre imediatamente do Teorema 2.1.2.

(4) $\Rightarrow$ (3) Basta observar que como $C_R(R^\alpha)$ é uma extensão α-Galois parcial de $C(A)$, existem elementos $x_i, y_i \in C_R(R^\alpha) \subseteq R$ com $1 \leq i \leq n$ tais que $\sum_i x_i\alpha_g(y_i 1_{g^{-1}}) = \delta_{1,g}1_g$ para todo $g \in G$. Donde segue que R é α-Galois parcial sobre R^α. $\square$

Para o teorema seguinte observemos primeiramente que α induz, por restrição, uma ação parcial de G sobre $E = C_R(R^\alpha)$ (ver Proposição 1.2.11).

Demonstração do Teorema 2.1.2:

Decorre das equivalências (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) do Teorema 2.1.1 que R^α é uma $C(A)$-álgebra de Azumaya e do Teorema 1.1.12 que $C_A(R^\alpha)$ é uma $C(A)$-álgebra de Azumaya e $A \simeq R^\alpha \otimes_{C(A)} C_A(R^\alpha)$, mas $C_A(R^\alpha) = C_R(R^\alpha) *_\alpha G = E *_\alpha G$ o que demonstra as afirmações (1) e (2).

Para demonstrar a afirmação (3) observemos que para todo $x \in R^\alpha$,

$$(\sum_{g\in G} r_g\delta_g)x = x(\sum_{g\in G} r_g\delta_g),$$

ou seja,

$$\sum_{g\in G} r_g x\delta_g = \sum_{g\in G} x r_g\delta_g$$

o que significa que $r_g x = x r_g$ para todo $g \in G$ e isto ocorre se e somente se $r_g \in C_R(R^\alpha)$ para todo $g \in G$. Além disso,

$$C(E *_\alpha G) = C(A) = C(R^\alpha) \subseteq C_R(R^\alpha) = E.$$

Logo, $E *_\alpha G$ satisfaz as condições do Teorema 2.1.1((1) $\Leftrightarrow$ (3)) e por conseguinte E é uma extensão α-Galois parcial de $C(A)$. $\square$

Demonstração do Teorema 2.1.3:

(1) $\Leftrightarrow$ (2) Segue imediatamente da Proposição 2.2.3.

(1) $\Rightarrow$ (3) Segue da Proposição 2.2.2.

(3) $\Rightarrow$ (4) e (4) $\Rightarrow$ (1) Seguem conforme a demonstração da Proposição 2.2.4, etapas 3, 4 e 5. $\square$

A seguir temos uma consequência do Teorema 2.1.1, a qual estende um resultado similar de Ikehata [23] ao contexto de ações parciais de grupos.

Corolário 2.3.1. *Suponha que R é comutativo. Então as seguintes afirmações são equivalentes:*

(1) A é uma álgebra de Azumaya.

(2) A é H-separável sobre R.

(3) R é uma extensão de Galois parcial sobre R^α.

Demonstração. Pelo Teorema 1.2.7 toda extensão α-Galois parcial é separável. Como R é comutativo R^α é álgebra de Azumaya sobre si mesma e $C(R^\alpha) = R^\alpha = C(R)^\alpha$. Da H-separabilidade de A sobre R decorre que $C(A) \subseteq C_A(C_A(R)) = R$. Portanto o Teorema 2.1.1 se aplica e temos as equivalências desejadas. $\square$

Observe que no Corolário 2.3.1, não temos a afirmação (4). Neste caso, como R é comutativo as afirmações 3 e 4 do Teorema 2.1.1 são coincidentes.

Capítulo 3

Extensões de Azumaya e Correspondência de Galois Parcial

Em todo este capítulo H denotará uma álgebra de Hopf de dimensão finita sobre um corpo $\mathbf{k}$ e A denotará um H-módulo álgebra parcial à esquerda via a ação parcial $\alpha : H \otimes A \to A$, $h \otimes a \mapsto h \cdot a$. Recordemos que $\otimes$ denota o produto tensorial sobre $\mathbf{k}$.

Pelo Teorema 1.4.14, sempre existe uma envolvente (B, β) para (A, α). Em particular, B é um H-módulo álgebra à esquerda via a ação $\beta : H \otimes B \to B$, $h \otimes b \mapsto h \triangleright b$, tal que $h \cdot a = 1_A(h \triangleright a)$, para qualquer $a \in A$ e $h \in H$.

Sempre que necessário usaremos a identificação de A com sua imagem no produto smash parcial $A\#_\alpha H$, via $a \mapsto a\#_\alpha 1_H$. Denotaremos por $C(A\#_\alpha H)$ o centro de $A\#_\alpha H$ e por Δ o centralizador $C_{A\#_\alpha H}(A)$ de A em $A\#_\alpha H$ e denotaremos por Δ_H a comultiplicação da álgebra de Hopf H.

Nosso propósito neste capítulo é apresentar condições necessárias e suficientes para que o produto smash parcial $A\#_\alpha H$ seja uma álgebra separável sobre seu centro $C(A\#_\alpha H)$ em termos de Hirata-separabilidade, separabilidade e condições de Galois-Hopf parciais. Também estabelecemos correspondências de Galois para extensões Galois-Azumaya-Hopf parciais.

3.1 Caracterização de Extensões Galois-Hopf Parciais

Nesta seção trataremos de provar um teorema que nos fornece uma série de caracterizações para extensões Galois-Hopf parciais.

Os produtos smash global $W = B\#_\beta H$ e parcial $V = A\#_\alpha H$ são módulos à esquerda sobre si mesmos via a multiplicação à esquerda. Denotamos os respectivos subespaços dos elementos invariantes por

$$W^H = \{w \in W \mid hw := (1_A\#_\beta h)w = \varepsilon_H(h)w, \forall h \in H\}$$

e

$$V^{\underline{H}} = \{v \in V \mid hv := (1_A\#_\alpha h)v = (h \cdot 1_A)v, \forall h \in H\}.$$

Lema 3.1.1. *Seja A um H-módulo álgebra parcial. Então*

$$(A\#_\alpha H)^{\underline{H}} \supseteq (1_A\#_\alpha \int_H^l)(A\#_\alpha 1_H).$$

Demonstração. Sejam $(1_A\#_\alpha t)(a\#_\alpha 1_H) \in (1_A\#_\alpha \int_H^l)(A\#_\alpha 1_H)$ e $h \in H$, então

$$\begin{aligned} h \cdot ((1_A\#_\alpha t)(a\#_\alpha 1_H)) &= (1_A\#_\alpha h)(1_A\#_\alpha t)(a\#_\alpha 1_H) \\ &= (\sum h_1 \cdot 1_A\#_\alpha h_2 t)(a\#_\alpha 1_H) \\ &= (\sum h_1 \cdot 1_A\#_\alpha \varepsilon_H(h_2)t)(a\#_\alpha 1_H) \\ &= (h \cdot 1_A)(1_A\#_\alpha t)(a\#_\alpha 1_H). \end{aligned}$$

□

A inclusão contrária do Lema 3.1.1 vale no caso em que a álgebra de Hopf age globalmente ([26, Lemma 4.3]), no entanto no caso parcial conseguimos obter a igualdade somente sob certas condições conforme veremos a seguir.

O resultado que obtivemos é consequência imediata dos seguintes dois lemas.

Lema 3.1.2. $1_A W 1_A = V$ *e* $1_A W^H 1_A \subseteq V^{\underline{H}}$.

Demonstração. Note que $W = B \otimes H$, $V = (A \otimes H)(1_A \otimes 1_H)$ e $A = 1_A B$. Consequentemente,

$$\begin{aligned} V &= (A \otimes H)(1_A \otimes 1_H) = (1_A B \otimes H)(1_A \otimes 1_H) \\ &= (1_A \otimes 1_H)(B \otimes H)(1_A \otimes 1_H) = 1_A W 1_A \end{aligned}$$

Além disso, para todo $a \#_\alpha g \in V$ e $h \in H$,

$$\begin{aligned} h(a \#_\alpha g) &= \sum (h_1 \cdot a) \#_\alpha h_2 g = \sum (h_1 \cdot a) \otimes h_2 g)(1_A \otimes 1_H) \\ &= \sum (1_A (h_1 \triangleright a) \otimes h_2 g)(1_A \otimes 1_H) \\ &= \sum (1_A \otimes 1_H)((h_1 \triangleright a) \otimes h_2 g)(1_A \otimes 1_H) \\ &= 1_A (h(a \#_\beta g)) 1_A. \end{aligned}$$

Logo, dado $w = b \#_\beta g \in W^H$ temos

$$\begin{aligned} 1_A w 1_A &= (1_A \#_\beta 1_H)(b \#_\beta g)(1_A \#_\beta 1_H) = (1_A b \#_\beta g)(1_A \#_\beta 1_H) \\ &= \sum 1_A b (g_1 \triangleright 1_A) \#_\beta g_2 = \sum a (g_1 \cdot 1_A) \otimes g_2 \\ &= a \#_\alpha g \qquad (\text{com } a = 1_A b) \end{aligned}$$

e portanto

$$\begin{aligned} h(a \#_\alpha g) &= 1_A (hw) 1_A = \sum 1_A \left((h_1 \triangleright a) \#_\beta h_2 g \right) 1_A \\ &= \sum 1_A \left((h_1 \triangleright (1_A b)) \#_\beta h_2 g \right) 1_A \\ &= \sum 1_A \left((h_1 \triangleright 1_A)(h_2 \triangleright b) \#_\beta h_3 g \right) 1_A \end{aligned}$$

$$
\begin{aligned}
&= \sum (1_A(h_1 \triangleright 1_A))(h_2(b\#_\beta g))1_A \\
&= \sum (h_1 \cdot 1_A)\varepsilon_H(h_2)(b\#_\beta g)1_A \\
&= ((h \cdot 1_A)b \otimes g)(1_A \otimes 1_H) \\
&= \sum (h \cdot 1_A)b(g_1 \triangleright 1_A) \otimes g_2 \\
&= \sum (h \cdot 1_A)1_A b 1_A(g_1 \triangleright 1_A) \otimes g_2 \\
&= \sum (h \cdot 1_A)(a(g_1 \cdot 1_A) \otimes g_2) \\
&= (h \cdot 1_A)(a\#_\alpha g)
\end{aligned}
$$

para todo $h \in H$, o que conclui a demonstração. $\square$

Para o que se segue tomemos $0 \neq t \in \int_H^l$ e consideremos as aplicações traço $\hat{t}_W : W \to W$ e $\hat{t}_V : V \to V$ respectivamente definidas por $\hat{t}_W(w) = tw$ e $\hat{t}_V(v) = tv$ para todo $w \in W$ e $v \in V$. Seja $W_A := A\#_\beta H \subseteq W$.

Lema 3.1.3. *(1) $\hat{t}_V(V) = 1_A\hat{t}_W(W_A)1_A$.*

(2) $\hat{t}_W$ é uma aplicação W^H-linear à esquerda e à direita de W em W^H.

(3) $\hat{t}_V$ é uma aplicação $V^{\underline{H}}$-linear à esquerda e à direita de V em $V^{\underline{H}}$.

Demonstração. (1) Decorre imediatamente do que vimos na demonstração do Lema 3.1.2 pois para todo $v = a\#_\alpha g \in V$ temos $\hat{t}_V(v) = t(a\#_\alpha g) = 1_A(t(a\#_\beta g))1_A = 1_A\hat{t}_W(a\#_\beta g)1_A$.

(2) Dados $w \in W$, $w', w'' \in W^H$ e $h \in H$ temos $h(tw) = (ht)w = \varepsilon_H(h)(tw)$ e $t(w'ww'') = \sum(t_1w')(t_2w)(t_3w'') = \sum(\varepsilon_H(t_1)w')(t_2w)(\varepsilon_H(t_3)w'') = w'(tw)w''$.

(3) Decorre de (1) e (2). $\square$

Corolário 3.1.4. *Se $\hat{t}_V$ é sobrejetor então $1_AW^H1_A = V^{\underline{H}}$. Em particular, neste caso $V^{\underline{H}} = (1_A\#_\alpha t)(A\#_\alpha 1_H)$.*

Demonstração. É suficiente observar que $V^{\underline{H}} = \hat{t}_V(V) = 1_A\hat{t}_W(W_A)1_A \subseteq 1_A\hat{t}_W(W)1_A \subseteq 1_AW^H1_A \subseteq V^{\underline{H}}$.

Agora, como $W^H = (1_B\#_\beta t)(B\#_\beta 1_H)$ (confira [26, Lemma 4.3]) temos então $V^{\underline{H}} = 1_A(1_B\#_\beta t)(B\#_\beta 1_H)1_A = (1_A\otimes 1_H)(1_B\otimes t)(B\otimes 1_H)(1_A\otimes 1_H) = (1_A\otimes t)(A\otimes 1_H)(1_A\otimes 1_H) = (1_A\otimes t)(A\#_\alpha 1_H) = (1_A\otimes t)((1_A\#_\alpha 1_H)(A\#_\alpha 1_H)) = ((1_A\otimes t)(1_A\otimes 1_H))(A\#_\alpha 1_H) = (1_A\#_\alpha t)(A\#_\alpha 1_H)$. □

A seguir exibiremos alguns exemplos onde ocorre a igualdade

$$(A\#_\alpha H)^{\underline{H}} = (1_A\#_\alpha \int_H^l)(A\#_\alpha 1_H). \tag{3.1.1}$$

Exemplos:

1) Álgebra do Grupo. Sejam A uma $\mathbf{k}$-álgebra, G um grupo finito e $\alpha = (\{D_g\}_{g\in G}, \{\alpha_g\}_{g\in G})$ uma ação parcial de G em A. Suponha que cada D_g é unitário com unidade 1_g. Por [7] sabemos que $H = \mathbf{k}G$ age parcialmente em A via ação dada por

$$g\cdot a = \alpha_g(a1_g^{-1}).$$

Além disso, H age em $A\#_\alpha(\mathbf{k}G)$ via a multiplicação, isto é,

$$h\cdot(a\#_\alpha g) = (1_A\#_\alpha h)(a\#_\alpha g) = \alpha_h(a1_{h^{-1}})\#_\alpha hg,$$

para todos $g, h \in G$.

Também é sabido que $\int_H^l = kt$, onde $0 \neq t = \sum_{g\in G} g$. Pelo Lema 3.1.1 temos que $(1_A\#_\alpha \int_H^l)(A\#_\alpha 1_H) \subseteq (A\#_\alpha H)^{\underline{H}}$. Reciprocamente, dado $x = \sum_{g\in G} a_g\#_\alpha g \in (A\#_\alpha H)^{\underline{H}}$ temos que $h\cdot x = (h\cdot 1_A)x$, para todo

$h \in H$. Então, para todo $h \in G$

$$
\begin{aligned}
& \sum_{g\in G} (1_A \#_\alpha h)(a_g \#_\alpha g) = \sum_{g\in G}(h \cdot 1_A)(a_g \#_\alpha g) \\
\Leftrightarrow \quad & \sum_{g\in G} \alpha_h(a_g 1_{h^{-1}}) \#_\alpha hg = \sum_{g\in G}(h \cdot 1_A) a_g \#_\alpha g \\
\Leftrightarrow \quad & \sum_{l\in G} \alpha_h(a_{h^{-1}l} 1_{h^{-1}}) \#_\alpha l = \sum_{l\in G}(h \cdot 1_A) a_l \#_\alpha l \\
\Leftrightarrow \quad & \alpha_h(a_{h^{-1}l} 1_{h^{-1}}) = (h \cdot 1_A) a_l, \quad \text{para todo } l \in G.
\end{aligned}
$$

Tomando $h = l$ obtemos $\alpha_l(a_1 1_{l^{-1}}) = (l \cdot 1_A) a_l = 1_l a_l$ para todo $l \in G$. Donde segue que,

$$
\begin{aligned}
\sum_{g\in G} a_g \#_\alpha g &= \sum_{g\in G} a_g 1_g \otimes g = \sum_{g\in G} \alpha_g(a_1 1_{g^{-1}}) \otimes g \\
&= \sum_{g\in G} (1_A \otimes g)(a_1 \otimes 1_H) = (1_A \otimes t)(a_1 \otimes 1_H) \\
&= (1_A \otimes t)(1_A \otimes 1_H)(a_1 \otimes 1_H)(1_A \otimes 1_H) \\
&= (1_A \#_\alpha t)(a_1 \#_\alpha 1_H).
\end{aligned}
$$

Logo, $x \in (1_A \#_\alpha \int_H^l)(A \#_\alpha 1_H)$.

2) Álgebra de Sweedler. A álgebra de Sweedler é a álgebra de Hopf gerada pelos seguintes elementos $H = \{1, c, x, cx\}$ que satisfazem as seguintes relações:

$$c^2 = 1, x^2 = 0, xc = -cx.$$

A estrutura de álgebra de Hopf é dada por:

$$
\begin{aligned}
\Delta_H(c) &= c \otimes c, \quad \Delta_H(x) = c \otimes x + x \otimes 1, \\
\varepsilon_H(c) &= 1, \quad \varepsilon_H(x) = 0 \\
S_H(c) &= c, \quad S_H(x) = xc.
\end{aligned}
$$

Tome A=**k** um corpo (ou anel comutativo com unidade). Seja

$$e = e_\xi = \frac{1}{2} + \frac{1}{2}c + \xi cx \in H.$$

Fazendo as contas vemos que e é um idempotente de H e que satisfaz $e \otimes e = \Delta_H(e)(e \otimes 1_H)$.
Então H coage parcialmente em A via

$$\begin{aligned} \overline{\rho} : A &\rightarrow A \otimes H \\ a &\mapsto a \otimes e. \end{aligned}$$

Como H coage parcialmente à direita em A, temos, pela Proposição 1.4.8, que $H^* = \{1^*, c^*, x^*, z^* = (cx)^*\}$ age parcialmente à esquerda em A, com ação $\alpha : H^* \otimes A \rightarrow A$ induzida por $\overline{\rho}$ da seguinte forma

$$\alpha(h^* \otimes a) := h^* \cdot a = ah^*(e).$$

Os elementos de H^* satisfazem a seguinte tábua de multiplicação:

	1^*	c^*	x^*	z^*
1^*	1^*	0	0	z^*
c^*	0	c^*	x^*	0
x^*	x^*	0	0	0
z^*	0	z^*	0	0

Lembremos que:

$$\begin{aligned} \Delta_{H^*}(f) &= \sum f_1 \otimes f_2 \\ \varepsilon_{H^*}(f) &= f(1_H) \\ S_{H^*}(f) &= f \circ S_H. \end{aligned}$$

Nesta situação, $A\#_\alpha H^* = (A \otimes H^*)(1_A \otimes 1_{H^*}) = (1_{\mathbf{k}} \otimes H^*)(1_{\mathbf{k}} \otimes 1_{H^*})$ onde os elementos básicos são da forma $(1_{\mathbf{k}} \otimes h^*)(1_{\mathbf{k}} \otimes 1_{H^*})$. A estrutura de álgebra de Hopf para H^* é dada por

$$\begin{aligned}
\Delta_{H^*}(1^*) &= 1^* \otimes 1^* + c^* \otimes c^*, \quad \varepsilon_{H^*}(1^*) = 1,\\
\Delta_{H^*}(c^*) &= 1^* \otimes c^* + c^* \otimes 1^*, \quad \varepsilon_{H^*}(c^*) = 0,\\
\Delta_{H^*}(x^*) &= 1^* \otimes x^* - c^* \otimes z^* + x^* \otimes 1^* + z^* \otimes c^*, \quad \varepsilon_{H^*}(x^*) = 0,\\
\Delta_{H^*}(z^*) &= 1^* \otimes z^* - c^* \otimes x^* + x^* \otimes c^* + z^* \otimes 1^*, \quad \varepsilon_{H^*}(z^*) = 0,\\
S_{H^*}(1^*) &= 1^*, \quad S_{H^*}(c^*) = c^*, \quad S_{H^*}(x^*) = z^*, \quad S_{H^*}(z^*) = x^*.
\end{aligned}$$

Os elementos de $A\#_\alpha H^*$ que são invariantes pela ação parcial de H^* são os elementos que satisfazem a seguinte condição:

$$g^* * h^* = (g^* \cdot 1_{\mathbf{k}})h^* = g^*(e)h^*.$$

Observemos que

- $0 = x^*(e)1^* = x^*(e) \otimes 1^* \neq x^* \cdot (1_A\#_\alpha 1^*) = 1^*(e)x^*$,
- $x^* \cdot (1_A\#_\alpha c^*) = -c^*(e) \otimes z^* + x^*(e) \otimes 1^* = -\frac{1}{2}z^* \neq 0 = x^*(e)c^*$,
- $x^* \cdot (1_A\#_\alpha x^*) = z^*(e)x^* \neq 0 = x^*(e)x^*$,

donde segue que os elementos $1_A\#_\alpha 1^*, 1_A\#_\alpha c^*, 1_A\#_\alpha x^*$ não são invariantes pela ação $A\#_\alpha H^*$ em $A\#_\alpha H^*$. Porém $1_A\#_\alpha z^* \in (A\#_\alpha H^*)^{\underline{H}}$. De fato,

- $1^* \cdot (1_A\#_\alpha z^*) = \frac{1}{2}z^* = 1^*(e)z^*$,
- $c^* \cdot (1_A\#_\alpha z^*) = \frac{1}{2}z^* = c^*(e)z^*$,
- $x^* \cdot (1_A\#_\alpha z^*) = 0 = x^*(e)z^*$,
- $z^* \cdot (1_A\#_\alpha z^*) = z^*(e) \otimes z^* = z^*(e)z^*$.

Sendo assim, $(A\#_\alpha H^*)^{\underline{H}}$ é o $\mathbf{k}$-subespaço vetorial gerado pelo elemento $1\#_\alpha z^*$.

Vejamos agora que $z^* \in \int_{H^*}^{l}$, ou seja que $g^* * z^* = \varepsilon_{H^*}(g^*)z^*$ para todo $g^* \in H^*$:

- $1^* * z^* = z^* = \varepsilon_{H^*}(1^*)z^*$,
- $c^* * z^* = 0 = \varepsilon_{H^*}(c^*)z^*$,
- $x^* * z^* = 0 = \varepsilon_{H^*}(x^*)z^*$,
- $z^* * z^* = 0 = \varepsilon_{H^*}(z^*)z^*$.

E como $1\#_\alpha z^* = (1_A\#_\alpha z^*)(1_{\mathbf{k}}\#_\alpha 1_{H^*}) \in (1_A\#_\alpha \int_{H^*}^{l})(A\#_\alpha 1_{H^*})$ temos que $(A\#_\alpha H^*)^{\underline{H^*}} = (1_A\#_\alpha \int_{H^*}^{l})(A\#_\alpha 1_{H^*})$. $\square$

Recordemos que, pelo Lema 1.4.9, um H-módulo álgebra parcial à esquerda A é um H^*-comódulo álgebra à direita e reciprocamente, assim como $A^{\underline{coH^*}} = A^{\underline{H}}$.

Teorema 3.1.5. *Sejam H uma álgebra de Hopf de dimensão finita, $0 \neq t \in \int_{H}^{l}$ e A um H-módulo álgebra parcial à esquerda. Considere as seguintes afirmações:*

(1) A é uma extensão H^*-Galois parcial à direita de $A^{\underline{H}}$.

(2) A é $A^{\underline{H}}$ -módulo à direita projetivo finitamente gerado e a aplicação $\pi : A\#_\alpha H \to End(A_{A^{\underline{H}}})$ dada por $\pi(a\#_\alpha h)(b) := (a\#_\alpha h) \triangleright b = a(h \cdot b)$ é um isomorfismo de álgebras e de A-módulos à esquerda.

(3) A é $A^{\underline{H}}$-módulo à direita projetivo finitamente gerado e para todo $A\#_\alpha H$-módulo à esquerda M a aplicação $\mu : A \otimes_{A^{\underline{H}}} M^{\underline{H}} \to M$, dada por $\mu(a \otimes h) = am$, é um isomorfismo de $A\#_\alpha H$-módulos à esquerda.

(4) A aplicação $[,] : A \otimes_{A^{\underline{H}}} A \to A\#_\alpha H$ dada por $[a, b] = atb$ é sobrejetora.

(5) A é um gerador para a categoria dos $A\#_\alpha H$-módulos à esquerda.

(6) Existem $x_1, ..., x_n, y_1, ..., y_n \in A$ tais que para qualquer $h \in H$, temos $\sum x_i(h \cdot y_i) = T(h)1_A$, com $0 \neq T \in \int_{H^*}^r$.

(7) $AtA = A\#_\alpha H$.

Então: (1) $\Leftrightarrow$ (4) $\Leftrightarrow$ (7),(4) $\Leftrightarrow$ (5), (2) $\Leftrightarrow$ (5) *e* (1) $\Rightarrow$ (6) $\Rightarrow$ (2) $\Rightarrow$ (3). *Além disso, se a igualdade 3.1.1 é satisfeita então todas as afirmações são equivalentes.*

Demonstração. (2) $\Leftrightarrow$ (5) Comecemos por observar que A tem uma estrutura de $(A^{\underline{H}})^{op}$-módulo à esquerda, via a multiplicação à direita, a qual é compatível com a sua estrutura de $A\#_\alpha H$-módulo à esquerda via π, isto é, A é um $((A^{\underline{H}})^{op}, A\#_\alpha H)$-bimódulo. De fato, pois para quaisquer $a, b, x \in A$ e $h \in H$ temos

$$\begin{aligned} a^{op} \cdot [(b\#_\alpha h) \cdot x] &= a^{op} \cdot (b(h \cdot x)) = b(h \cdot x)a \\ &= b\sum(h_1 \cdot x)(h_2 \cdot 1_A)a = b\sum(h_1 \cdot x)(h_2 \cdot a) \\ &= b(h \cdot xa) = (b\#_\alpha h) \cdot (xa) = (b\#_\alpha h) \cdot (a^{op} \cdot x). \end{aligned}$$

Pelo Lema 1.4.4 temos que $(A^{\underline{H}})^{op} \backsimeq End({}_{A\#_\alpha H}A)$ como anéis. Sendo assim, estamos nas hipóteses do Teorema 1.1.11, donde segue que A é um gerador para a categoria dos $A\#_\alpha H$-módulos à esquerda se e somente se A é $(A^{\underline{H}})^{op}$-módulo à esquerda projetivo finitamente gerado e $A\#_\alpha H \backsimeq End({}_{(A^{\underline{H}})^{op}}A)$ se e somente se A é $A^{\underline{H}}$-módulo à direita projetivo finitamente gerado e $A\#_\alpha H \backsimeq End(A_{A^{\underline{H}}})$.

(4) $\Rightarrow$ (5) Assuma que $[A, A] = A\#_\alpha H = (A \otimes H)(1_A \otimes 1_H)$, ou seja $[,]$ é sobrejetora. Com isso, existem $\{b_i\}$, $\{c_i\} \subseteq A$ tais que $1_A\#_\alpha 1_H = \sum_{i=1}^n b_i t c_i$. Defina $\psi : A^{(n)} \to A\#_\alpha H$ por $\psi(a_1, ..., a_n) = \sum_{i=1}^n a_i t c_i$. Note que ψ é claramente aditiva. Observe ainda que $A^{(n)}$ tem uma estrutura de $A\#_\alpha H$-módulo à esquerda induzida naturalmente pela estrutura de $A\#_\alpha H$-módulo de A. Mostremos que:

(i) ψ é $A\#_\alpha H$-linear à esquerda:

$$\begin{aligned}
\psi((a\#_\alpha h)\triangleright(a_1,...,a_n)) &= \psi((a\#_\alpha h)\triangleright a_1,...,(a\#_\alpha h)\triangleright a_n))\\
&= \psi((ah\cdot a_1,...,ah\cdot a_n)) = \sum_{i=1}^{n}(ah\cdot a_i)tc_i\\
&= \sum_{i=1}^{n} a[(h\cdot a_i)t]c_i\\
&= \sum_{i=1}^{n} a[(h\cdot a_i\#_\alpha 1_H)(1_A\#_\alpha t)]c_i\\
&= \sum_{i=1}^{n} a[(h\cdot a_i\#_\alpha t)]c_i\\
&= \sum_{i=1}^{n} a[(h_1\cdot a_i\#_\alpha \varepsilon_H(h_2)t)]c_i\\
&= \sum_{i=1}^{n} a[(h_1\cdot a_i\#_\alpha h_2 t)]c_i\\
&= \sum_{i=1}^{n} a[(1_A\#_\alpha h)(a_i\#_\alpha t)]c_i\\
&= \sum_{i=1}^{n}(a\#_\alpha h)(a_i t c_i) = (a\#_\alpha h)(\sum_{i=1}^{n} a_i t c_i)\\
&= (a\#_\alpha h)\psi(a_1,...,a_n).
\end{aligned}$$

(ii) ψ é sobrejetora. De fato, seja $a\#_\alpha h \in A\#_\alpha H$. Como $1_A\#_\alpha 1_H = \sum_{i=1}^{n} b_i t c_i$ temos que

$$1_A\#_\alpha 1_H = \sum_{i=1}^{n} b_i t c_i = \psi((b_1,...,b_n)).$$

Sendo assim,

$$\psi(a\#_\alpha h\triangleright(b_1,...,b_n)) = (a\#_\alpha h)\psi(b_1,...,b_n) = (a\#_\alpha h)(1_A\#_\alpha 1_H) = a\#_\alpha h.$$

Portanto, A é gerador para a categoria dos $A\#_\alpha H$-módulos à esquerda.

(4) $\Leftrightarrow$ (7) Basta observar que $AtA = [A, A] = A\#_\alpha H$.

(1) $\Rightarrow$ (6) Suponha que $\beta : A \otimes_{A^{\underline{H}}} A \to \underline{A \otimes H^*}$,dada por $\beta(a \otimes b) = \sum ab_{(0)} \otimes b_{(1)}$, é uma bijeção. Seja $0 \neq T \in \displaystyle\int_{H^*}^{r}$ e considere $\displaystyle\sum_i x_i \otimes y_i \in A \otimes_{A^{\underline{H}}} A$ a imagem inversa de $\sum 1_{A_{(0)}} \otimes T1_{A_{(1)}}$ por β, isto é,

$$\sum 1_{A_{(0)}} \otimes T1_{A_{(1)}} = \sum x_i y_{i_{(0)}} \otimes y_{i_{(1)}}.$$

Note que para qualquer $x \in A$ e $h^* \in H^*$ podemos definir a aplicação $x \otimes h^* : A \otimes_{\mathbf{k}} H \to A \otimes \mathbf{k} \backsimeq A$ por $a \otimes h \mapsto xa \otimes h^*(h) = xah^*(h) \otimes 1_{\mathbf{k}} \backsimeq xah^*(h)$. Logo, para todo $h \in H$ temos

$$(\sum 1_{A_{(0)}} \otimes T1_{A_{(1)}})(1_A \otimes h) \;=\; \sum_{i=1}^{n} x_i y_{i_{(0)}} \otimes y_{i_{(1)}}(h),$$

o que implica que

$$\begin{aligned}
\sum 1_{A_{(0)}} T1_{A_{(1)}}(h) \otimes 1_{\mathbf{k}} &= \sum_{i=1}^{n} x_i y_{i_{(0)}} y_{i_{(1)}}(h) \otimes 1_{\mathbf{k}} \\
\sum 1_{A_{(0)}} \varepsilon_{H^*}(1_{A_{(1)}}) T(h) \otimes 1_{\mathbf{k}} &= \sum_{i=1}^{n} x_i y_{i_{(0)}} y_{i_{(1)}}(h) \otimes 1_{\mathbf{k}} \\
1_A T(h) \otimes 1_{\mathbf{k}} &= \sum_{i=1}^{n} x_i y_{i_{(0)}} y_{i_{(1)}}(h) \otimes 1_{\mathbf{k}}
\end{aligned}$$

donde segue que,

$$1_A T(h) \;=\; \sum_{i=1}^{n} x_i y_{i_{(0)}} y_{i_{(1)}}(h) = \sum_{i=1}^{n} x_i (h \cdot y_i),$$

onde a última igualdade segue da Observação 1.4.7.

$(4) \Leftrightarrow (1)$ Vamos usar o fato de que para $0 \neq t \in \int_H^l$ a aplicação

$$\theta : H^* \to H$$

dada por $\theta(h^*) = t \leftharpoonup h^* = \sum h^*(t_1)t_2$ é um isomorfismo de H^*-módulos de Hopf à direita (decorre do Teorema 1.3.13). Observemos agora que

$$\begin{aligned}
(id_A \otimes \theta) \circ \beta(a \otimes b) &= (id_A \otimes \theta)(\beta(a \otimes b)) \\
&= (id_A \otimes \theta)(\sum ab_{(0)} \otimes b_{(1)}) \\
&= \sum ab_{(0)} \otimes \theta(b_{(1)}) = \sum ab_{(0)} \otimes (t \leftharpoonup b_{(1)}) \\
&= \sum ab_{(0)} \otimes b_{(1)}(t_1)t_2 = \sum ab_{(0)}b_{(1)}(t_1) \otimes t_2 \\
&= \sum a(t_1 \cdot b) \otimes t_2 = (a\#_\alpha t)(b\#_\alpha 1_H) = atb = [a, b]
\end{aligned}$$

Como θ é bijeção, segue $[,]$ é sobrejetora se e somente se β é sobrejetora. E assim, pelo Teorema 1.4.10 temos que β é injetora e portanto bijetora. Portanto, $(1) \Rightarrow (4)$. Observe que também temos $(4) \Rightarrow (1)$ pois como H tem dimensão finita, β é injetora sempre que for sobrejetora pelo Teorema 1.4.10.

$(6) \Rightarrow (2)$ Seja $0 \neq T \in \int_{H^*}^r$, ou seja, $Tf = T\varepsilon_{H^*}(f) = Tf(1_H)$, para todo $f \in H^*$. Então,

$$\begin{aligned}
f(\sum T(h_1)h_2) &= \sum T(h_1)f(h_2) = (T * f)(h) = (T\varepsilon_{H^*}(f))(h) \\
&= (Tf(1_H))(h) = T(h)f(1_H) = f(T(h)1_H)
\end{aligned}$$

para todo $h \in H$, $f \in H^*$, donde segue que $\sum T(h_1)h_2 = T(h)1_H$. Considere ainda $t \in \int_H^l$ tal que $T(t) = 1_A$ (isto decorre do Teorema 1.3.13). Vamos mostrar que A é um $A^{\underline{H}}$-módulo á direita projetivo finitamente gerado. Para tanto defina $f_i(x) = t \cdot (y_i x)$, para todo $x \in A$.

(i) $\underline{f_i(x) \in A^{\underline{H}}, \text{ para todo } 1 \leq i \leq n.}$ De fato, seja $h \in H$ qualquer, então

$$\begin{aligned} h \cdot (f_i(x)) &= h \cdot (t \cdot (y_i x)) = \sum (h_1 \cdot 1_A)(h_2 t \cdot (y_i x)) \\ &= \sum (h_1 \cdot 1_A)(\varepsilon_H(h_2) t \cdot (y_i x)) = \sum (\varepsilon_H(h_2) h_1 \cdot 1_A)(t \cdot (y_i x)) \\ &= (h \cdot 1_A)(t \cdot (y_i x)). \end{aligned}$$

(ii) $\underline{f_i \text{ é homomorfismo de } A^{\underline{H}}\text{ -módulos à direita.}}$ De fato, f_i é claramente aditiva e para todo $x \in A$, $a \in A^{\underline{H}}$ e $1 \leq i \leq n$ temos:

$$\begin{aligned} f_i(xa) &= t \cdot (y_i(xa)) = t \cdot ((y_i x)a) = \sum t_1 \cdot (y_i x)(t_2 \cdot a) \\ &= \sum (t_1 \cdot (y_i x))(t_2 \cdot 1_A)a = t \cdot (y_i x)a = f_i(x)a \end{aligned}$$

e portanto para todo $x \in A$, temos

$$\begin{aligned} \sum_i x_i f_i(x) &= \sum_i t \cdot (y_i x) = \sum_{i,t} x_i(t_1 \cdot y_i)(t_2 \cdot x) \\ &= \sum_t (\sum_i x_i(t_1 \cdot y_i))(t_2 \cdot x) = \sum_t T(t_1)(t_2 \cdot x) \\ &= \sum_t T(t_1)t_2 \cdot x = T(t)1_H \cdot x = 1_H \cdot x = x. \end{aligned}$$

Vejamos que $\pi : A\#_\alpha H \to End(A_{A^{\underline{H}}})$ dada por $\pi(a\#_\alpha h)(b) := (a\#_\alpha h) \triangleright b$ é um homomorfismo de A-módulos à esquerda e de álgebras. Note que π está bem definida pois para todo $a \in A$, $h \in H$ e $x \in A^{\underline{H}}$ temos

$$\begin{aligned} \pi(a\#_\alpha h)(bx) &= a(h \cdot (bx)) = \sum a(h_1 \cdot b)(h_2 \cdot x) \\ &= \sum a(h_1 \cdot b)(h_2 \cdot 1_A)x = a(h \cdot b)x \\ &= \pi(a\#_\alpha h)(b)x. \end{aligned}$$

É imediato da definição que π é um homomorfismo de A-módulos à esquerda e que $\pi(1_A \#_\alpha 1_H) = id_A$. Além disso, $\pi(a\#_\alpha h)(b) = (a\#_\alpha h) \triangleright b$ é $\mathbf{k}$-linear e para todos $a\#_\alpha h, b\#_\alpha g$ em $A\#_\alpha H, x \in A$, temos

$$\begin{aligned}
\pi[(a\#_\alpha h)(b\#_\alpha g)](x) &= \pi(\sum a(h_1 \cdot b\#_\alpha h_2 g))(x) = \sum a(h_1 \cdot b)(h_2 g \cdot x) \\
&= \sum a(h_1 \cdot b)(h_2 \cdot 1_A)(h_3 g \cdot x) \\
&= \sum a(h_1 \cdot b)(h_2 \cdot (g \cdot x)) \\
&= a(h \cdot (b(g \cdot x))) = \pi(a\#_\alpha h)(b(g \cdot x)) \\
&= \pi(a\#_\alpha h) \circ \pi(b\#_\alpha g)(x).
\end{aligned}$$

Para a injetividade da aplicação π necessitamos da seguinte igualdade

$$\sum (h \cdot x_i)(ty_i) = \sum_h (h_1 \cdot 1_A) \otimes h_2,$$

onde $ty_i = (1_A \otimes t)(1_A \otimes 1_H)(y_i \otimes 1_H)(1_A \otimes 1_H) = (1_A \otimes t)(y_i \otimes 1_H) = (1_A\#_\alpha t)(y_i\#_\alpha 1_H)$. De fato temos

$$\begin{aligned}
\sum_{i=1}^{n} (h \cdot x_i)(ty_i) &= \sum_{i=1}^{n} (h \cdot x_i)(1_A \otimes t)(y_i \otimes 1_H) \\
&= \sum_{i=1}^{n} \sum_t (h \cdot x_i)(t_1 \cdot y_i \otimes t_2) \\
&= \sum_t (\sum_{i=1}^{n} (h \cdot x_i)(t_1 \cdot y_i \otimes 1_H)(1_A \otimes t_2)) \\
&= \sum_t (\sum_{i=1}^{n} (h \cdot x_i)(t_1 \cdot y_i))t_2 \\
&= \sum_{t,h} (\sum_{i=1}^{n} (h_1 \cdot x_i)(\varepsilon_H(h_2)t_1 \cdot y_i))t_2 \\
&= \sum_{t,h} (\sum_{i=1}^{n} (h_1 \cdot x_i)(h_2 S_H(h_3)t_1 \cdot y_i))t_2
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{t,h}(\sum_{i=1}^{n}(h_1 \cdot x_i)(h_2 \cdot 1_A)(h_3 S_H(h_4)t_1 \cdot y_i))t_2 \\
&= \sum_{t,h}(\sum_{i=1}^{n}(h_1 \cdot x_i)(h_2 \cdot (S_H(h_3)t_1 \cdot y_i)))t_2 \\
&= \sum_{t,h}(\sum_{i=1}^{n} h_1 \cdot (x_i(S_H(h_2)t_1 \cdot y_i)))t_2 \\
&= \sum_{t,h} h_1 \cdot (T(S_H(h_2)t_1)1_A)t_2 \\
&= \sum_{t,h}(h_1 \cdot 1_A)(T(S_H(h_2))t_1)t_2 \\
&\overset{(\star)}{=} \sum_{h}(h_1 \cdot 1_A)h_2 = \sum_{h}(h_1 \cdot 1_A) \otimes h_2.
\end{aligned}
$$

A igualdade $(\star)$ é válida pois S_H é bijetora e

$$
\begin{aligned}
S_H(\sum_t T(S_H(h)t_1)t_2) &= \sum_t T(S_H(h)t_1)S_H(t_2) \\
&= \sum_{h,t} T((S_H(h))_1 t_1)(S_H(h))_2 t_2 S_H(t_3) \\
&= \sum_{h,t} T(S_H(h_1)t_1)S_H(h_2)\varepsilon_H(t_2)1_H \\
&= \sum_{h,t} T(S_H(h_1)t_1\varepsilon_H(t_2))S_H(h_2) \\
&= \sum_{h} T(S_H(h_1)t)S_H(h_2) \\
&= \sum_{h} T(t)\varepsilon_H(S_H(h_1))S_H(h_2) = S_H(h).
\end{aligned}
$$

Observemos que se $\{h_i\}_{i=1}^{n}$ uma base de H sobre $\mathbf{k}$, então todo elemento de $A\#_\alpha H$ é da forma $\sum_{i=1}^{n} a_i\#_\alpha h_i$ onde $a_i \in A$. Usando este fato temos que

$$
\begin{aligned}
\sum_j (\pi(\sum_{i=1}^n a_i \#_\alpha h_i)(x_j))(ty_j) &= \sum_{i,j} a_i(h_i \cdot x_j)(ty_j) \\
&= \sum_i a_i(\sum_j (h_i \cdot x_j)(ty_j)) \\
&= \sum_i a_i(\sum_{h_i} (h_{i_1} \cdot 1_A) \otimes h_{i_2}) \\
&= \sum_{i,h_i} a_i(h_{i_1} \cdot 1_A) \otimes h_{i_2} \\
&= \sum_i a_i \#_\alpha h_i.
\end{aligned}
$$

Portanto, se $\pi(\sum_{i=1}^n a_i \#_\alpha h_i) = 0$ segue que

$$
\sum_i a_i \#_\alpha h_i = \sum_j (\pi(\sum_{i=1}^n a_i \#_\alpha h_i)(x_j))(ty_j) = 0.
$$

Logo $Ker(\pi) = \{0\}$ e portanto temos que π é injetora.

Por fim, mostremos que π é sobrejetora. De fato, dado $\phi \in End(A_{A^{\underline{H}}})$ e tomando $b = \sum_i \phi(x_i) t y_i$ temos:

$$
\begin{aligned}
\pi(b)(x) &= \pi(\sum_i \phi(x_i) t y_i)(x) = \pi(\sum_i \phi(x_i)(1_A \#_\alpha t)(y_i \#_\alpha 1_H))(x) \\
&= \pi(\sum_i \phi(x_i)(t_1 \cdot y_i) \#_\alpha t_2)(x) = \sum_i \phi(x_i) \pi((t_1 \cdot y_i) \#_\alpha t_2)(x) \\
&= \sum_i \phi(x_i)(t \cdot y_i)(t_2 \cdot x) = \sum_i \phi(x_i) t \cdot (y_i x) \\
&= \sum_i \phi(x_i) f_i(x) = \phi(\sum_i x_i f_i(x)) = \phi(x),
\end{aligned}
$$

para todo x em A.

(2) $\Rightarrow$ (3) Como A é projetivo finitamente gerado, existem $x_i \in A, f_i \in Hom(A_{A^{\underline{H}}}, A^{\underline{H}})$, $1 \leq i \leq n$ tais que $\sum_{i=1}^{n} x_i f_i(x) = x$, para todo $x \in A$. Como π é isomorfismo, existe $d_i \in A\#_\alpha H$ tal que $\pi(d_i) = f_i$, para todo $i = 1, .., n$. Comecemos por observar que d_i é invariante pela ação de H no produto smash parcial $A\#_\alpha H$ e $\sum_i x_i d_i = 1_A \#_\alpha 1_H$. De fato,

(i) $\underline{\sum_{i=1}^{n} x_i d_i = 1_A \#_\alpha 1_H}$: Seja x um elemento qualquer de A, então

$$\begin{aligned}
\pi(\sum_{i=1}^{n} x_i d_i)(x) &= \sum_{i=1}^{n} x_i \pi(d_i)(x) = \sum_{i=1}^{n} x_i f_i(x) = x \\
&= 1_A 1_H \cdot x = \pi(1_A \#_\alpha 1_H)(x).
\end{aligned}$$

Como a aplicação π é um isomorfismo, temos que $\sum_{i=1}^{n} x_i d_i = 1_A \#_\alpha 1_H$.

(ii) $\underline{h \cdot d_i = (h \cdot 1_A) d_i}$: Para qualquer elemento h em H e x em A temos

$$\begin{aligned}
\pi(h \cdot d_i)(x) &= \pi((1_A \#_\alpha h) d_i)(x) = \pi(1_A \#_\alpha h) \circ \pi(d_i)(x) \\
&= \pi(1_A \#_\alpha h)(f_i(x)) = h \cdot f_i(x) = (h \cdot 1_A) f_i(x) \\
&= (h \cdot 1_A) \pi(d_i)(x) = \pi((h \cdot 1_A) d_i)(x).
\end{aligned}$$

Seja M um $A\#_\alpha H$-módulo à esquerda. Notemos que $d_i m \in M^{\underline{H}}$ para qualquer $m \in M$ pois

$$h \cdot (d_i m) = (1_A \#_\alpha h)(d_i m) = ((1_A \#_\alpha h) d_i) m = ((h \cdot 1_A) d_i) m = (h \cdot 1_A) d_i m,$$

para qualquer $h \in H$.

Além disso, para todo $a \in A$, $m \in M^{\underline{H}}$ e $h \in H$

$$(1_A \#_\alpha h) a m \;=\; (1_A \#_\alpha h)(a \#_\alpha 1_H) m = (\sum h_1 \cdot a \#_\alpha h_2) m$$

$$
\begin{aligned}
&= \sum(h_1 \cdot a)(1_A \#_\alpha h_2)m = \sum(h_1 \cdot a)(h_2 \cdot 1_A)m \\
&= (h \cdot a)m = \pi(1_A \#_\alpha h)(a)m.
\end{aligned}
$$

Donde segue que $\pi(d)(a)m = d(am)$ para todo $d \in A\#_\alpha H$.

Observemos que A é um $A\#_\alpha H$-módulo à esquerda via π, e portanto $A \otimes_{A^{\underline{H}}} M^{\underline{H}}$ tem estrutura de $A\#_\alpha H$-módulo à esquerda. Com isso, para $\mu : A \otimes_{A^{\underline{H}}} M^{\underline{H}} \to M$ dada por $\mu(a \otimes h) = am$ temos:

$$
\begin{aligned}
\mu((a\#_\alpha h)(b \otimes m)) &= \mu(\pi(a\#_\alpha h)(b) \otimes m) = \mu(a(h \cdot b) \otimes m) = a(h \cdot b)m \\
&= \pi(a\#_\alpha h)(b)m = (a\#_\alpha h)(bm) = (a\#_\alpha h)\mu(b \otimes m)
\end{aligned}
$$

Defina $\nu : M \to A \otimes_{A^{\underline{H}}} M^{\underline{H}}$ por $\nu(m) = \sum x_i \otimes d_i m$. Então,

$$
\mu \circ \nu(m) = \mu(\sum x_i \otimes d_i m) = \sum x_i d_i m = (\sum x_i d_i)m = (1_A \#_\alpha 1_H)m = m.
$$

Por outro lado, para todo $a \in A$ e $m \in M^{\underline{H}}$

$$
\begin{aligned}
\nu \circ \mu(a \otimes m) &= \nu(am) = \sum_{i=1}^{n} x_i \otimes d_i(am) = \sum_{i=1}^{n} x_i \otimes (\pi(d_i)(a))m \\
&= \sum_{i=1}^{n} x_i \otimes f_i(a)m = \sum_{i=1}^{n} x_i f_i(a) \otimes m \\
&= (\sum_{i=1}^{n} x_i f_i(a)) \otimes m = a \otimes m.
\end{aligned}
$$

Portanto, μ é um isomorfismo de $A\#_\alpha H$-módulos à esquerda.

Agora, se assumirmos que a igualdade 3.1.1 é satisfeita temos:

(3) $\Rightarrow$ (4) Definamos a seguinte aplicação

$$
\begin{aligned}
\Phi : A &\to (A\#_\alpha H)^{\underline{H}} \\
a &\mapsto (1_A \#_\alpha t)(a\#_\alpha 1_H)
\end{aligned}
$$

com $0 \neq t \in \int_H^l$. Decorre da igualdade 3.1.1 que esta aplicação está bem definida e é sobrejetora. Com isso, a composição

$$\begin{array}{ccccc} A \otimes_{A^{\underline{H}}} A & \stackrel{id_A \otimes \Phi}{\longrightarrow} & A \otimes (A\#_\alpha H)^{\underline{H}} & \stackrel{\mu}{\longrightarrow} & A\#_\alpha H \\ a \otimes b & \mapsto & a \otimes \Phi(b) & \mapsto & a\Phi(b) = atb = [a,b] \end{array}$$

é sobrejetora. E mais, $[,] = \mu \circ (id_A \otimes \Phi)$ é claramente um homomorfismo de A-módulos à esquerda. $\square$

Observação 3.1.6. Para a demonstração do próximo resultado recordemos que:

(i) H é um H^*-módulo à direita via ação $\leftharpoonup$ dada por:

$$h \leftharpoonup h^* = \sum h^*(h_1)h_2.$$

(ii) $A\#_\alpha H$ é um H^*-módulo à direita via ação $\leftharpoonup$ dada por:

$$(a\#_\alpha h) \leftharpoonup h^* = a\#_\alpha(h \leftharpoonup h^*).$$

(iii) As aplicações (ver [5, Section 3])

$$\begin{array}{rcl} [,] : A \otimes_{A^{\underline{H}}} A & \rightarrow & A\#_\alpha H \\ a \otimes b & \mapsto & [a,b] = atb, \\ (,) : A \otimes_{A\#_\alpha H} A & \rightarrow & A^H \\ a \otimes b & \mapsto & (a,b) = \widehat{t}(ab) = t \cdot (ab), \end{array}$$

satisfazem

$$(a,b)c = a[b,c],$$

para quaisquer a, b, $c \in A$.

Teorema 3.1.6. *Sejam H uma álgebra de Hopf, $A \supseteq A^{\underline{H}}$ uma extensão H^*-Galois parcial e $\{x_i, y_i\} \subseteq A$ tal que $\sum_i [x_i, y_i] = 1_A \#_\alpha 1_H$. Então as seguintes afirmações são equivalentes:*

(1) $A \supseteq A^{\underline{H}}$ é separável.

(2) Existe $\omega \in C_{A\#_\alpha H}(A)$ com $\omega \leftharpoonup T = 1_A \#_\alpha 1_H$.

(3) A é um A-bimódulo somando direto de $A\#_\alpha H$.

(4) Existe $c \in A$ tal que $\sum x_i c y_i = 1_A$.

(5) Existe $c \in C_A(A^{\underline{H}})$ tal que $\sum x_i c y_i = 1_A$.

Demonstração. Como A é uma extensão H^*-Galois parcial de $A^{\underline{H}}$, temos pelo Teorema 3.1.5, que $[,]$ é sobrejetora e portanto injetora, pois $(id \otimes \theta) \circ \beta = [,]$ onde $\theta : H^* \to H$ dada por $\theta(h^*) = t \leftharpoonup h^* = \sum h^*(t_1)t_2$ é um isomorfismo de H^*-módulos de Hopf à direita e $\beta : A \otimes_{A^{\underline{H}}} A \to \underline{A \otimes H^*}$, dada por $\beta(a \otimes b) = \sum ab_{(0)} \otimes b_{(1)}$ é uma bijeção.

(1) $\Rightarrow$ (2) Sejam $\sum a_i \otimes b_i \in A \otimes_{A^{\underline{H}}} A$ o idempotente de separabilidade de A sobre $A^{\underline{H}}$ e $\omega = \sum [a_i, b_i] \in A\#_\alpha H$. Então, $\omega \in C_{A\#_\alpha H}(A)$ pois, para qualquer $a \in A$,

$$a \sum a_i \otimes b_i = \sum a a_i \otimes b_i = \sum a_i \otimes b_i a = (\sum a_i \otimes b_i)a$$

e aplicando $[,]$ temos $a \sum [a_i, b_i] = \sum [a_i, b_i]a$. Considere $0 \neq T \in H^*$ tal que $T = \theta^{-1}(1_H)$. Observemos que T é uma integral à direita de H^*, pois para qualquer $h^* \in H^*$ temos

$$\begin{aligned} Th^* &= \theta^{-1}(1_H)h^* = \theta^{-1}(1_H \leftharpoonup h^*) = \theta^{-1}(h^*(1_H)1_H) = \theta^{-1}(\varepsilon_{H^*}(h^*)1_H) \\ &= \theta^{-1}(1_H \varepsilon_{H^*}(h^*)) = \theta^{-1}(1_H)\varepsilon_{H^*}(h^*) = T\varepsilon_{H^*}(h^*). \end{aligned}$$

Com isso,

$$\begin{aligned}
\omega \leftharpoonup T &= \sum [a_i, b_i] \leftharpoonup T = \sum a_i t b_i \leftharpoonup T \\
&= \sum [(a_i \#_\alpha 1_H)(1_A \#_{\alpha 1_H})(b_i \#_\alpha 1_H)] \leftharpoonup T \\
&= \sum (a_i(t_1 \cdot b_i) \#_\alpha t_2) \leftharpoonup T \\
&= \sum a_i(t_1 \cdot b_i) \#_\alpha (t_2 \leftharpoonup T) \\
&= \sum a_i(t_1 \cdot b_i) \#_\alpha T(t_2) t_3 \\
&= \sum a_i(t_1 \cdot b_i) \#_\alpha T(t_2) 1_H \\
&= \sum a_i(T(t_2) t_1 \cdot b_i) \#_\alpha 1_H \\
&= \sum a_i(t \leftharpoonup T) b_i \#_\alpha 1_H \\
&= \sum a_i b_i \#_\alpha 1_H = 1_A \#_\alpha 1_H.
\end{aligned}$$

Da última igualdade decorre imediatamente que $\sum a_i b_i = 1_A$.

(2) $\Rightarrow$ (1) Seja $\sum a_i \otimes b_i = [,]^{-1}(\omega)$. Então, como $\omega \in C_{A\#_\alpha H}(A)$ temos $a\omega = \omega a, \forall a \in A$, logo

$$[,]^{-1}(a\omega) = [,]^{-1}(\omega a) \Rightarrow \sum a a_i \otimes b_i = \sum a_i \otimes b_i a,$$

e de $\omega \leftharpoonup T = 1_A \#_\alpha 1_H$ obtemos $\displaystyle\sum_i a_i b_i \otimes 1_H$ e consequentemente $\displaystyle\sum_i a_i b_i = 1_A$.

Portanto, A é uma extensão separável de $A^{\underline{H}}$.

(5) $\Rightarrow$ (4) Óbvio.

(4) $\Rightarrow$ (1) Mostremos que $\sum x_i c \otimes y_i$ é o idempotente de separabilidade que procuramos. De fato, temos que $\sum x_i c y_i = 1_A$ por hipótese e consequentemente $a \sum x_i c y_i = \sum a x_i c y_i = a 1_A = 1_A a = (\sum x_i c y_i) a = \sum x_i c y_i a$. Decorre agora dessa última igualdade e de [10, Remark 0.13(b)] que $\sum a x_i c \otimes y_i = \sum x_i c \otimes y_i a$, para todo $a \in A$. Portanto A é uma extensão separável de $A^{\underline{H}}$.

(1) $\Rightarrow$ (5) Seja $\sum a_j \otimes b_j$ um idempotente de separabilidade e tome $c = \sum a_j(t \cdot b_j)$. Note que $\sum xa_j \otimes b_j = \sum a_j \otimes b_j x$ para qualquer $x \in A$. Em particular temos, $(id_A \otimes \pi(t))(\sum x_i a_j \otimes b_j) = (id_A \otimes \pi(t))(\sum a_j \otimes b_j x_i)$ o que implica $\sum x_i a_j(t \cdot b_j) = \sum a_j(t \cdot (b_j x_i)$ e assim

$$\begin{aligned}
\sum_i x_i c y_i &= \sum_{i,j} x_i a_j(t \cdot b_j) y_i = \sum_{i,j} a_j(t \cdot b_j x_i) y_i = \sum_j a_j(\sum_i t \cdot (b_j x_i) y_i) \\
&= \sum_j a_j(\sum_i (b_j, x_i) y_i) = \sum_j a_j(\sum_i b_j[x_i, y_i]) \\
&= \sum_j a_j b_j(\sum_i [x_i, y_i]) = 1_A.
\end{aligned}$$

Resta-nos mostrar que $c \in C_A(A^{\underline{H}})$. De fato, seja $a \in A^{\underline{H}}$ então

$$\begin{aligned}
\sum_j a a_j(t \cdot b_j) &= \sum_j a_j(t \cdot b_j a) = \sum_{j,t} a_j(t_1 \cdot b_j)(t_2 \cdot a) \\
&= \sum_{j,t} a_j(t_1 \cdot b_j)(t_2 \cdot 1_A) a = \sum_j a_j(t \cdot b_j) a.
\end{aligned}$$

(1) $\Leftrightarrow$ (3) Pelo Teorema 1.1.2 temos que A é uma extensão separável de $A^{\underline{H}}$ se e somente se A é um A-bimódulo somando direto de $A \otimes_{A^{\underline{H}}} A$. Como A é uma extensão H^*-Galois parcial de $A^{\underline{H}}$ se e somente $[,]$ é sobrejetora e portanto injetora, temos que $A \otimes_{A^{\underline{H}}} A \simeq A \#_\alpha H$ como A-módulos. Portanto, $A \supseteq A^{\underline{H}}$ é separável se e somente se A é um A-bimódulo somando direto de $A \#_\alpha H \simeq A \otimes_{A^{\underline{H}}} A$. $\square$

3.2 Extensões Galois-Azumaya-Hopf Parciais

Nesta seção estudaremos algumas relações entre extensões de Galois-Hopf parciais e o produto smash parcial $A \#_\alpha H$. Com esse intuito vejamos o seguinte lema.

Lema 3.2.1. *Sejam H uma álgebra de Hopf e A um H-módulo álgebra parcial à esquerda. Então, as seguintes afirmações são equivalentes:*

(1) $C(A\#_\alpha H) \subseteq A$

(2) $C(A\#_\alpha H) = C(A) \cap A^{\underline{H}}$

Demonstração. (1) $\Rightarrow$ (2) Tome $x \in C(A\#_\alpha H) \subseteq A$. Logo x comuta com qualquer elemento de A bem como com qualquer elemento de H e assim, $x \in C(A)$. Mostremos que $x \in A^{\underline{H}}$. Tome $h \in H$ qualquer. Notemos que,

$$\begin{aligned}
\sum (h_1 \cdot 1_A)x\#_\alpha h_2 &= \sum x((h_1 \cdot 1_A)\#_\alpha h_2) \\
&= \sum ((h_1 \cdot 1_A)\#_\alpha h_2)x \\
&= \sum ((h_1 \cdot 1_A)\#_\alpha h_2)(x\#_\alpha 1_H) \\
&= \sum (h_1 \cdot 1_A)(h_2 \cdot x)\#_\alpha h_3 \\
&= \sum h_1 \cdot x\#_\alpha h_2.
\end{aligned}$$

Aplicando $I \otimes \varepsilon$ em ambos os lados obtemos

$$\begin{aligned}
(I \otimes \varepsilon_H) \quad & \sum ((h_1 \cdot 1_A)x\#_\alpha h_2) = (I \otimes \varepsilon_H)(\sum h_1 \cdot x\#_\alpha h_2) \\
\Rightarrow \quad & \sum (h_1 \cdot 1_A)x \otimes \varepsilon_H(h_2) = \sum h_1 \cdot x \otimes \varepsilon_H(h_2) \\
\Rightarrow \quad & \sum (\varepsilon_H(h_2)h_1 \cdot 1_A)x \otimes 1_{\mathbf{k}} = \sum \varepsilon_H(h_2)h_1 \cdot x \otimes 1_{\mathbf{k}} \\
\Rightarrow \quad & (h \cdot 1_A)x \otimes 1_{\mathbf{k}} = h \cdot x \otimes 1_{\mathbf{k}} \\
\Rightarrow \quad & (h \cdot 1_A)x = h \cdot x \\
\Rightarrow \quad & x \in A^{\underline{H}}.
\end{aligned}$$

Reciprocamente, sejam $x \in C(A) \cap A^{\underline{H}}$, $a \in A$ e $h \in H$. Então,

$$\begin{aligned}
(a\#_\alpha h)x &= (a\#_\alpha h)(x\#_\alpha 1_H) = \sum a(h_1 \cdot x)\#_\alpha h_2 = \sum a(h_1 \cdot 1_A)x\#_\alpha h_2 \\
&= \sum xa(h_1 \cdot 1_A)\#_\alpha h_2 = x(\sum a(h_1 \cdot 1_A)\#_\alpha h_2) \\
&= x(a\#_\alpha h)(1_A\#_\alpha 1_H) = x(a\#_\alpha h).
\end{aligned}$$

Portanto, $C(A\#_\alpha H) = C(A) \cap A^{\underline{H}}$.

(2) $\Rightarrow$ (1) É imediato que $C(A\#_\alpha H) = C(A) \cap A^{\underline{H}} \subseteq A$. $\square$

Lema 3.2.2. *Se $A\#_\alpha H$ é um $C(A\#_\alpha H)$-módulo projetivo finitamente gerado e $C(A\#_\alpha H) \subseteq A$, então A é um $C(A\#_\alpha H)$-módulo projetivo finitamente gerado.*

Demonstração. Seja $\{m_i, f_i\}$ a base dual de $A\#_\alpha H$ sobre $C(A\#_\alpha H)$, ou seja, para qualquer $x \in A\#_\alpha H$ temos $x = \sum_i f_i(x)m_i$. Seja $m_i = \sum_{j=1}^{n} a_{ij}\#_\alpha h_j$, onde $n = dim_{\mathbf{k}}H$ e $\{h_j\}$ é uma base de H sobre $\mathbf{k}$, com $h_1 = 1_H$. Para qualquer $a \in A$,

$$\begin{aligned}
a = a\#_\alpha 1_H &= \sum_i m_i f_i(a) = \sum_i (\sum_j a_{ij}\#_\alpha h_j) f_i(a) \\
&= \sum_i \sum_j (a_{ij}\#_\alpha 1_H)(1_A\#_\alpha h_j) f_i(a) \\
&= \sum_i \sum_j (a_{ij}\#_\alpha 1_H) f_i(a)(1_A\#_\alpha h_j) \\
&= \sum_i \sum_j (a_{ij} f_i(a)\#_\alpha 1_H)(1_A\#_\alpha h_j) \\
&= \sum_j (\sum_i a_{ij} f_i(a))\#_\alpha h_j.
\end{aligned}$$

Como $h_1 = 1_H$, temos $a = \sum_i a_{i1} f_i(a)$. Então, $\{a_{i1}, f_i\}$ forma uma base dual para A sobre $C(A\#_\alpha H)$. $\square$

Para o que se segue assumiremos que a igualdade 3.1.1 vale e portanto que todas as afirmações do Teorema 3.1.5 são equivalentes.

Teorema 3.2.3. *As seguintes afirmações são equivalentes:*

(1) $A\#_\alpha H$ *é uma álgebra de Azumaya,* A *é um* A*-bimódulo somando direto de* $A\#_\alpha H$ *e* $C(A\#_\alpha H) \subseteq A$*.*

(2) $A\#_\alpha H$ *é uma extensão Hirata-separável de* A *e* A *é separável sobre* $C(A) \cap A^{\underline{H}}$*.*

(3) A *é uma extensão* H^**-Galois parcial e separável sobre* $A^{\underline{H}}$*,* $A^{\underline{H}}$ *é uma álgebra de Azumaya e* $C(A) \cap A^{\underline{H}} = C(A^{\underline{H}})$*.*

Demonstração. (1) $\Rightarrow$ (2) Como $A\#_\alpha H$ é Azumaya sobre $C(A\#_\alpha H) \subseteq A$ e A é um A-bimódulo somando direto de $A\#_\alpha H$, então pelo Teorema 1.1.19, A é uma extensão separável de $C(A\#_\alpha H)$ e $A\#_\alpha H$ é uma extensão Hirata-separável de A. Mas pelo Lema 3.2.1 $C(A\#_\alpha H) = C(A) \cap A^{\underline{H}}$, portanto A é uma extensão separável de $C(A) \cap A^{\underline{H}}$.

(2) $\Rightarrow$ (3) Procederemos em etapas.

Etapa 1: *A é uma extensão H^*-Galois parcial de $A^{\underline{H}}$.*

Como $A\#_\alpha H$ é Hirata-separável sobre A e A é um gerador como A-módulo à esquerda, então pelo Lema 1.1.14, A é um gerador como $A\#_\alpha H$-módulo à esquerda. Sendo assim, pelo Teorema 3.1.5, A é uma extensão H^*-Galois parcial de $A^{\underline{H}}$.

Etapa 2: *A é uma extensão separável de $A^{\underline{H}}$.*

Como A é uma extensão separável de $C(A) \cap A^{\underline{H}}$ e A é um $A^{\underline{H}}$-módulo à direita projetivo finitamente gerado (pelo Teorema 3.1.5) segue pelo Teorema 1.1.17 que A é uma extensão separável de $A^{\underline{H}}$.

Etapa 3: *$A\#_\alpha H$ é Azumaya sobre $C(A) \cap A^{\underline{H}}$ (ou seja* (1) $\Rightarrow$ (2)*).*

Comecemos por observar que extensões Hirata-separáveis são, em particular, separáveis (Teorema 1.1.15). Logo, pela transitividade da separabilidade (Proposição 1.1.21) segue que $A\#_\alpha H$ é separável sobre $C(A) \cap A^{\underline{H}}$. Notemos que pelo Teorema 3.1.5 existem $x_i, y_i \in A \otimes_{A^{\underline{H}}} A$ tais que $\displaystyle\sum_i [x_i, y_i] = 1_A \#_\alpha 1_H$

e sabendo que A é uma extensão separável de $A^{\underline{H}}$ temos que A é um A-bimódulo somando direto de $A\#_\alpha H$ (Teorema 3.1.6). Além disso, $A\#_\alpha H$ é uma extensão Hirata-separável de A. Portanto, pela Proposição 1.1.13, $\Delta := C_{A\#_\alpha H}(A)$. é uma extensão separável de $C(A\#_\alpha H)$ e $C_{A\#_\alpha H}(\Delta) = A$. E mais,

$$C(A\#_\alpha H) \subseteq C_{A\#_\alpha H}(\Delta) = A,$$

donde segue $C(A\#_\alpha H) = C(A) \cap A^{\underline{H}}$, pelo Lema 3.2.1.

Etapa 4: *$E := End_{C(A\#_\alpha H)}(A)$ é uma $C(A\#_\alpha H)$-álgebra de Azumaya.*

Decorre da etapa 3 e do Teorema 1.1.7 que $A\#_\alpha H$ é um $C(A\#_\alpha H)$-módulo projetivo finitamente gerado e pelo Lema 3.2.2 temos que A é projetivo finitamente gerado como $C(A\#_\alpha H)$-módulo. Portanto E é uma $C(A\#_\alpha H)$-álgebra de Azumaya pela Proposição 1.1.8

Etapa 5: *$C_E(A\#_\alpha H)$ é uma $C(A\#_\alpha H)$-álgebra de Azumaya.*
Decorre da etapa 2 e do Teorema 1.1.12.

Etapa 6: $C_E(A\#_\alpha H) = End_{A\#_\alpha H}(A) \simeq (A^{\underline{H}})^{op}$.

A primeira igualdade é imediata e o isomorfismo decorre do Lema 1.4.4 .

Etapa 7: *$A^{\underline{H}}$ é uma $C(A) \cap A^{\underline{H}}$-álgebra de Azumaya.*

Decorre imediatamente das etapas 5 e 6.

Etapa 8: $C(A) \cap A^{\underline{H}} = C(A^{\underline{H}})$.

Decorre imediatamente da hipótese sobre A e das etapas 3 e 6.

(3) $\Rightarrow$ (1) Pelo Teorema 3.1.5 segue que $A\#_\alpha H \simeq End(A_{A^{\underline{H}}})$ e A é $A^{\underline{H}}$-módulo à direita projetivo finitamente gerado. Além disso, decorre do Teorema 1.1.7, $A^{\underline{H}}$ é um $C(A^{\underline{H}})$-gerador projetivo finitamente gerado. Portanto, $End_{C(A^{\underline{H}})}(A)$ é uma álgebra de Azumaya, conforme Proposição 1.1.8. Finalmente, $End(A_{A^{\underline{H}}}) = C_{End_{C(A^{\underline{H}})}(A)}(A^{\underline{H}})$. De fato, basta observar que $End(A_{A^{\underline{H}}})$ é uma subálgebra de $End_{C(A^{\underline{H}})}(A)$ e um $(A^{\underline{H}}, A^{\underline{H}})$-bimódulo via as ações definidas como em 2.1.1(3) $\Rightarrow$ (1). Portanto, pelo Teorema 1.1.12 segue que $A\#_\alpha H$ é uma álgebra de Azumaya e $C(A\#_\alpha H) = C(A^{\underline{H}})$. Decorre do Teorema 3.1.6 que A é A-bimódulo somando direto de $A\#_\alpha H$. $\square$

Definição 3.2.4. Se A é um H-módulo álgebra parcial à esquerda e satisfaz uma das condições do Teorema 3.2.3, então A é dita uma *extensão Galois-Azumaya-Hopf parcial* de $A^{\underline{H}}$, ou simplemente uma extensão H^*-Galois-Azumaya parcial de $A^{\underline{H}}$.

3.3 Correspondências de Galois para Extensões Galois-Azumaya-Hopf Parciais

Nesta seção estabelecemos correspondências de Galois para extensões Galois-Azumaya-Hopf parciais.

Lema 3.3.1. *Seja A uma extensão H^*-Galois Azumaya parcial de $A^{\underline{H}}$. Sejam Y uma $C(A\#_\alpha H)$-subálgebra separável de $A^{\underline{H}}$ e $Y' = C_A(Y)$. Então Y' é uma extensão H^*-Galois Azumaya parcial de $(Y')^{\underline{H}}$ e é separável como uma $C(A\#_\alpha H)$-subálgebra de A.*

Demonstração. Procederemos em etapas.

Etapa 1: *$Y'' = C_{A\#_\alpha H}(Y)$ é uma extensão separável de $C(A\#_\alpha H)$ e $C_{A\#_\alpha H}(Y'') = Y$.*

Comecemos por observar que, pelo Teorema 3.2.3, $A\#_\alpha H$ é uma $C(A\#_\alpha H)$-álgebra Azumaya. Considerando Y como uma $C(A\#_\alpha H)$-subálgebra separável de $A\#_\alpha H$ ($A^{\underline{H}} \simeq A^{\underline{H}}\#_\alpha 1_H \hookrightarrow A\#_\alpha H$) temos que $Y'' = C_{A\#_\alpha H}(Y)$ é uma $C(A\#_\alpha H)$-subálgebra separável de $A\#_\alpha H$ e $C_{A\#_\alpha H}(Y'') = Y$, pela Proposição 1.1.12.

Etapa 2: *Y' é H-invariante e $Y'' = Y'\#_\alpha H$.*

Sejam $x \in C_A(Y) = Y', h \in H$ e $b \in Y \subseteq A^{\underline{H}}$. Então:

$$\begin{aligned}(h\cdot x)b &= (h\cdot(x1_A))b = \sum(h_1\cdot x)(h_2\cdot 1_A)b = \sum(h_1\cdot x)(h_2\cdot b) = h\cdot(xb)\\ &= h\cdot(bx) = \sum(h_1\cdot b)(h_2\cdot x) = \sum b(h_1\cdot 1_A)(h_2\cdot x) = b(h\cdot x).\end{aligned}$$

Além disso, dados $b \in Y$ e $\sum a_i\#_\alpha h_i \in C_{A\#_\alpha H}(Y)$, onde $\{h_i\}$ é uma base de H sobre $\mathbf{k}$ e $a_i \in A$, temos:

$$\begin{aligned}
\sum ba_i \#_\alpha h_i &= b(\sum a_i \#_\alpha h_i) = (\sum a_i \#_\alpha h_i)b \\
&= \sum a_i(h_{i_1} \cdot b)\#_\alpha h_{i_2} = \sum a_i b(h_{i_1} \cdot 1_A)\#_\alpha h_{i_2} \\
&= (\sum a_i b \#_\alpha h_i)(1_A \#_\alpha 1_H) = \sum a_i b \#_\alpha h_i.
\end{aligned}$$

Sendo assim, $ba_i = a_i b$ para qualquer i, isto é, $a_i \in Y'$. Então:

$$\sum a_i \#_\alpha h_i \in Y' \#_\alpha H \Rightarrow Y'' \subseteq Y' \#_\alpha H.$$

Reciprocamente, dados $\sum b_i \#_\alpha h_i \in Y' \#_\alpha H$, temos

$$\begin{aligned}
y(\sum b_i \#_\alpha h_i) &= \sum y b_i \#_\alpha h_i = \sum b_i y \#_\alpha h_i \\
&= (\sum b_i y \#_\alpha h_i)(1_A \#_\alpha 1_H) = \sum b_i y(h_{i1} \cdot 1_A)\#_\alpha h_{i_2} \\
&= \sum b_i (h_{i1} \cdot y)\#_\alpha h_{i_2} = (\sum b_i \#_\alpha h_i)y,
\end{aligned}$$

ou seja, $\sum b_i \#_\alpha h_i \in Y''$.

Etapa 3: $C_{A\#_\alpha H}(A^{\underline{H}}) = C_A(A^{\underline{H}})\#_\alpha H$ *e* $C_{A\#_\alpha H}(C_{A\#_\alpha H}(A^{\underline{H}})) = A^{\underline{H}}$.

Decorre da Etapa 2, tomando $Y = A^{\underline{H}}$, do Teorema 3.2.3 e do Teorema 1.1.12.

Etapa 4: Y' *é um* Y'*-bimódulo somando direto de* Y''.

Como A é um somando direto de $A\#_\alpha H$, segue da Proposição 1.3.11 que existe um elemento $c \in C_{A\#_\alpha H}(A)$ de traço 1. Entretanto,

$$C_{A\#_\alpha H}(A) \subseteq C_{A\#_\alpha H}(A^H) = C_A(A^H) \subseteq C_A(Y)\#_\alpha H = Y''.$$

Assim, $c \in Y''$ e pela Proposição 1.3.11 aplicada a $Y'' \supseteq Y'$ obtemos o afirmado.

Etapa 5: Y'' *é uma álgebra de Azumaya e* $C(Y'') \subseteq Y'$.

Decorre da etapa 3 e do Teorema 1.1.9, aplicado à $A^{\underline{H}}$, que

$$C_{A\#_\alpha H}(C_A(A^{\underline{H}})\#_\alpha H) = C_{A\#_\alpha H}(C_{A\#_\alpha H}(A^{\underline{H}})) = A^{\underline{H}}.$$

Além disso, como $C_A(A^{\underline{H}})\#_\alpha H \subseteq C_A(Y)\#_\alpha H = Y'\#_\alpha H$ temos

$$\begin{aligned} C(C_A(Y)\#_\alpha H) &\subseteq C_{A\#_\alpha H}(C_A(Y)\#_\alpha H) \\ &\subseteq C_{A\#_\alpha H}(C_A(A^{\underline{H}})\#_\alpha H) = A^{\underline{H}}. \end{aligned}$$

Disto decorre que $C(Y'\#_\alpha H) \subseteq C_{A^{\underline{H}}}(Y) \subseteq C_A(Y) = Y'$. Logo, pelo Lema 3.2.1 e pela etapa 1 temos que Y'' é uma álgebra de Azumaya.

Etapa 6: *Y' é uma extensão H^*-Galois-Azumaya parcial de $(Y')^{\underline{H}}$.*

Decorre das etapas 4, 5 e do Teorema 3.2.3.

Etapa 7: *Y' é uma $C(A\#_\alpha H)$-subálgebra separável.*

Novamente pelo Teorema 3.2.3 temos que Y' é uma extensão separável de $C(Y'\#_\alpha H)$. Da etapa 1 temos que $Y'\#_\alpha H$ é uma extensão separável de $C(A\#_\alpha H)$, logo pelo Teorema 1.1.3 $C(Y'\#_\alpha H)$ é uma extensão separável de $C(A\#_\alpha H)$. Finalmente, pela transitividade de extensões separáveis temos que Y' é uma $C(A\#_\alpha H)$-subálgebra separável. □

Lema 3.3.2. *Sejam A uma extensão H^*-Galois-Azumaya parcial de $A^{\underline{H}}$ e W um subanel de A contendo $C_A(A^{\underline{H}})$. Se W é uma extensão H^*-Galois-Azumaya parcial e separável sobre $C(A\#_\alpha H)$, então existe uma $C(A\#_\alpha H)$-subálgebra separável Y de $A^{\underline{H}}$ tal que $W = C_A(Y)$ e $Y = C_{A^{\underline{H}}}(W)$.*

Demonstração. Procederemos por etapas.

Etapa 1: *$W\#_\alpha H$ é uma álgebra de Azumaya e $C(W\#_\alpha H) = C(W) \cap W^{\underline{H}} = C(W^{\underline{H}})$.*

Decorre imediatamente do Teorema 3.2.3.

Etapa 2: *$W\#_\alpha H$ é uma extensão separável de $C(A\#_\alpha H)$.*

Comecemos por observar que pelo Teorema 3.2.3, $W\#_\alpha H$ é uma extensão Hirata-separável de W, que em particular é uma extensão separável (Teorema 1.1.15). A afirmação segue da hipótese sobre W e do Teorema 1.1.21.

Etapa 3: *$C_{A\#_\alpha H}(W\#_\alpha H)$ é uma $C(A\#_\alpha H)$-subálgebra separável de $A\#_\alpha H$ e $C_{A\#_\alpha H}(C_{A\#_\alpha H}(W\#_\alpha H)) = W\#_\alpha H$.*

Decorre das etapas 1, 2 e do Teorema 1.1.12.

Etapa 4: *$C_{A\#_\alpha H}(W\#_\alpha H) \subseteq A^{\underline{H}}$.*

De acordo com a prova do Lema 3.3.1, temos que $C_A(A^{\underline{H}})$ é H-invariante, $C_{A\#_\alpha H}(A^{\underline{H}}) = C_A(A^{\underline{H}})\#_\alpha H$ e $C_{A\#_\alpha H}(C_{A\#_\alpha H}(A^{\underline{H}})) = A^{\underline{H}}$. Também temos por hipótese que $C_A(A^{\underline{H}})$, que implica que $C_{A\#_\alpha H}(A^{\underline{H}}) \subseteq W\#_\alpha H$. Portanto, $C_{A\#_\alpha H}(W\#_\alpha H) \subseteq C_{A\#_\alpha H}(C_{A\#_\alpha H}(A^{\underline{H}}) = A^{\underline{H}}$.

Denotemos por $Y := C_{A\#_\alpha H}(W\#_\alpha H)$.

Etapa 5: *$W = C_A(Y)$.*

Decorre da etapa 4 e da prova do Lema 3.3.1 que $C_{A\#_\alpha H}(Y) = C_A(Y)\#_\alpha H$, logo $W\#_\alpha H = C_{A\#_\alpha H}(C_{A\#_\alpha H}(W\#_\alpha H)) = C_{A\#_\alpha H}(Y) = C_A(Y)\#_\alpha H$. Portanto $W = C_A(Y)$.

Etapa 6: *$Y = C_{A^{\underline{H}}}(W)$.*

Como $Y \subseteq A^{\underline{H}}$ temos $Y = C_{A\#_\alpha H}(W\#_\alpha H) \subseteq C_{A^{\underline{H}}}(W)$. Além disso, $C_{A^{\underline{H}}}(W) \subseteq C_{A^{\underline{H}}}(W\#_\alpha H) \subseteq C_{A\#_\alpha H}(W\#_\alpha H) = Y$, ou seja $Y = C_{A^{\underline{H}}}(W)$. $\square$

Teorema 3.3.3. *Suponha que A é uma extensão H^*-Galois Azumaya parcial de $A^{\underline{H}}$. Então existe uma correspondência um a um entre o conjunto das $C(A\#_\alpha H)$-subálgebras separáveis Y de $A^{\underline{H}}$ e o conjunto das extensões H^*-Galois Azumaya parciais W contendo $C_A(A^{\underline{H}})$ e separáveis sobre $C(A\#_\alpha H)$ dada por $Y \overset{f}{\mapsto} C_A(Y)$ com inversa $W \overset{g}{\mapsto} C_{A^{\underline{H}}}(W)$.*

Demonstração. Seja Y uma $C(A\#_\alpha H)$-subálgebra separável de $A^{\underline{H}}$. Então, $f(Y) = C_A(Y)$ é uma extensão H^*-Galois Azumaya parcial contendo $C_A(A^{\underline{H}})$ e separável sobre $C(A\#_\alpha H)$, pelo Lema 3.3.1. Observe que a sobrejetividade de f é dada pelo Lema 3.3.2. Já para mostrar a injetividade de f, basta mostrar que $C_{A^{\underline{H}}}(C_A(Y)) = Y$ para qualquer Z-subálgebra separável de $A^{\underline{H}}$. Claramente, $Y \subseteq C_{A^{\underline{H}}}(C_A(Y))$. Por outro lado,

$$C_{A^{\underline{H}}}(C_A(Y) \subseteq C_{A\#_\alpha H}(C_A(Y)\#_\alpha H) = C_{A\#_\alpha H}(C_{A\#_\alpha H}(Y)).$$

Como $A\#_\alpha H$ é Azumaya sobre $C(A\#_\alpha H)$ e Y é uma $C(A\#_\alpha H)$-subálgebra separável de $A\#_\alpha H$, decorre do Teorema 1.1.12 que $C_{A\#_\alpha H}(C_{A\#_\alpha H}(Y)) = Y$. E assim, $C_{A^{\underline{H}}}(C_A(Y)) = Y$. □

Teorema 3.3.4. *Suponha que A é uma extensão H^*-Galois Azumaya parcial de $A^{\underline{H}}$. Então existe uma correspondência um a um entre o conjunto das $C(A\#_\alpha H)$-subálgebras separáveis D de A contendo $A^{\underline{H}}$ e o conjunto das $C(A\#_\alpha H)$-subálgebras separáveis E de $C_A(A^{\underline{H}})$ dada por $D \stackrel{f}{\mapsto} C_D(A^{\underline{H}})$ com inversa $E \stackrel{g}{\mapsto} A^{\underline{H}}E$.*

Demonstração. Procederemos por etapas. Seja D uma $C(A\#_\alpha H)$-subálgebra separável contendo $A^{\underline{H}}$.

Etapa 1: *D é uma extensão separável de $C(A)$ e $C(A)$ é uma extensão separável de $C(A\#_\alpha H)$.*

Decorre da hipótese sobre D e do Teorema 1.1.3.

Etapa 2: *$A^{\underline{H}} \otimes_{C(A\#_\alpha H)} C(D)$ é uma $C(D)$-álgebra de Azumaya.*

Segue do Teorema 3.2.3 que $A^{\underline{H}}$ é uma $C(A\#_\alpha H)$-álgebra de Azumaya e assim pelo Lema 1.1.10 temos que $A^{\underline{H}} \otimes_{C(A\#_\alpha H)} C(D)$ é uma $C(D)$-álgebra de Azumaya.

Etapa 3: *$A^{\underline{H}}C(D)$ é uma $C(D)$-álgebra de Azumaya.*

A afirmação segue do isomorfismo de álgebras $\mu : A^{\underline{H}} \otimes_{C(A\#_\alpha H)} C(D) \to A^{\underline{H}}C(D)$.

Etapa 4: *$C_D(A^{\underline{H}}C(D))$ é uma $C(D)$-álgebra de Azumaya.*

Decorre das etapas 1 e 3 e do Teorema 1.1.12.

Etapa 5: *$D = A^{\underline{H}}C_D(A^{\underline{H}})$.*

Notemos que $C_D(A^{\underline{H}}C(D)) = C_D(A^{\underline{H}})$ e novamente pelo Teorema 1.1.12 temos

$$\begin{aligned} D &\simeq A^{\underline{H}}C(D) \otimes_{C(D)} C_D(A^{\underline{H}}C(D)) = A^{\underline{H}}C(D) \otimes_{C(D)} C_D(A^{\underline{H}}) \\ &\simeq A^{\underline{H}}C(D)C_D(A^{\underline{H}}) = A^{\underline{H}}C_D(A^{\underline{H}}). \end{aligned}$$

Etapa 6: *A aplicação* $D \overset{f}{\mapsto} C_D(A^{\underline{H}})$ *está bem definida.*

Das etapas 1 e 4, juntamente com o Teorema 1.1.21 segue que $C_D(A^{\underline{H}})$ é uma extensão separável de $C(A\#_\alpha H)$. Logo, $f(D) = C_D(A^{\underline{H}})$ é uma extensão separável de $C(A\#_\alpha H)$. Observemos ainda que $C_D(A^{\underline{H}}C(D)) = C_D(A^{\underline{H}})$ obviamente, portanto f está bem definida.

Etapa 7: *A aplicação* $E \overset{g}{\mapsto} A^{\underline{H}}E$ *está bem definida.*

Seja E uma $C(A\#_\alpha H)$-subálgebra separável de $C_A(A^{\underline{H}})$ e defina $g(E) = A^{\underline{H}}E$. Como $A^{\underline{H}}$ é $C(A\#_\alpha H)$-separável temos $A^{\underline{H}} \otimes_{C(A\#_\alpha H)} E$ é $C(A\#_\alpha H)$-separável. Desde que $A^{\underline{H}}E = \mu(A^{\underline{H}} \otimes E)$ é imagem homomórfica de $A^{\underline{H}} \otimes_{C(A\#_\alpha H)} E$ segue que $A^{\underline{H}}E$ é $C(A\#_\alpha H)$-separável. Como $A^{\underline{H}} \subseteq A^{\underline{H}}E$ segue que g está bem definida.

Etapa 8: *f e g são inversas uma da outra.*

É imediato da etapas anteriores que $g(f(D)) = g(C_D(A^{\underline{H}})) = A^{\underline{H}}C_D(A^{\underline{H}}) = D$. Além disso,

$$\begin{aligned} f(g(E)) &= f(A^{\underline{H}}E) = f(A^{\underline{H}} \otimes_{C(E)} E) = C_{A^{\underline{H}} \otimes_{C(E)} E}(A^{\underline{H}}) \\ &= C_{A^{\underline{H}} \otimes_{C(E)} E}(A^{\underline{H}} \otimes_{C(E)} C(E)) = C_{A^{\underline{H}}}(A^{\underline{H}}) \otimes_{C(E)} C_E(C(E)) \\ &= C(A^{\underline{H}}) \otimes_{C(E)} E = C(A^{\underline{H}})E = E, \end{aligned}$$

onde a última igualdade decorre do fato que $C(A^{\underline{H}}) = C(A\#_\alpha H) \subseteq E$. $\square$

Bibliografia

[1] R. Alfaro and G. Szeto, *The centralizer on H-separable skew group rings*, Proc. of the conf. Rings, Extensions, and Cohomology, Marcel Dekker, New York, (1994), 1-7.

[2] R. Alfaro and G. Szeto, *Skew group rings which are Azumaya*, Communications in Algebra, 23(6), (1995), 2255-2261.

[3] R. Alfaro and G. Szeto, *On Galois extensions of an Azumaya algebra*, Communications in Algebra, 25(6), (1997), 1873-18882

[4] M. M. S. Alves and E. Batista, *Envelopings actions for partial Hopf actions*, Communications in Algebra (in press).

[5] M. M. S. Alves and E. Batista, *Partial actions, partial invariants and a Morita context*, Journal Algebra and Discret Math, 3 (2009), 1-19.

[6] D. Bagio, J. Lazzarin and A. Paques, *Crossed products by twisted partial actions: separability, semisimplicity and Frobenius properties*, Communications in Algebra, 38, (2010), 496-508.

[7] S. Caenepeel and K. Jansen, *Partial (co)-actions of Hopf algebras and partial Hopf-Galois theory*, Communications in Algebra, 36:8, (2008), 2923-2946.

[8] P. Carvalho, *On the Azumaya locus of some crossed products*, Comm. Algebra 33 (2005), 51-72.

[9] S.U. Chase, D.K. Harrison, A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. AMS 52 (1968), 1-19 .

[10] M. Cohen and D. Fischman , *Semisimple extensions and elements of trace 1*, Journal of Algebra, 149, (1992), 419-437.

[11] M. Cohen, D. Fischman and S. Montgomery, *Hopf Galois extensions, smash products, and Morita equivalence*, Journal of Algebra, 133, (1990), 351-372.

[12] S. Dăscălescu, C. Năstăsescu e S. Raianu, *Hopf Algebras: An Introduction*, Monographs and textbooks in pure and applied mathematics, 235, 2001.

[13] F. R. DeMeyer, *Some notes on the general Galois theory of rings*, Osaka J. Math., 2, (1965), 117-127.

[14] F. DeMeyer e E. Ingraham, *Separable Algebras over Commutative Rings*, Volume 181, Springer Verlag (1971).

[15] F. DeMeyer and G. Janusz, *Group rings that are Azumaya algebras*, Trans. AMS 279 (1983), 238

[16] M. Dokuchaev and E. Exel, *Associativity of crossed products by partial actions, enveloping actions and partial representations*, Trans. AMS 357 (2005), 1931-1952.

[17] M. Dokuchaev, R. Exel and J.J. Simón, *Crossed products by twisted partial actions and graded algebras*, J. Algebra 320 (2008), 3278-3310.

[18] M. Dokuchaev, M. Ferrero and A. Paques *Partial actions and Galois theory*, Journal of Pure and Applied Algebra, 208, (2007), 77-87.

[19] J. A. Guzmán and J. Lazzarin, *A Morita context related to finite groups acting partially on a ring*, Journal Algebra and Discret Math., 3, (2009), 49-60.

[20] M. Harada, *Suplementary results on Galois extensions*, Osaka J. Math., 2, (1965), 287-295.

[21] K. Hirata, *Some types of separable extensions of rings*, Nagoya Math. J., Vol.33, (1968), 107-115.

[22] K. Hirata and K. Sugano, *On semisimple extensions and separable extensions over non commutative rings*, J. Math. Soc. Japan, Vol.18, (1966), 360-373.

[23] S. Ikehata, *Note on Azumaya algebras and H-separable extensions*, Math. J. OKayama Univ.23(1981),17-18.

[24] T. Kanzaki, *On Galois algebra over commutative ring*, Osaka J. of Math., 2, (1965),309-317.

[25] H. F. Kreimer and M. Takeuchi, *Hopf algebras and Galois extensions of an algebra*, Indiana University Math. J., Vol. 30(5), (1981), 675-692.

[26] C. Lomp, *Integrals in Hopf algebras over rings*, Communications in Algebra 32 (2004), no. 12, 4687–4711.

[27] C. Lomp, *Duality for partial group actions*, International Eletronic Journal of Algebra 4, (2008), 53-62.

[28] S. Montgomery, *Hopf Algebras and their Actions on Rings*, CBMS 82, 1992.

[29] H. Okamoto, H. Komatsu and S. Ikehata, *On H-separable extension in Azumaya algebras*, Mathematical Journal of Okayama University, 29, (1987), 103-107.

[30] M. Ouyang, *Azumaya extensions and Galois correpondence*, Algebra Colloquium, 7:1, (2000), 43-57.

[31] A. Paques, V. Rodrigues and A. Sant'Ana, *Galois correspondences for partial Galois Azumaya Extensions*, to appear.

[32] A. Paques, A. Sant'Ana, *When is a crossed product by a twisted partial action Azumaya?*, Communications in Algebra, 38, (2010), 1093-1103.

[33] K. Sugano, *Note on semisimples extensions and separable extensions*, Osaka J.Math., 4 (1967), 265-270.

[34] K. Sugano, *On centralizers in separable extensions*, Osaka J. Math., 7, (1970), 29-40.

[35] G. Szeto and Y. Wong, *On Azumaya projective group rings*, Contemporary Math. 124 (1992), 251-256.

[36] R. Wisbauer, *Foundations of Module and Ring Theory*, Gordon and Breach Sc. Pub., 1991.

Índice