Universidade Federal do Rio Grande do Sul

Instituto de Matemática e Estatística

Programa de Pós-Graduação em Matemática

Álgebras de Hopf fracas sobre anéis comutativos e extensões de Hopf-Ore primitivas fracas

Dissertação de Mestrado

Rafael Haag Petasny

Porto Alegre, 10 de abril de 2024.

Dissertação submetida por Rafael Haag Petasny[1] como requisito parcial para a obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática e Estatística da Universidade Federal do Rio Grande do Sul.

Professor Orientador:
Prof. Dr. Alveri Alves Sant'Ana (PPGMat/UFRGS)

Banca Examinadora:
Profa. Dra. Grasiela Martini (PPGMat/UFRGS)
Profa. Dra. Thaísa Tamusiunas (PPGMat/UFRGS)
Prof. Dr. Leonardo Duarte Silva (UFRGS)
Prof. Dr. Ricardo Leite dos Santos (FURG)

Data da Apresentação: 10/04/2024.

[1]Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES.
Contato: rafaelpetasny@gmail.com.

Agradecimentos

Agradeço àqueles que, de alguma forma, implicam na existência deste trabalho.

Agradeço ao meu colega, Wesley, pois dês do inicio da graduação compartilha comigo seu trabalho e sua visão sobre a matemática, mas que, principalmente, me disse *"ouvi dizer que álgebra de grupóide são álgebra de Hopf fracas, igual álgebras de grupos são álgebras de Hopf"*, o que foi um dos primeiros fatores para que eu escolhesse estudar álgebras de Hopf fracas durante o mestrado.

Agradeço ao meu colega, Adriano, que conheci no inicio do mestrado e igualmente compartilha comigo seu trabalho, apresentando de uma forma muito elegante e descontraída resultados e ideias sobre a teoria de anéis não comutativos. Mesmo que estes resultados não constem explicitamente escritos, as conversas contigo ajudaram a clarear o caminho que levou à escrita de cada seção do último capítulo deste trabalho.

Agradeço à minha colega e namorada, Vanessa, que apesar de não ter tanta familiaridade com a maioria dos assuntos deste texto, sempre esteve disponível para me ouvir e ajudar na revisão das ideias e contas que não chegavam ao resultado esperado. Ter uma companhia confiável, na vida, nos estudos ou no trabalho, muitas vezes pode ser o diferencial para chegarmos ao final de uma jornada satisfeitos pelo que conquistamos.

Agradeço ao meu orientador, Prof. Alveri, pelos 68 meses dedicando parte do seu tempo à minha formação. O senhor me acolheu como aluno de iniciação científica no meu segundo semestre de graduação, quando eu mal sabia o que era matemática, e me orientou através da álgebra abstrata, sendo responsável pela maioria do que conheço e me tornando alguém capaz de *fazer um epsilon a mais.*

Agradeço aos professores da banca examinadora por se disporem a ler este texto. Mais ainda, agradeço ao Prof. Leonardo e à Prof. Grasiela, pelas recomendações de textos para o desenvolvimento do meu conhecimento sobre álgebras de Hopf fracas. Agradeço especialmente ao Prof. Ricardo, autor das referências dos principais resultadso que guiaram a escrita deste texto. Sua participação neste trabalho é intrinseca.

Por fim, agradeço à CAPES pelo financiamento. Sem este auxilio, eu não poderia dedicar o tempo que gostaria, e que foi necessário, para o desenvolvimento do meu conhecimento e, consequentemente, para a realização deste trabalho.

Resumo

Uma extensão de Ore é, essencialmente, uma estrutura de anel no módulo livre $A[X]$, onde os elementos de A não necessariamente comutam com a indeterminada X e para a qual vale a regra do grau, $\deg(pq) \leq \deg(p) + \deg(q)$. Uma álgebra de Hopf fraca sobre um anel comutativo é um módulo, munido de uma estrutura de álgebra, uma estrutura de coálgebra, alguns axiomas de compatibilidade entre estas estruturas e um morfismo especial $S \in End_k(H)$. Assim, uma extensão de Hopf-Ore fraca é uma extensão de Ore de uma álgebra de Hopf fraca, munida de uma estrutura de álgebra de Hopf fraca que estende a estrutura da álgebra de Hopf fraca original. Neste trabalho, vamos apresentar condições necessárias e suficientes para a construção de uma extensão de Hopf-Ore fraca cujo gerador é primitivo fraco, trazendo para o contexto de álgebras sobre anéis comutativos os resultados obtidos por R. dos Santos [16, 2017]. Em especial, vamos apresentar a classificação destas extensões quando H é uma álgebra de grupóide conexo.

Palavras-chave: Extensões de Ore. Álgebras de Hopf fracas. Aneis comutativos. Álgebras de grupóide.

Abstract

An Ore extension is, essentially, a ring structure on the free module $A[X]$, where the elements of A do not necessarily commute with the indeterminate X and for which holds the degree rule, $\deg(pq) \leq \deg(p) + \deg(q)$. A weak Hopf algebra over a commutative ring is a module, equipped with an algebra structure, a coalgebra structure, some compatibility axioms between these structures and a special morphism $S \in End_k(H)$. Thus, a weak Hopf-Ore extension is an Ore extension of a weak Hopf algebra endowed with a weak Hopf algebra structure that extends the structure of the original weak Hopf algebra. In this work, we will present necessary and sufficient conditions for the construction of a weak Hopf-Ore extension whose generator is a weak primitive element, bringing to the context of algebras over commutative rings the results obtained by R. dos Santos [16, 2017]. In particular, we present the classification of these extensions when H is a connected groupoid algebra.

Keywords: Ore extensions. Weak hopf algebras. Commutative rings. Groupoid algebras.

Sumário

Introdução

As extensões de Ore foram introduzidas por Oystein Ore, em [19, 1933], a fim de criar uma teoria que englobasse, principalmente, duas famílias de exemplos: os anéis de polinômios quase comutativos em n indeterminadas sobre o anel de funções infinitamente diferenciáveis, $K[\{x_i\};\{\sigma_i\}]$, estudados por Hilbert, Noether e Schmeidler entre os anos de 1890 e 1920, e os anéis de operadores diferenciais parciais $A_n(K) = K[\{x_i\};\{D_i\}]$, estudados por Dirac, Weyl e Littlewood entre os anos de 1926 e 1933. O anel $A_n(K)$ é conhecido como a n-ésima álgebra de Weyl, devido ao seu uso por Weyl no estudo do princípio de incerteza de Heisenberg na mecânica quântica. Algumas décadas após a publicação do trabalho de Ore, a envolvente universal $U(sl_2(k))$ da álgebra de Lie $sl_2(k)$ e os anéis de coordenadas de um plano quântico, definidos por $\mathcal{O}_q(k^2)$, bem como suas quantizações, foram reconhecidos como extensões de Ore.

Em [3, 1999], Beattie, Dăscălescu e Grünenfelder responderam negativamente a décima conjectura de Kaplansky, apresentando infinitas classes de isomorfismo de álgebras de Hopf de mesma dimensão sobre um corpo algebricamente fechado de característica zero, as quais foram obtidas através de quocientes de iteradas de extensões de Ore sobre álgebras de grupos, considerando as indeterminadas x_i como elementos $(g_i, 1)$-primitivos. Em 2001 (republicado em [18, 2004]) Nenciu estudou as estruturas quasitriangulares das álgebras de Hopf obtidas pela construção apresentada por Beattie *et al*, as quais geram soluções para a equação de Yang-Baxter quântica. O método de construção utilizado em ambos os trabalhos foi generalizado por Panov em [20, 2003], caracterizando quando é possível munir uma extensão de Ore de uma álgebra de Hopf (sobre um anel comutativo) com uma estrutura de álgebra de Hopf, a qual estende a estrutura da álgebra original.

O resultado de Panov foi utilizado pelo mesmo para classificar as extensões de Hopf-Ore das álgebras de grupo kG, das envolventes universais de álgebras de Lie $U(\mathfrak{g})$ e $U_q(\mathfrak{g})$, das álgebras quânticas "$ax + b$" e, em [22, 2020], da álgebra de Sweedler H_4, todas estas sobre corpos algebricamente fechados de característica zero. Em sua dissertação [9, 2019], C. Garcia reobteve os exemplos de Beattie *et al* utilizando o teorema de Panov, concluindo em particular que álgebras de Taft são quocientes de extensões de Ore.

Por outro lado, a definição de álgebra de Hopf fraca que usaremos neste trabalho foi introduzida por Böhm, Nill e Szlachányi em 1996 como uma generalização coassociativa das álgebras de Hopf, contendo como exemplos as *face algebras* e os grupóides quânticos, e tendo como objetivo abordar problemas da teoria de grupos quânticos e das álgebras de operadores. A teoria de álgebras de Hopf fracas foi desenvolvida inicialmente considerando álgebras de dimensão finita sobre corpos e posteriormente alguns resultados iniciais foram reobtidos para álgebras de dimensão infinita. Em [16, 2017], A. Sant'Ana, C. Lomp e R. dos Santos publicaram uma generalização do teorema de Panov para álgebras de Hopf fracas sobre corpos, caracterizando, sob certas hipóteses, quando uma extensão de Ore de uma álgebra de Hopf fraca possui uma estrutura de álgebra de Hopf fraca, a qual estende a estrutura da álgebra original e cujo gerador é um elemento $(g, 1)$-primitivo fraco.

Neste trabalho vamos abordar as álgebras de Hopf fracas sobre anéis comutativos, tendo como enfoque a generalização do teorema de Panov para álgebras de Hopf fracas e a classificação das extensões de Hopf-Ore fracas geradas por elementos primitivos fracos. Este trabalho está organizado da forma que segue.

No primeiro capítulo vamos apresentar os tópicos mais gerais do texto. A primeira seção destina-se a definir o conceito de módulo sobre um anel [17], trazendo resultados sobre módulos livres [14], a construção do produto tensorial de módulos sobre anéis comutativos [1] e uma breve discussão sobre propriedades universais. Na segunda seção trazemos a definição de álgebras e coálgebras sobre anéis comutativos e a construção da álgebra de convolução [21]. A terceira seção contém a construção das extensões de Ore e os resultados necessários para o restante do trabalho [11]. Na quarta seção, reobtemos os resultados elementares da teoria de álgebras de Hopf fracas no contexto de álgebras sobre anéis comutativos, notando que a única mudança significativa ocorre na Proposição 1.4.11.

No segundo capítulo apresentaremos os conceitos direcionados ao resultado principal deste texto, trazendo em paralelo o Teorema de Panov para álgebras de Hopf e sua generalização para o contexto de álgebras de Hopf fracas. Na primeira seção faremos uma breve exposição do teorema obtido por Panov em [20]. Nas seções seguintes, apresentaremos os conceitos de elementos group-like fracos, elementos primitivos fracos, caracteres fracos e coderivações [16]. Na última seção apresentamos a generalização do teorema de Panov para álgebras de Hopf fracas, agora no contexto de álgebras sobre anéis comutativos. Ao longo deste capítulo, caracterizamos tais extensões para o caso em que H é uma álgebra de Hopf fraca obtida pela construção do tipo Kaplansky [5], e classificamos as extensões quando H é uma *face algebra*, derivada de um grafo orientado sem arestas [13].

No terceiro e último capítulo, traremos alguns tópicos da teoria de anéis não comutativos e exemplos relacionados aos resultados discutidos neste texto. Na primeira seção, mostraremos que extensões de Ore de anéis noetherianos são anéis noetherianos [11], obtendo que, neste caso, não existem elementos não inversíveis que admitem inversos unilaterais [15]. Com isso, concluímos que a caracterização das extensões de Hopf-Ore $(g, 1)$-primitivas fracas implica na caracterização das extensões de Hopf-Ore (g, h)-primitivas fracas. Na segunda seção, construiremos uma família de exemplos de álgebras de Hopf fracas que não são álgebras de Hopf apenas no contexto de álgebras sobre anéis comutativos, apresentando métodos para construir estes exemplos através de idempotentes ou famílias de ideais primários e coprimos [1], encerrando com uma aplicação do Teorema de Bézout para determinar quando $\mathbb{Z}_n$ admite uma estrutura de álgebra de Hopf fraca sobre o anel comutativo $\mathbb{Z}_m$. Na última seção deste trabalho, apresentaremos um teorema de estrutura para grupóides conexos [12], a construção das álgebras de Hopf fracas de grupóide e a classificação das extensões de Hopf-Ore geradas por um elemento $(g, 1)$-primitivo fraco, quando H é uma álgebra de grupóide conexo.

Ao longo deste texto, *anel* significa *anel associativo e unitário*, e morfismos de anéis são morfismos de anéis unitários, exceto quando estabelecido o contrário. Para um anel A, denotaremos por $\mathcal{U}(A) = \{x \in A \colon \exists y \in A, xy = 1_A = yx\}$ o conjunto dos elementos inversíveis de A, e por $Z(A) = \{x \in A \colon \forall y \in A, xy = yx\}$ o conjunto dos elementos centrais de A. Para evitar confusão com a notação de derivações, ao invés de utilizarmos o delta de Kronecker, δ_{ij}, utilizaremos do símbolo $[\mathcal{P}]$, o qual representa 1, se a propriedade $\mathcal{P}$ for verdadeira, e 0 caso contrário. Desta forma, $[i = j] = 1$, se $i = j$, e $[i = j] = 0$, se $i \neq j$. Mais ainda, $[i = j, r = s] := [i = j \text{ e } r = s] = [i = j][r = s]$.

Capítulo 1

Pré-requisitos

Neste capítulo vamos apresentar os principais resultados que são necessários para o entendimento dessa dissertação. Será presumido conhecimento básico sobre anéis não comutativos, grupos, morfismos e somas diretas.

1.1 Módulos e produto tensorial

A teoria de módulos é o fundamento teórico deste trabalho. Nesta seção apresentaremos a definição de módulos, morfismos e módulos livres, a construção do produto tensorial de módulos sobre anéis comutativos e uma breve discussão sobre propriedades universais. As referências para esta seção são [1], [14], [15] e [17].

Definição 1.1.1. Seja A um anel. Um **A-módulo à esquerda** é um grupo abeliano M munido de uma função $\triangleright\colon A \times M \to M$ satisfazendo

- $(a +_A b) \triangleright m = a \triangleright m +_M b \triangleright m$,
- $a \triangleright (m +_M n) = a \triangleright m +_M a \triangleright n$,
- $1_A \triangleright m = m$,
- $a \triangleright (b \triangleright m) = (ab) \triangleright m$,

para todo $a, b \in A$ e $m, n \in M$. A função $\triangleright$ é chamada **ação** de A em M.

Antes de apresentar exemplos de A-módulos à esquerda vamos fixar algumas notações.

Poderíamos definir um **A-módulo à direita** de maneira análoga através de uma função $\triangleleft\colon M \times A \to M$. Considerando A^{op} o **anel oposto** de A - o conjunto A munido da soma original e com multiplicação definida por $a \bullet^{op} b = ba$, para quaisquer $a, b \in A$ - temos que um A-módulo à esquerda $(M, \triangleright)$ possui uma estrutura de A^{op}-módulo à direita via $(m, a) \mapsto a \triangleright m$. Da mesma forma, se $(M, \triangleleft)$ é um A-módulo à direita, então M possui uma estrutura de A^{op}-módulo à esquerda. Como $(A^{op})^{op} = A$ e a ação obtida tomando o anel oposto duas vezes coincide com a ação original, podemos nos restringir ao estudo os A-módulos à esquerda, de forma que resultados análogos podem ser obtidos para os A-módulos à direita através dos A^{op}-módulos à esquerda.

Por simplicidade omitiremos os índices A e M nas operações de soma e, quando não houver possibilidade de confusão, denotaremos am em lugar de $a \triangleright m$. Fixado um anel A

vamos denotar por ${}_A\mathfrak{M}$ o *conjunto* dos A-módulos à esquerda.

Como todo módulo é, em particular, um grupo abeliano, podemos considerar o conjunto $End(M)$ dos morfismos de grupo $M \to M$, o qual possui uma estrutura de anel, onde a soma é definida pontualmente, por $(f+g)(m) := f(m) + g(m)$, o produto é dado pela composição, $(fg)(m) := (f \circ g)(m)$, e com unidade $1_{End(M)} = id_M$. Isto nos permite definir **módulo** através de morfismos de anéis.

Lema 1.1.2. *Sejam A um anel e M um grupo abeliano. Então existe uma bijeção entre as ações de A em M e os morfismos de anéis $A \to End(M)$.*

Demonstração. Se $\triangleright \colon A \times M \to M$ é uma ação, então a função $\varphi \colon A \to End(M)$, definida por $\varphi(a)(m) = a \triangleright m$, é um morfismo de anéis. O segundo axioma de ação mostra que $\varphi(a)$ preserva a soma de M - e portanto é um morfismo de grupos abelianos e φ está bem definida - o primeiro axioma de ação mostra que φ é uma função aditiva, o terceiro axioma implica que $\varphi(1_A) = 1_{End(M)}$ e o quarto axioma mostra que φ é uma função multiplicativa.

Reciprocamente, se $\varphi \colon A \to End(M)$ é um morfismo de anéis, então $\triangleright \colon A \times M \to M$, definida por $(a, m) \mapsto \varphi(a)(m)$, é uma ação de A em M. O segundo axioma de ação é garantido por $\varphi(a)$ ser um morfismo de grupos abelianos, o primeiro, terceiro e quarto axiomas vêm respectivamente de φ ser uma função aditiva, unitária e multiplicativa.

Por fim, se $\succ \colon A \times M \to M$ é uma ação, φ é o morfismo de anéis obtido de $\succ$ e $\triangleright$ é a ação obtida de φ, então

$$a \succ m = \varphi(a)(m) = a \triangleright m, \quad \forall a \in A, m \in M \quad \therefore \quad \succ = \triangleright,$$

enquanto que, se $\psi \colon A \to End(M)$ é um morfismo de anéis, $\triangleright$ é a ação obtida de ψ e φ é o morfismo de anéis obtido de $\triangleright$, então

$$\varphi(a)(m) = a \triangleright m = \psi(a)(m), \quad \forall a \in A, m \in M \quad \therefore \quad \varphi = \psi,$$

de onde as associações $\triangleright \mapsto \varphi$ e $\varphi \mapsto \triangleright$ são inversas. $\square$

Definição 1.1.3. Sejam $M, N \in {}_A\mathfrak{M}$. Um morfismo de grupos $f \colon M \to N$ é dito um **morfismo de módulos** à esquerda (ou uma função A-linear à esquerda) se para quaisquer $a \in A$ e $m \in M$ vale $f(a \triangleright_M m) = a \triangleright_N f(m)$.

Dizemos que um morfismo de módulos é um **monomorfismo** se é injetor, um **epimorfismo** se é sobrejetor e um **isomorfismo** se é bijetor. No caso de um isomorfismo $f \colon M \to N$, existe uma função inversa $g \colon N \to M$. Dados $n, n' \in N$ e $a \in A$, calculamos

$$\begin{aligned} g(n) + g(n') &= (g \circ f)(g(n) + g(n')) \\ &= g(f(g(n)) + f(g(n'))) = g(n + n'), \end{aligned}$$

e

$$\begin{aligned} g(a \triangleright_N n) &= g(a \triangleright_N (f \circ g)(n)) \\ &= (g \circ f)(a \triangleright_M g(n)) = a \triangleright_M g(n), \end{aligned}$$

de onde a inversa de um morfismo de módulos bijetor é também um morfismo de módulos. Tendo em vista que morfismos de módulos são, em particular, morfismos de grupos abelianos, vale que $f \colon M \to N$ é um monomorfismo se, e somente se,

$$ker(f) = \{m \in M \colon f(m) = 0_N\} = \{0_M\}.$$

Exemplos triviais, porém essenciais: a função identidade $id_M \colon M \to M$, $m \mapsto m$, e a função nula $0 \colon M \to N$, $m \mapsto 0_N$, são sempre morfismos de módulos.

Exemplo 1.1.4. Listamos abaixo alguns exemplos de A-módulos à esquerda.

(1) $(A, +)$ com a multiplicação pela esquerda. Chamamos esta estrutura de **módulo regular à esquerda** e, para indicá-la, denotamos ${}_AA$;

(2) Seja $I \subseteq A$ um ideal à esquerda. Então $(I, +)$ é um A-módulo à esquerda, onde a ação é dada pela multiplicação à esquerda;

(3) Seja $\varphi\colon A \to B$ um morfismo de anéis. Então $(B, +)$ é um A-módulo à esquerda, onde a ação é dada por $a \triangleright b = \varphi(a)b$. Note que, neste caso o, terceiro axioma de ação vale se, e somente se, $\varphi(1_A) = 1_B$;

(4) Suponha que A é comutativo e sejam $M, N \in \mathfrak{M}_A$. Então o conjunto dos morfismos de A-módulos $M \to N$ com a soma pontual, denotado $Hom_A(M, N)$, é um A-módulo, onde a ação é dada por

$$(a \triangleright f)(m) := f(m) \triangleleft_N a = f(m \triangleleft_M a), \quad \forall a \in A, m \in M, f \in Hom_A(M, N);$$

(5) Seja X um conjunto. Considere A^X o conjunto das sequências $(a_x)_{x\in X}$ de elementos de A indexados por X, onde apenas uma quantidade finita de coordenadas são distintas de zero, com soma definida por $(a_x)_{x\in X} + (b_x)_{x\in X} = (a_x + b_x)_{x\in X}$. Então A^X é um A-módulo à esquerda com a ação $a \triangleright (a_x)_{x\in X} = (aa_x)_{x\in X}$.

Na notação do exemplo (5), denote por $e_x \in A^X$ a sequência tal que $a_x = 1$ e $a_y = 0$, para $y \neq x$. Como todo elemento de A^X possui uma quantidade finita de coordenadas não nulas, podemos escrever $(a_x)_{x\in X} = \sum_{x\in X} a_x \triangleright e_x$, de forma que esta soma é também finita. Mais ainda, dado $m \in A^X$, são únicos os elementos $a_x \in A$ para os quais vale $m = \sum_{x\in X} a_x \triangleright e_x$. De fato, se $b_x \in A$ também satisfazem esta identidade, então

$$0 = \sum_{x\in X} a_x \triangleright e_x - \sum_{x\in X} b_x \triangleright e_x = \sum_{x\in X} (a_x - b_x) \triangleright e_x = (a_x - b_x)_{x\in X}$$

e aplicando projeções obtemos $0 = \pi_x(0) = a_x - b_x$, para todo $x \in X$. Os módulos desta forma serão especialmente úteis neste texto.

Proposição 1.1.5. *Sejam $M \in {}_A\mathfrak{M}$ e I um conjunto. São equivalentes:*

(i) Existe um isomorfismo $M \to A^I$.

(ii) Existe um subconjunto $\{m_i\colon i \in I\} \subseteq M$ tal que, para todo elemento $m \in M$, existem únicos $a_i \in A$, quase todos nulos, tais que $m = \sum a_i m_i$.

(iii) Existe um subconjunto $\{m_i\colon i \in I\} \subseteq M$ tal que, para todo $N \in {}_A\mathfrak{M}$ e todo subconjunto $\{n_i\colon i \in I\} \subseteq N$, existe um único morfismo $f\colon M \to N$ tal que $f(m_i) = n_i$.

Demonstração. Supondo (i), denote por $f\colon M \to A^I$ o isomorfismo dado e, para cada $i \in I$, considere $e_i \in A^I$ como na observação após o Exemplo 1.1.4(5). Então, denotando $m_i = f^{-1}(e_i)$, temos que, dado $m \in M$, existe uma única sequência $(a_i) \in A^I$ tal que $m = f^{-1}((a_i))$. Escrevendo $(a_i) = \sum a_i e_i$ e utilizando que f^{-1} é um morfismo de módulos, obtemos

$$m = f^{-1}((a_i)) = f^{-1}\left(\sum a_i e_i\right) = \sum a_i f^{-1}(e_i) = \sum a_i m_i,$$

portanto vale (ii) com $m_i = f^{-1}(e_i)$.

Suponha (ii). Então, por hipótese, para todo $m \in M$, existem únicos $a_i \in A$ tais que $m = \sum a_i m_i$. Desta forma, temos que $f\colon M \to N$, dada por $f(m) = \sum a_i n_i$, está bem definida como função. Em particular $f(m_i) = n_i$, para cada $i \in I$.

Para ver que f é um morfismo de módulos, note que, se $m = \sum a_i m_i$ e $n = \sum b_i m_i$, então $m + n = \sum (a_i + b_i) m_i$ e, dado $a \in A$, temos $am = a \sum a_i m_i = \sum a a_i m_i$. Como tal escrita é única, obtemos

$$f(m+n) = \sum (a_i + b_i) n_i = \sum a_i n_i + \sum b_i n_i = f(m) + f(n),$$
$$f(am) = \sum a a_i n_i = a \sum a_i n_i = a f(m),$$

portanto f é um morfismo de módulos. Por fim, f é único, pois, se $g\colon M \to N$ é um morfismo de módulos tal que $g(m_i) = n_i$, para todo $i \in I$, então, dado $m \in M$ temos que existem únicos $a_i \in A$ tais que $m = \sum a_i m_i$, portanto

$$g(m) = g\left(\sum a_i m_i\right) = \sum a_i g(m_i) = \sum a_i n_i = f(m),$$

de onde segue que $g = f$. Logo vale (iii).

Suponha (iii). Então, para $e_i \in A^I$ como no primeiro parágrafo da demonstração, temos que deve existir um único morfismo $f\colon M \to A^I$ tal que $f(m_i) = e_i$. Como A^I satisfaz (i) com $id\colon A^I \to A^I$ e mostramos que (i) implica (iii), deve existir um único morfismo $g\colon A^I \to M$ tal que $g(e_i) = m_i$, e este é dado por $g((a_i)) = \sum a_i m_i$. Como a composição $g \circ f\colon M \to M$ satisfaz

$$(g \circ f)(m_i) = g(e_i) = m_i = id_M(m_i)$$

e existe um único morfismo $M \to M$ tal que $m_i \mapsto m_i$, devemos ter $g \circ f = id_M$. Analogamente, a composição $f \circ g\colon A^I \to A^I$ satisfaz $(f \circ g)(e_i) = e_i = id_{A^I}(e_i)$, para todo $i \in I$. Logo, devemos ter $f \circ g = id_{A^I}$. Isso mostra que f é inversível, portanto um isomorfismo. $\square$

Definição 1.1.6. Um módulo M satisfazendo qualquer item da proposição acima será chamado de **módulo livre**, e o conjunto $\{m_i : i \in I\}$ é dito uma **base** para M. Neste caso, denotaremos $M = \bigoplus_{i \in I} A m_i$.

Como uma aplicação da Proposição 1.1.5, considere o módulo $A^{\mathbb{N}}$ com base $\{e_n : n \in \mathbb{N}\}$ e $A[X]$ o anel de polinômios na indeterminada X com a estrutura de A-módulo à esquerda do Exemplo 1.1.4(3). Então existe um único morfismo $f\colon A^{\mathbb{N}} \to A[X]$ tal que $f(e_n) = X^n$. Como um polinômio $p \in A[X]$ é uma combinação linear finita $p = \sum a_n X^n$, basta tomarmos $(a_n) = \sum a_n e_n \in A^{\mathbb{N}}$ para obter $f((a_n)) = p$, enquanto que $(a_n) \in ker(f)$ implica em $\sum a_n X^n = 0$ e, consequentemente, $a_n = 0$, para todo $n \in \mathbb{N}$. Logo $ker(f) = 0$ e esta função é um isomorfismo. Com isso, $A[X]$ é um módulo livre com base $\{X^n : n \in \mathbb{N}\}$.

Adiante vamos utilizar esta estrutura de módulo livre em $A[X]$ para construir uma estrutura de anel não comutativo no lugar da multiplicação usual de polinômios.

Gostaríamos de chamar atenção para o item (iii) da Proposição 1.1.5. Este é usualmente chamado de *propriedade universal dos módulos livres* ou *definição de módulo livre* *via propriedade universal.* A implicação (iii) $\implies$ (i) diz que quaisquer dois A-módulos à esquerda que possuam uma base indexada por I são isomorfos.

Propriedades deste tipo aparecerão diversas vezes ao longo deste texto e suas demonstrações são, em geral, idênticas. Portanto, para evitar repetições, vamos considerar um caso mais abstrato.

Sejam X um conjunto, $\mathcal{P}$ e $\mathcal{Q}$ propriedades e (M,i) um par satisfazendo a propriedade $\mathcal{P}$, onde $M \in {}_A\mathfrak{M}$ e $i\colon X \to M$ é uma função, de forma que, para todo par (N,j) satisfazendo a propriedade $\mathcal{Q}$, com $N \in {}_A\mathfrak{M}$ e $j\colon X \to N$ uma função, exista um único morfismo de módulo $f\colon M \to N$ tal que $f \circ i = j$.

Quando a propriedade $\mathcal{P}$ implica a propriedade $\mathcal{Q}$, dados (M,i) e (N,j) satisfazendo $\mathcal{P}$ obtemos morfismos $f\colon M \to N$ e $g\colon N \to M$ tais que $f \circ i = j$ e $g \circ j = i$, respectivamente. Com isso, a composição $g \circ f\colon M \to M$ satisfaz

$$(g \circ f) \circ i = g \circ (f \circ i) = g \circ j = i$$

e, analogamente, a composição $f \circ g\colon N \to N$ satisfaz $(f \circ g) \circ j = j$. Por outro lado $id_M\colon M \to M$ e $id_N\colon N \to N$ também satisfazem $id_M \circ i = i$ e $id_N \circ j = j$. Pela unicidade dos morfismos satisfazendo estas identidades, concluímos que $f \circ g = id_N$ e $g \circ f = id_M$, ou seja, $f\colon M \to N$ é um isomorfismo de módulos. Em suma, podemos concluir o seguinte:

Corolário (Unicidade via Propriedade Universal)**.** *Sejam X um conjunto e $\mathcal{P}$ e $\mathcal{Q}$ propriedades, onde $\mathcal{P}$ implica $\mathcal{Q}$. Se existe um par (M,i) satisfazendo $\mathcal{P}$ tal que para todo par (N,j) satisfazendo $\mathcal{Q}$ existe um único morfismo $f\colon M \to N$ para o qual $f \circ i = j$, então M é único a menos de isomorfismo.*

Ressaltamos ainda que este argumento não depende da estrutura de módulos, utilizando apenas que a função identidade e a composição de morfismos são morfismos. Desta forma podemos considerar propriedades universais de anéis, grupos e outras estruturas.

Um resultado clássico que pode ser visto como uma propriedade universal, agora no contexto de grupos, é o Teorema do Homomorfismo para Grupos: *Sejam G um grupo e $N \subseteq G$ um subgrupo normal, então o conjunto quociente G/N admite uma única estrutura de grupo tal que a projeção $\pi\colon G \to G/N$ seja um morfismo de grupos. Mais ainda, para todo morfismo de grupos $f\colon G \to H$ tal que $N \subseteq ker(f)$ existe um único morfismo de grupos $g\colon G/N \to H$ tal que $g \circ \pi = f$.*

Neste caso $X = G$, a propriedade $\mathcal{P}$ é *"a função é um morfismo de grupos com núcleo N"*, a propriedade $\mathcal{Q}$ é *"a função é um morfismo de grupos cujo núcleo contém N"* e o par que satisfaz a propriedade universal é $(G/N, \pi)$. Este resultado pode ser adaptado para módulos.

Definição 1.1.7. Sejam $M \in {}_A\mathfrak{M}$. Um subconjunto $N \subseteq M$ é um **submódulo** se N é um subgrupo aditivo de M e a restrição $\triangleright\colon A \times N \to M$ tem imagem em N. Neste caso denotamos $N \leq M$.

Adiante utilizaremos a noção de **submódulo gerado** por um subconjunto. Fixados $M \in {}_A\mathfrak{M}$, $X \subseteq M$ e $N \leq M$ tal que $X \subseteq N$, são equivalentes: se $N' \leq M$ com $X \subseteq N'$ então $N \subseteq N'$; $N = \bigcap\{N' \leq M\colon X \subseteq N'\}$; e $N = \{\sum_{i=1}^{n} a_i x_i\colon a_i \in A, x_i \in X, n \in \mathbb{N}\}$. Neste caso N é dito o submódulo de M gerado por X e denotamos $N = AX$.

Proposição 1.1.8 (Teorema do Homomorfismo)**.** *Sejam $M \in {}_A\mathfrak{M}$ e $N \leq M$. Então o grupo quociente M/N possui uma única estrutura de A-módulo à esquerda de forma* *que a projeção $\pi\colon M \to M/N$ seja um morfismo de módulos. Mais ainda, para todo morfismo de módulos $f\colon M \to L$ tal que $N \subseteq ker(f)$, existe um único morfismo de módulos $g\colon M/N \to L$ tal que $g \circ \pi = f$.*

Demonstração. Como todo módulo é um grupo abeliano, todo subgrupo é normal. Portanto temos do Teorema do Homomorfismo para Grupos que M/N admite uma única estrutura de grupo abeliano tal que $\pi\colon M \to M/N$ seja um morfismo de grupos.

Defina $\bar{\triangleright}\colon A \times M/N \to M/N$ por $(a, \pi(m)) \mapsto \pi(a \triangleright m)$, então $\bar{\triangleright}$ é aditiva em ambas as coordenadas, pois $\triangleright$ é aditiva em ambas as coordenadas e π é aditiva. Além disso, para quaisquer $a, b \in A$ e $\pi(m) \in M/N$, vale

$$a \mathbin{\bar{\triangleright}} (b \mathbin{\bar{\triangleright}} \pi(m)) = a \mathbin{\bar{\triangleright}} \pi(b \triangleright m) = \pi(a \triangleright (b \triangleright m)) = \pi(ab \triangleright m) = ab \mathbin{\bar{\triangleright}} \pi(m),$$

portanto $\bar{\triangleright}$ define uma estrutura de módulo em M/N de forma que $a \mathbin{\bar{\triangleright}} \pi(m) = \pi(a \triangleright m)$, ou seja, tal que π seja um morfismo de módulos. Pela definição de morfismo de módulos esta estrutura é única.

Por fim, como todo morfismo de módulos é em particular um morfismo de grupos, temos do Teorema do Homomorfismo para Grupos que, dado um morfismo de módulos $f\colon M \to L$ tal que $N \subseteq ker(f)$, existe um único morfismo de grupos $g\colon M/N \to L$ tal que $g \circ \pi = f$. Como f e π são morfismos, para todo $a \in A$ e $\pi(m) \in M/N$, calculamos

$$g(a \mathbin{\bar{\triangleright}} \pi(m)) = (g \circ \pi)(a \triangleright m) = f(a \triangleright m) = af(m) = ag(\pi(m)),$$

de onde g é também um morfismo de módulos, o qual é o único que satisfaz $g \circ \pi = f$, pela unicidade do morfismo de grupos satisfazendo esta identidade. □

Para o restante desta seção, k denotará um anel comutativo. Pela discussão no início da seção, temos que todo k-módulo à esquerda possui uma estrutura de $k^{op} = k$-módulo à direita e vice versa, portanto ${}_k\mathfrak{M} = \mathfrak{M}_k$, o que nos permite falar apenas em k-módulos, sem o adjetivo de lateralidade.

Definição 1.1.9. Sejam $M, N, L \in {}_k\mathfrak{M}$. Uma função $f\colon M \times N \to L$ satisfazendo

- $f(m + m', n) = f(m, n) + f(m', n)$,
- $f(m, n + n') = f(m, n) + f(m, n')$,
- $f(am, n) = af(m, n) = f(m, an)$,

para quaisquer $m, m' \in M$, $n, n' \in N$ e $a \in k$, será chamada de **k-bilinear**.

Como exemplo: se $M \in {}_k\mathfrak{M}$, então, por definição, $\triangleright\colon {}_kk \times M \to M$ é uma função k-bilinear. Em particular, a multiplicação $m\colon {}_kk \times {}_kk \to {}_kk$ é k-bilinear.

A próxima proposição define um módulo em função de uma propriedade universal. Este possui uma versão para módulos sobre um anel não necessariamente comutativo, utilizando hipóteses mais restritas. Porém, no contexto deste trabalho, apresentaremos e utilizaremos apenas o resultado sobre anéis comutativos.

Proposição 1.1.10 (Propriedade Universal do Produto Tensorial)**.** *Sejam k um anel comutativo e $M, N \in {}_k\mathfrak{M}$. Então existe um par (T, φ), onde $T \in {}_k\mathfrak{M}$ e $\varphi\colon M \times N \to T$ é uma função k-bilinear, tal que, para todo par (L, f) com $L \in {}_k\mathfrak{M}$ e $f\colon M \times N \to L$ uma função k-bilinear, existe um único morfismo de módulos $g\colon T \to L$ tal que $g \circ \varphi = f$.*

Demonstração. Considere P o módulo livre de base $M \times N$ e Q o submódulo de P gerado pelos elementos da forma

$$\begin{gathered}(m+m', n) - (m, n) - (m', n),\\ (m, n+n') - (m, n) - (m, n'),\\ a(m, n) - (am, n),\\ a(m, n) - (m, an),\end{gathered}$$

onde $m, m' \in M$, $n, n' \in N$ e $a \in k$. Pela Proposição 1.1.8, o quociente $T = P/Q$ possui uma única estrutura de módulo tal que $\pi\colon P \to T$ seja um morfismo de módulos. Vamos denotar um elemento $\pi((m, n)) \in T$ por $m \otimes n$. Considere $\varphi\colon M \times N \to T$ dada por $\varphi(m, n) = m \otimes n$, então φ é k-bilinear, pois dados $m \in M$, $n \in N$ e $a \in k$, temos

$$\varphi(am, n) = (am) \otimes n = a(m \otimes n) = a\varphi(m, n),$$

onde a segunda igualdade segue de $a(m, n) - (am, n) \in Q$. Portanto, as classes de equivalência $a(m \otimes n)$ e $(am) \otimes n$ são iguais em $T = P/Q$. Analogamente, mostra-se que $\varphi(m, an) = a\varphi(m, n)$ e que φ é aditiva em ambas a coordenadas. Seja $f\colon M \times N \to L$ uma função k-bilinear, utilizando a Proposição 1.1.5 obtemos um único morfismo $h\colon P \to L$ tal que $h((m, n)) = f(m, n)$, para todo $(m, n) \in M \times N$. Temos que $Q \subseteq ker(h)$. De fato, considere um gerador de Q da forma $x = a(m, n) - (am, n)$, então

$$h(x) = h(a(m, n) - (am, n)) = ah((m, n)) - h((am, n)) = af(m, n) - f(am, n) = 0,$$

onde a segunda igualdade segue de h ser um morfismo de módulos e a última de f ser k-bilinear. De maneira análoga, mostra-se que, se $x \in P$ é um gerador de Q, de qualquer forma, então $h(x) = 0$. Como h é um morfismo de módulos e anula os geradores de Q, segue que $h(Q) = 0$, ou seja, $Q \subseteq ker(h)$. Pela Proposição 1.1.8, existe um único morfismo $g\colon T \to L$ tal que $g \circ \pi = h$. Identificando o conjunto $M \times N \subseteq P$ via inclusão, temos que $\varphi = \pi|_{M \times N}$ e $f = h|_{M \times N}$, portanto vale

$$g \circ \varphi = (g \circ \pi)|_{M \times N} = h|_{M \times N} = f.$$

O morfismo g é único pois os morfismos obtidos das Proposições 1.1.5 e 1.1.8 são únicos. $\square$

Como o par (T, φ) da proposição acima satisfaz uma propriedade universal, obtemos pelo Corolário da Unicidade via Propriedade Universal que o módulo T é único a menos de isomorfismo. Assim, vamos denotar $T = M \otimes_k N$, ou simplesmente $M \otimes N$, e chamá-lo de **produto tensorial** de M por N. Algumas propriedades do produto tensorial serão úteis.

Proposição 1.1.11. *Sejam $M, N, L \in {}_k\mathfrak{M}$, então valem os seguintes isomorfismos:*

(i) $M \otimes (N \otimes L) \simeq (M \otimes N) \otimes L$;

(ii) $M \otimes N \simeq N \otimes M$;

(iii) $M \otimes k \simeq M \simeq k \otimes M$.

Demonstração. (*Ideia*) A demonstração completa não será apresentada por ser repetitiva.

Tomando como exemplo o item (ii), defina $f\colon M \times N \to N \otimes M$ por $(m,n) \mapsto n \otimes m$ e $g\colon N \times M \to M \otimes N$ por $(n,m) \mapsto m \otimes n$. Aplique a Propriedade Universal do Produto Tensorial para obter morfismos $f'\colon M \otimes N \to N \otimes M$ e $g'\colon N \otimes M \to M \otimes N$. Conclua que g' e f' são inversos e portanto definem um isomorfismo.

O item (iii) utiliza a estrutura de k-módulo regular e o isomorfismo é dado pelos morfismos $(a,m) \mapsto a \triangleright m$ e $m \mapsto 1_k \otimes m$. □

O item (i) da proposição acima indica que podemos considerar, de certa forma, o produto tensorial $M_1 \otimes \cdots \otimes M_n$ de n k-módulos, utilizando a propriedade universal recursivamente de forma que $T_1 = M_1$ e $T_j = T_{j-1} \otimes M_j$, para cada $j = 2, \dots, n$.

Sejam $M, N, P, Q \in {}_k\mathfrak{M}$ e $f\colon M \to P$, $g\colon N \to Q$ morfismos de k-módulos. Então da k-linearidade de f e g, bem como da k-bilinearidade da função $(p,q) \mapsto p \otimes q$, temos que a função $(f \times g)\colon M \times N \to P \otimes Q$, definida por $(f \times g)((m,n)) = f(m) \otimes g(n)$, é k-bilinear. Aplicando a propriedade universal do produto tensorial, obtemos um único morfismo $f \otimes g\colon M \otimes N \to P \otimes Q$ tal que $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$. Recursivamente, podemos construir o produto $f_1 \otimes \cdots \otimes f_n\colon M_1 \otimes \cdots \otimes M_n \to N_1 \otimes \cdots \otimes N_n$ de n morfismos $f_j\colon M_j \to N_j$.

Na próxima seção vamos apresentar um resultado relacionando o produto tensorial com módulos livres, o qual será crucial para o desenvolvimento dos principais resultados deste texto.

1.2 Álgebras e coálgebras

Nesta seção vamos apresentar as definições de álgebras e coálgebras sobre anéis comutativos e a álgebra de convolução, além de finalizar os pré-requisitos sobre módulos livres. Os resultados desta seção são baseados em [1], [6] e [21].

Definição 1.2.1. Seja R um anel. Uma **extensão** de R é um par (A,u), onde A é um anel e $u\colon R \to A$ é um morfismo de anéis unitários. Se R for comutativo e $im(u) \subseteq Z(A)$, dizemos que (A,u) é uma **R-álgebra**.

Quando A é um anel comutativo, temos $im(u) \subseteq A = Z(A)$, portanto toda extensão comutativa de R é uma R-álgebra. Por conta disso, em [1], o par (A,u) definido acima é sempre chamado de R-álgebra. Porém trabalharemos, a partir da próxima seção, com extensões que não são necessariamente álgebras.

Exemplo 1.2.2. Abaixo listamos alguns exemplos de k-álgebras.

(1) $k^n = \bigoplus_{i=1}^n ke_i$ com multiplicação coordenada-a-coordenada e $u(a) = \sum_{i=1}^n ae_i$.

(2) $k[X]$ com o produto usual de polinômios e $u(a) = a = aX^0$.

(3) $M_n(k)$ com o produto usual de matrizes e $u(a) = \sum_{i=1}^n ae_{ii}$.

(4) Sejam G um grupo com identidade e e kG o k-módulo livre de base G. Então kG é uma k-álgebra com multiplicação dada por $a_g g \cdot a_h h = (a_g a_h)gh$, onde $g, h \in G$ e $a_g, a_h \in k$, e $u(a) = ae$, para todo $a \in k$.

Seja (A, u) uma extensão de um anel comutativo k. Então A se torna um k-módulo via $\triangleright\colon k \times A \to A$, dada por $(a, r) \mapsto u(a)r$, de onde existe o produto tensorial $A \otimes A$. Quando A for uma k-álgebra, podemos utilizar a Propriedade Universal do Produto Tensorial para descrever a estrutura de álgebra através de morfismos e identidades.

Proposição 1.2.3. *Existe uma correspondência entre o conjunto Alg_k das k-álgebras, e as triplas (A, μ, u), onde $A \in {}_k\mathfrak{M}$, $\mu\colon A \otimes A \to A$ e $u\colon k \to A$ são morfismos de módulos satisfazendo*

$$\mu \circ (\mu \otimes id_A) = \mu \circ (id_A \otimes \mu), \quad \mu \circ (u \otimes id_A) = \triangleright \quad e \quad \mu \circ (id_A \otimes u) = \triangleleft,$$

onde $\triangleleft$ denota a ação oposta de $k^{op} = k$ em A.

Demonstração. Se (A, u) for uma k-álgebra, então, da associatividade da multiplicação em A, obtemos

$$\begin{array}{c} a \triangleright (rs) = u(a)(rs) = (u(a)r)s = (ru(a))s = r(u(a)s) = r(a \triangleright s) \\ \| \\ (a \triangleright r)s \end{array}$$

ou seja, a multiplicação $A \times A \to A$, $(r, s) \mapsto rs$, é k-bilinear. Segue da Propriedade Universal do Produto Tensorial que existe um único morfismo $\mu\colon A \otimes A \to A$ tal que $\mu(r \otimes s) = rs$. Ainda, da associatividade da multiplicação em A, devem ser iguais

$$\begin{aligned} (\mu \circ (id_A \otimes \mu))(r_1 \otimes r_2 \otimes r_3) &= \mu(r_1 \otimes r_2 r_3) = r_1(r_2 r_3) = (r_1 r_2) r_3 \\ &= \mu(r_1 r_2 \otimes r_3) = (\mu \circ (\mu \otimes id_A))(r_1 \otimes r_2 \otimes r_3), \end{aligned}$$

portanto μ satisfaz a identidade $\mu \circ (\mu \otimes id_A) = \mu \circ (id_A \otimes \mu)$.

Observe ainda que, com a estrutura de módulo regular ${}_k k$, temos $u(ab) = u(a)u(b) = a \triangleright u(b)$, logo u é um morfismo de módulos e, utilizando o isomorfismo $k \otimes A \simeq A$, $a \otimes r \mapsto a \triangleright r = u(a)r$, obtemos

$$(\mu \circ (u \otimes id_A))(a \otimes r) = \mu(u(a) \otimes r) = u(a)r = a \triangleright r,$$

e

$$(\mu \circ (id_A \otimes u))(r \otimes a) = \mu(r \otimes u(a)) = ru(a) = r \triangleleft a,$$

portanto valem as identidades $\mu \circ (u \otimes id_A) = \triangleright$ e $\mu \circ (id_A \otimes u) = \triangleleft$.

Reciprocamente, suponha que (A, μ, u) seja uma tripla, onde $A \in {}_k\mathfrak{M}$, $\mu\colon A \otimes A \to A$ e $u\colon k \to A$ são morfismos satisfazendo as três identidades enunciadas. Então valem

$$\begin{aligned} u(ab) &= a \triangleright u(b) = (\mu \circ (u \otimes id_A)(a \otimes u(b)) = u(a)u(b), \\ \mu(u(1_k) \otimes r) &= (\mu \circ (u \otimes id_A))(1_k \otimes r) = 1_k \triangleright r = r, \\ \mu(r \otimes u(1_k)) &= (\mu \circ (id_A \otimes u))(r \otimes 1_k) = r \triangleleft 1_k = r, \end{aligned}$$

de onde, definindo $m\colon A \times A \to A$ por $m(r, s) = \mu(r \otimes s) =: rs$, obtemos que $(A, +, m)$ é um anel associativo com $1_A = u(1_k)$, cuja estrutura de k-módulo é dada por $a \triangleright r = u(a)r$, e tal que $u\colon k \to A$ é um morfismo de anéis unitários. Por fim, pela bilinearidade da aplicação $(r, s) \mapsto r \otimes s$, obtemos

$$u(a)r \otimes u(1_k) = a \triangleright (r \otimes u(1_k)) = r \otimes u(a)u(1_k) = r \otimes u(a).$$

Aplicando μ à igualdade acima, resulta $u(a)r = ru(a)$, portanto $im(u) \subseteq Z(A)$. $\square$

Esta caracterização permite a construção de novas álgebras.

Lema 1.2.4. *Sejam $A, B \in Alg_k$. Então $A \otimes B \in Alg_k$.*

Demonstração. Como k é comutativo existe, o produto tensorial $A \otimes B$. Denotando por $\tau\colon A\otimes B \to B\otimes A$ o isomorfismo $r\otimes s \mapsto s\otimes r$, então $\mu\colon (A\otimes B)\otimes(A\otimes B) \mapsto A\otimes B$, definida por $\mu = (\mu_A \otimes \mu_B) \circ (id_A \otimes \tau \otimes id_B)$, e $u\colon k \to A \otimes B$, definida por $u(a) = a \triangleright (1_A \otimes 1_B)$, são morfismos de módulos, e satisfazem

$$\begin{aligned}
&(\mu \circ (\mu \otimes id_{A\otimes B}))((r_1 \otimes s_1) \otimes (r_2 \otimes s_2) \otimes (r_3 \otimes s_3)) \\
&= (r_1r_2)r_3 \otimes (s_1s_2)s_3 = r_1(r_2r_3) \otimes s_1(s_2s_3) \\
&= (\mu \circ (id_{A\otimes B} \otimes \mu))((r_1 \otimes s_1) \otimes (r_2 \otimes s_2) \otimes (r_3 \otimes s_3)),
\end{aligned}$$

$$\begin{aligned}
(\mu \circ (u \otimes id_{A\otimes B}))(a \otimes (r \otimes s)) &= \mu([a \triangleright (1_A \otimes 1_B)] \otimes (r \otimes s)) \\
&= a \triangleright \mu((1_A \otimes 1_B) \otimes (r \otimes s)) \\
&= a \triangleright (1_Ar \otimes 1_Bs) = a \triangleright (r \otimes s),
\end{aligned}$$

e

$$\begin{aligned}
(\mu \circ (id_{A\otimes B} \otimes u))((r \otimes s) \otimes a) &= \mu((r \otimes s) \otimes [a \triangleright (1_A \otimes 1_B)]) \\
&= a \triangleright \mu((r \otimes s) \otimes (1_A \otimes 1_B)) \\
&= a \triangleright (r1_A \otimes s1_B) = a \triangleright (r \otimes s) = (r \otimes s) \triangleleft a,
\end{aligned}$$

de onde segue que $(A \otimes B, \mu, u)$ é uma k-álgebra. □

Lema 1.2.5. *Sejam $A \in Alg_k$ e $ke \in {}_k\mathfrak{M}$ um módulo livre de base $\{e\}$. Então $A' = ke\oplus A$ possui uma estrutura de álgebra sobre k, com unidade $1_{A'} = e$ e cuja multiplicação estende a multiplicação de A.*

Demonstração. Todo elemento $x \in A'$ pode ser escrito, de maneira única, como $x = re+a$, onde $r \in k$ e $a \in A$. Considere as funções $\mu\colon A' \times A' \to A'$ e $u\colon k \to A'$, definidas respectivamente por

$$\mu(re + a, se + b) = rse + (rb + sa + ab) \quad \text{e} \quad u(r) = re, \quad \forall r, s \in k, a, b \in A.$$

Vamos mostrar que (A', μ, u) é uma álgebra sobre k. Primeiro, observamos que u e μ são morfismos de módulos. De fato, valem $u(rs) = (rs)e = r(se) = ru(s)$,

$$\begin{aligned}
\mu(r'(re + a), se + b) &= \mu(r're + r'a, se + b) \\
&= r'rse + (r'rb + sr'a + r'ab) \\
&= r'[rse + (rb + sa + ab)] \qquad (s, r, r' \in k = k^{op}) \\
&= r'\mu(re + a, se + b),
\end{aligned}$$

e

$$\begin{aligned}
\mu(re + a, r'(se + b)) &= \mu(re + a, r'se + r'b) \\
&= rr'se + (rr'b + r'sa + ar'b) \\
&= r'[rse + (rb + sa + ab)] \qquad (s, r, r' \in k = k^{op}, u_{A'}(r') \in Z(A')) \\
&= r'\mu(re + a, se + b).
\end{aligned}$$

Logo μ é k-bilinear. Pela Propriedade Universal do Produto Tensorial, μ define um morfismo de módulos $\mu\colon A' \otimes A' \to A'$, o qual é associativo, pois, dados $r, s, p \in k$ e $a, b, c \in A$, temos

$$\begin{aligned}
&\mu(\mu([re + a] \otimes [se + b]) \otimes [pe + c]) \\
&= \mu([rse + (rb + sa + ab)] \otimes [pe + c]) \\
&= rspe + (rsc + p(rb + sa + ab) + (rb + sa + ab)c) \\
&= rspe + (rsc + prb + psa + pab + rbc + sac + abc),
\end{aligned}$$

e, por outro lado,

$$\begin{aligned}
&\mu([re + a] \otimes \mu([se + b] \otimes [pe + c])) \\
&= \mu([re + a] \otimes [spe + (sc + pb + bc)]) \\
&= rspe + (r(sc + pb + bc) + spa + a(sc + pb + bc)) \\
&= rspe + (rsc + rpb + rbc + spa + asc + apb + abc) \\
&= rspe + (rsc + prb + rbc + psa + sac + pab + abc),
\end{aligned}$$

onde, na última igualdade, utilizamos que $r, s, p \in k = k^{op}$ e $u_A(p), u_A(s) \in Z(A)$.

Por fim,

$$\begin{aligned}
\mu(u(s) \otimes (re + a)) = \mu(se \otimes (re + a)) = sre + sa = s(re + a), \\
\mu((re + a) \otimes u(s)) = \mu((re + a) \otimes se) = rse + sa = (re + a)s.
\end{aligned}$$

Logo (A, μ, u) é uma álgebra sobre k, com unidade $1_{A'} = u(1_k) = e$, e tal que

$$\mu(a \otimes b) = \mu([0e + a] \otimes [0e + b]) = 0e + 0b + 0a + ab = ab, \quad \forall a, b \in A.$$

Ou seja, a multiplicação μ em A' estende a multiplicação de A. $\square$

Para o próximo resultado, observe que, se $A \in Alg_k$ e $M \in {}_A\mathfrak{M}$, então M possui uma estrutura de k-módulo dada por $a \bullet m = u(a) \triangleright m$. Desta forma dados $A, B \in Alg_k$, $M \in {}_A\mathfrak{M}$ e $N \in {}_B\mathfrak{M}$, temos $A \otimes B \in Alg_k$ e $M \otimes N \in {}_k\mathfrak{M}$, da seguinte forma.

Para cada $(r, s) \in A \times B$, considere uma função $\varphi(r, s)\colon M \times N \to M \otimes N$, dada por

$$\varphi(r, s)(m, n) = (r \triangleright m) \otimes (s \triangleright n), \quad \forall m \in N, n \in N.$$

Então cada $\varphi(r, s)$ é k-bilinear e, portanto, definem morfismos $\varphi(r, s) \in End_k(M \otimes N)$. Considere agora $\Phi\colon A \times B \to End_k(M \otimes N)$, dada por $\Phi(r, s) = \varphi(r, s)$. Então

$$\begin{aligned}
\Phi(u_A(a)r, s)(m \otimes n) &= ((u_A(a)r) \triangleright m) \otimes (s \triangleright n) \\
&= (u_A(a) \triangleright (r \triangleright m)) \otimes (s \triangleright n) \\
&= [a \bullet (r \triangleright m)] \otimes (s \triangleright n) \\
&= a \bullet [(r \triangleright m) \otimes (s \triangleright n)] = a \bullet \Phi(r, s)(m \otimes n) \\
&= (r \triangleright m) \otimes [a \bullet (s \triangleright n)] = \Phi(r, u_B(a)s)(m \otimes n),
\end{aligned}$$

e Φ é aditiva em cada coordenada, portanto k-bilinear. Da Propriedade Universal do Produto Tensorial obtemos um morfismo $\Phi\colon A \otimes B \to End_k(M \otimes N)$ tal que

$$\Phi(r \otimes s)(m \otimes n) = (r \triangleright m) \otimes (s \triangleright n).$$

Ainda, $\Phi(1_A \otimes 1_B)(m \otimes n) = (1_A \triangleright m) \otimes (1_B \triangleright n) = m \otimes n = id_{M\otimes N}(m \otimes n)$, e

$$\begin{aligned}
\Phi((r \otimes s)(r' \otimes s'))(m \otimes n) &= \Phi(rr' \otimes ss')(m \otimes n) \\
&= (rr' \triangleright m) \otimes (ss' \triangleright n) \\
&= (r \triangleright (r' \triangleright m)) \otimes (s \triangleright (s' \triangleright n)) \\
&= \Phi(r \otimes s)((r' \triangleright m) \otimes (s' \triangleright n)) \\
&= (\Phi(r \otimes s) \circ \Phi(r' \otimes s'))(m \otimes n),
\end{aligned}$$

portanto Φ é um morfismo de anéis unitários. Segue do Lema 1.1.2 que $M \otimes N$ é um $(A \otimes B)$-módulo, com ação $(r \otimes s) \triangleright (m \otimes n) = \Phi(r \otimes s)(m \otimes n) = (r \triangleright m) \otimes (s \triangleright n)$.

Agora podemos apresentar o último pré-requisito sobre módulos livres.

Proposição 1.2.6. *Sejam $A, B \in Alg_k$, $M \in {}_A\mathfrak{M}$ e $N \in {}_B\mathfrak{M}$. Se M é livre sobre A com base $\{m_i \colon i \in I\}$ e N é livre sobre B com base $\{n_j \colon j \in J\}$, então $M \otimes N$ é livre sobre $A \otimes B$ com base $\{m_i \otimes n_j \colon i \in I, j \in J\}$.*

Demonstração. Vamos utilizar o item (ii) da Proposição 1.1.5, notando que, para a unicidade de escrita, é suficiente mostrar a unicidade da escrita do elemento nulo.

Seja $\sum m_l \otimes n_l \in M \otimes N$ um elemento genérico. Então podemos escrever

$$\sum_l m_l \otimes n_l = \sum_l \left(\left(\sum_i r_{i,l} m_i \right) \otimes \left(\sum_j s_{j,l} n_j \right) \right) = \sum_{i,j} \left(\sum_l (r_{i,l} \otimes s_{j,l}) \right) (m_i \otimes n_j).$$

Portanto, todo elemento de $M \otimes N$ pode ser escrito como uma combinação $(A \otimes B)$-linear do conjunto $\{m_i \otimes n_j \colon i \in I, j \in J\}$.

Fixados $i_0 \in I$ e $j_0 \in J$, como M e N são livres, existem morfismos $p_{i_0} \colon M \to A$ e $q_{j_0} \colon N \to B$ tais que $p_{i_0}(m_i) = [i = i_0]$ e $q_{j_0}(n_j) = [j = j_0]$. Em particular, p_{i_0} e q_{j_0} são k-lineares, de onde existe um morfismo k-linear $p_{i_0} \otimes q_{j_0} \colon M \otimes N \to A \otimes B$ tal que

$$\begin{aligned}
(p_{i_0} \otimes q_{j_0})((r \otimes s)(m_i \otimes n_j)) &= (p_{i_0} \otimes q_{j_0})(rm_i \otimes sn_j) \\
&= p_{i_0}(rm_i) \otimes q_{i_0}(sm_j) \\
&= rp_{i_0}(m_i) \otimes sq_{i_0}(m_j) = [i = i_0][j = j_0](r \otimes s).
\end{aligned}$$

Com isso $\sum (r \otimes s)_{i,j}(m_i \otimes n_j) = 0$, onde $(r \otimes s)_{i,j} \in A \otimes B$, implica em

$$\begin{aligned}
0 &= (p_{i_0} \otimes q_{j_0}) \left(\sum_{i,j} (r \otimes s)_{i,j}(m_i \otimes n_j) \right) \\
&= \sum_{i,j} (p_{i_0} \otimes q_{j_0})((r \otimes s)_{i,j}(m_i \otimes n_j)) = (r \otimes s)_{i_0,j_0}.
\end{aligned}$$

Portanto, é única a maneira de escrever o elemento nulo como combinação $(A \otimes B)$-linear do conjunto $\{m_i \otimes n_j \colon i \in I, j \in J\}$. Assim, segue que $M \otimes N$ é um $(A \otimes B)$-módulo livre com base $\{m_i \otimes n_j \colon i \in I, j \in J\}$. $\square$

Utilizaremos este resultado no próximo capítulo da seguinte forma: seja $A \in Alg_k$, então $A[X] \in {}_A\mathfrak{M}$ tem base $\{X^n \colon n \in \mathbb{N}\}$. Portanto $A[X] \otimes A[X]$ é um $(A \otimes A)$-módulo à esquerda livre com base $\{X^i \otimes X^j \colon i, j \in \mathbb{N}\}$. Em particular, escrevendo

$$r \otimes sX + pX \otimes q = (r \otimes s)(1 \otimes X) + (p \otimes q)(X \otimes 1),$$

segue do lema anterior que $r \otimes sX + pX \otimes q = r' \otimes s'X + p'X \otimes q'$ em $A[X] \otimes A[X]$ se, e somente se, $r \otimes s = r' \otimes s'$ e $p \otimes q = p' \otimes q'$ em $A \otimes A$. Assim, se os elementos $r \otimes s$ e $p \otimes q$ são conhecidos e $r' \otimes s'$ e $p' \otimes q'$ precisam ser determinados, o resultado acima garante que é suficiente "igualar os coeficientes" de $X^i \otimes X^j$ em ambas as escritas.

Uma última observação sobre o produto de álgebras de maneira geral. Se $A, B \in Alg_k$, podemos definir funções $i_A\colon A \to A \otimes B$ por $i_A(r) = r \otimes 1_B$ e $i_B\colon B \to A \otimes B$ por $i_B(s) = 1_A \otimes s$. Pela bilinearidade de $(r, s) \mapsto r \otimes s$, temos que i_A e i_B são morfismos de k-módulos e, pela definição do produto em $A \otimes B$, temos

$$i_A(rr') = rr' \otimes 1_B = (r \otimes 1_B)(r' \otimes 1_B) = i_A(r)i_A(r')$$

de onde i_A, e analogamente i_B, são morfismos de anéis unitários e, para todo $r \otimes s \in A \otimes B$, vale $r \otimes s = (r \otimes 1_B)(1_A \otimes s) = i_A(r)i_B(s)$. Como consequência, se em A vale uma identidade $r = r'$, então em $A \otimes B$ vale a identidade

$$r \otimes s = i_A(r)i_B(s) = i_A(r')i_B(s) = r' \otimes s.$$

Com isso podemos aplicar identidades das álgebras A em *"partes dos tensores"* de $A \otimes B$, o que será particularmente útil para os cálculos no contexto de álgebras de Hopf fracas.

Como consequência da Proposição 1.2.3, podemos definir uma k-álgebra através de *diagramas comutativos* - esquemas de morfismos tais que qualquer caminho ligando os mesmos pontos iniciais e finais devem ter composições iguais - ou seja, utilizando os isomorfismos canônicos $\triangleright\colon k \otimes A \to A$ e $\triangleleft\colon A \otimes k \to A$, é equivalente (A, u) ser uma k-álgebra e a tripla (A, μ, u) satisfazer os seguintes diagramas:

$$\mu \circ (\mu \otimes id_A) = \mu \circ (id_A \otimes \mu), \qquad \mu \circ (u \otimes id_A) = \triangleright \quad \text{e} \quad \mu \circ (id_A \otimes u) = \triangleleft.$$

$$\begin{tikzcd}
A \otimes A \otimes A \arrow[r, "\mu \otimes id_A"] \arrow[d, "id_A \otimes \mu"'] & A \otimes A \arrow[d, "\mu"] \\
A \otimes A \arrow[r, "\mu"'] & A
\end{tikzcd}
\qquad
\begin{tikzcd}
& A \otimes A \arrow[dd, "\mu"] & \\
k \otimes A \arrow[ur, "u \otimes id_A"] \arrow[dr, "\simeq"'] & & A \otimes k \arrow[ul, "id_A \otimes u"'] \arrow[dl, "\simeq"] \\
& A &
\end{tikzcd}$$

Através desta descrição, podemos *dualizar* os diagramas - inverter o sentido dos morfismos preservando os esquemas e isomorfismos - para obter uma nova estrutura, descrita em função de módulos e morfismos.

Definição 1.2.7. Seja k um anel comutativo. Uma **k-coálgebra** é uma tripla (C, Δ, ϵ), onde $C \in {}_k\mathfrak{M}$, $\Delta\colon C \to C \otimes C$ e $\epsilon\colon C \to k$ são morfismos satisfazendo os diagramas:

$$\begin{tikzcd}
C \otimes C \otimes C & C \otimes C \arrow[l, "\Delta \otimes id_C"'] \\
C \otimes C \arrow[u, "id_C \otimes \Delta"] & C \arrow[l, "\Delta"] \arrow[u, "\Delta"']
\end{tikzcd}
\qquad
\begin{tikzcd}
& C \otimes C \arrow[dl, "\epsilon \otimes id_C"'] \arrow[dr, "id_C \otimes \epsilon"] & \\
k \otimes C & & C \otimes k \\
& C \arrow[ul, "\simeq"] \arrow[ur, "\simeq"'] \arrow[uu, "\Delta"] &
\end{tikzcd}$$

O morfismo Δ é chamado **comultiplicação** e ϵ é chamado **counidade**. Os diagramas são chamados, respectivamente, de **axioma da coassociatividade** e **axioma da counidade**, em contraste com a associatividade e unidade das k-álgebras.

Apesar do axioma da counidade significar $(\epsilon \otimes id_C) \circ \Delta = \triangleright^{-1}$, é comum utilizarmos a identidade equivalente, $\triangleright \circ (\epsilon \otimes id_C) \circ \Delta = id_C$, e omitir o isomorfismo $\triangleright$. Desta forma, para cada $c \in C$, denotando $\Delta(c) = \sum_{(c)} c_1 \otimes c_2 \in C \otimes C$, temos

$$c = \sum_{(c)} \epsilon(c_1)c_2 = \sum_{(c)} c_1\epsilon(c_2),$$

enquanto o axioma da coassociatividade implica que as expressões

$$((\Delta \otimes id_C) \circ \Delta)(c) = (\Delta \otimes id_C)\left(\sum_{(c)} c_1 \otimes c_2\right) = \sum_{(c),(c_1)} c_{1_1} \otimes c_{1_2} \otimes c_2,$$

e

$$((id_C \otimes \Delta) \circ \Delta)(c) = (id_C \otimes \Delta)\left(\sum_{(c)} c_1 \otimes c_2\right) = \sum_{(c),(c_2)} c_1 \otimes c_{2_1} \otimes c_{2_2},$$

denotam o mesmo elemento. Portanto, podemos escrever

$$\Delta_2(c) = ((\Delta \otimes id_C) \circ \Delta)(c) = \sum_{(c)} c_1 \otimes c_2 \otimes c_3,$$

e, quando não houver a possibilidade de confusão, apenas $\Delta_2(c) = c_1 \otimes c_2 \otimes c_3$. Mais geralmente, definindo $\Delta_i = (\Delta \otimes id_C) \circ \Delta_{i-1}$, vamos denotar $\Delta_i(c) = c_1 \otimes \cdots \otimes c_{i+1}$. Uma demonstração completa de que podemos simplificar a notação de Δ_i desta forma pode ser encontrada em [6, 1.1.11 Computation rule].

Exemplo 1.2.8. Abaixo listamos alguns exemplos de k-coálgebras.

(1) (k, Δ, id_k), onde $\Delta\colon k \to k \otimes k$ é dada por $\Delta(a) = a \otimes 1$, para todo $a \in k$.

(2) Sejam X um conjunto e k^X o k-módulo livre com base X. Então (k^X, Δ, ϵ) é uma coálgebra sobre k, onde

$$\Delta(x) = x \otimes x \quad \text{e} \quad \epsilon(x) = 1, \quad \forall x \in X.$$

(3) Pelo exemplo anterior, $k[X]$ é uma k-coálgebra com $\Delta(X^n) = X^n \otimes X^n$ e $\epsilon(X^n) = 1$.

(4) O módulo $k[X]$ possui uma segunda estrutura de k-coálgebra, onde $\Delta(1) = 1 \otimes 1$, $\epsilon(1) = 1$ e, para todo $n > 0$, $\epsilon(X^n) = 0$ e

$$\Delta(X^n) = \sum_{i=0}^{n} \binom{n}{i} X^i \otimes X^{n-i}.$$

(5) Seja $(X, \prec)$ um conjunto preordenado tal que, para quaisquer $x, y \in X$, o conjunto $\{z \in X \colon x \prec z \prec y\}$ seja finito. Considere $X^2_\prec$ o k-módulo livre de base $\{(x, y) \in X^2 \colon x \prec y\}$, então $X^2_\prec$ é uma coálgebra, com

$$\Delta((x, y)) = \sum_{x \prec z \prec y} (x, z) \otimes (z, y) \quad \text{e} \quad \epsilon((x, y)) = [x = y].$$

(6) Se k é um corpo e (A, μ, u) é uma k-álgebra de dimensão finita, então $A^* = Hom_k(A, k)$, com $\Delta = \mu^*$ e $\epsilon = u^*$, é uma k-coálgebra, onde $\mu^*(f) = f \circ \mu$ e $u^*(f) = f \circ u$ são as *adjuntas*, ou *transpostas*, usuais.

(7) Como consequência do exemplo (6), seja $\{e_{ij} \colon i, j = 1, \ldots, n\}$ a base canônica de $M_n(k)$, denotando a base dual de $C = (M_n(k))^*$ por $\{E_{ij} \colon i, j = 1, \ldots, n\}$, onde $E_{ij}(e_{rs}) = [i = r][j = s]$, temos que C é uma k-coálgebra com morfismos

$$\Delta(E_{ij}) = \sum_{l} E_{il} \otimes E_{lj} \quad \text{e} \quad \epsilon(E_{ij}) = [i = j].$$

Este exemplo pode ser obtido via (5) com $X = \{1, \ldots, n\}$ e $1 \leq 2 \leq \cdots \leq n \leq 1$.

Em contraste com os Lemas 1.2.4 e 1.2.5, podemos construir coálgebras a partir de coálgebras conhecidas. Vamos denotar por $CoAlg_k$ o *conjunto* das k-coálgebras.

Lema 1.2.9. *Sejam $C, D \in CoAlg_k$. Então $C \otimes D \in CoAlg_k$.*

Demonstração. Considere $\Delta \colon C \otimes D \to (C \otimes D) \otimes (C \otimes D)$, definida por

$$\Delta = (id_C \otimes \tau \otimes id_D) \circ (\Delta_C \otimes \Delta_D),$$

onde $\tau \colon C \otimes D \to D \otimes C$ é o isomorfismo canônico, e $\epsilon \colon C \otimes D \to k \otimes k \simeq k$, definida por $\epsilon(c \otimes d) = \epsilon_C(c)\epsilon_D(d)$. Então, para $c \in C$ e $d \in D$, temos

$$\begin{aligned}
((\Delta \otimes id_{C\otimes D}) \circ \Delta)(c \otimes d) &= (\Delta \otimes id_{C\otimes D})(c_1 \otimes d_1 \otimes c_2 \otimes d_2) \\
&= (c_1 \otimes d_1 \otimes c_2 \otimes d_2) \otimes (c_3 \otimes d_3) \\
&= (c_1 \otimes d_1) \otimes (c_2 \otimes d_2 \otimes c_3 \otimes d_3) \\
&= (id_{C\otimes D} \otimes \Delta)(c_1 \otimes d_1 \otimes c_2 \otimes d_2) \\
&= ((id_{C\otimes D} \otimes \Delta) \circ \Delta)(c \otimes d),
\end{aligned}$$

de onde vale o axioma da coassociatividade.

$$\begin{aligned}
((\epsilon \otimes id_{C\otimes D}) \circ \Delta)(c \otimes d) &= (\epsilon \otimes id_{C\otimes D})(c_1 \otimes d_1 \otimes c_2 \otimes d_2) \\
&= (\epsilon_C(c_1)\epsilon_D(d_1)) \triangleright (c_2 \otimes d_2) \\
&= \epsilon_C(c_1)c_2 \otimes \epsilon_D(d_1)d_2 \\
&= c \otimes d,
\end{aligned}$$

e também

$$\begin{aligned}((id_{C\otimes D}\otimes\epsilon)\circ\Delta)(c\otimes d) &= (id_{C\otimes D}\otimes\epsilon)(c_1\otimes d_1\otimes c_2\otimes d_2)\\ &= (c_1\otimes d_1)\triangleright(\epsilon_C(c_2)\epsilon_D(d_2))\\ &= c_1\epsilon_C(c_2)\otimes d_1\epsilon_D(d_2)\\ &= c\otimes d.\end{aligned}$$

Portanto vale o axioma da counidade. Logo $(C\otimes D,\Delta,\epsilon)$ é uma k-coálgebra. □

Lema 1.2.10. *Sejam $C\in CoAlg_k$ e $ke\in {}_k\mathfrak{M}$ um módulo livre de base $\{e\}$. Suponha que existe $g\in C$ tal que $\Delta_C(g)=g\otimes g$ e $\epsilon_C(g)=1_k$. Então $C'=ke\oplus C$ possui uma estrutura de coálgebra, onde $\epsilon(e)=2$ e cuja comultiplicação estende a comultiplicação de C.*

Demonstração. Todo elemento $x\in C'$ pode ser escrito, de maneira única, como $x=re+c$, onde $r\in k$ e $c\in C$. Considere as funções $\Delta\colon C'\to C'\otimes C'$ e $\epsilon\colon C'\to k$, definidas respectivamente por

$$\Delta(re+c)=r(g\otimes g+f\otimes f)+\Delta_C(c)\quad\text{e}\quad\epsilon(re+c)=2r+\epsilon_C(c),$$

onde $f=e-g$. Vamos mostrar que (C',Δ,ϵ) é uma coálgebra sobre k. Primeiro, Δ e ϵ são morfismos de módulos, pois, para todo $s\in k$,

$$\epsilon(s(re+c))=\epsilon(sre+sc)=2sr+\epsilon_C(sc)=s(2r)+s\epsilon_C(c)=s\epsilon(re+c),$$

e também

$$\begin{aligned}\Delta(s(re+c)) &= \Delta(sre+sc)\\ &= sr(g\otimes g+f\otimes f)+\Delta_C(sc)\\ &= sr(g\otimes g+f\otimes f)+s\Delta_C(c)\\ &= s\Delta(re+c),\end{aligned}$$

onde, nas terceiras igualdades, utilizamos que ϵ_C e Δ_C são morfismos de módulos. Em particular, tomando $r=0$, obtemos que $\Delta|_C=\Delta_C$. Ainda,

$$\Delta(f)=\Delta(e-g)=\Delta(e)-\Delta_C(g)=(g\otimes g+f\otimes f)-g\otimes g=f\otimes f,$$

de onde calculamos

$$\begin{aligned}(\Delta\otimes id_{C'})\Delta(re+c) &= r(\Delta(g)\otimes g+\Delta(f)\otimes f)+(\Delta\otimes id_{C'})\Delta_C(c)\\ &= r(g\otimes g\otimes g+f\otimes f\otimes f)+(\Delta_C\otimes id_C)\Delta_C(c)\\ &= r(g\otimes\Delta(g)+f\otimes\Delta(f))+(id_C\otimes\Delta_C)\Delta_C(c)\\ &= (id_{C'}\otimes\Delta)\Delta(re+c).\end{aligned}$$

Ou seja, Δ é coassociativo. Por fim, de $f=e-g$ e $\epsilon(g)=1_k$, segue que $\epsilon(f)=1_k$, enquanto que $g_1\otimes g_2=\Delta(g)=g\otimes g$ implica $\epsilon_C(g)g=g=g\epsilon_C(g)$. Logo

$$\begin{aligned}\mu(u\epsilon\otimes id_{C'})\Delta(re+c)=r(\epsilon_C(g)g+\epsilon(f)f)+\epsilon_C(c_1)c_2=r(g+f)+c=re+c,\\ \mu(id_{C'}\otimes\epsilon)\Delta(re+c)=r(g\epsilon_C(g)+f\epsilon(f)+c_1\epsilon_C(c_2)=r(g+f)+c=re+c.\end{aligned}$$

Portanto vale o axioma da counidade. Logo (C',Δ,ϵ) é uma coálgebra sobre k. □

Vamos terminar esta seção construindo uma nova álgebra, a partir de uma álgebra e uma coálgebra, a qual é fundamental para a definição de álgebras de Hopf fracas.

Sejam (A, μ, u) uma k-álgebra e (C, Δ, ϵ) uma k-coálgebra. Então $Hom_k(C, A)$, o conjunto dos morfismos de k-módulos de C para A, possui uma estrutura de k-módulo, dada por $(a \triangleright f)(c) = f(a \triangleright c) = a \triangleright f(c)$, para quaisquer $a \in k$, $f \in Hom_k(C, A)$ e $c \in C$. Dados $f, g \in Hom_k(C, A)$, denote por $f * g$ a composição

$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{f \otimes g} A \otimes A \xrightarrow{\mu} A$$

então $f * g \in Hom_k(C, A)$, por ser composição de morfismos, e $(f * g)(c) = f(c_1)g(c_2)$, para cada $c \in C$. Como f e g são morfismos e $im(u) \subseteq Z(A)$, dado $a \in k$, temos

$$\begin{aligned}
((a \triangleright f) * g)(c) &= f(a \triangleright c_1)g(c_2) \\
&= u(a)f(c_1)g(c_2) = (a \triangleright (f * g))(c) \\
&= f(c_1)u(a)g(c_2) \\
&= f(c_1)g(a \triangleright c_2) = (f * (a \triangleright g))(c).
\end{aligned}$$

Portanto, a aplicação $Hom_k(C, A) \times Hom_k(C, A) \to Hom_k(C, A)$, dada por $(f, g) \mapsto f * g$, é k-bilinear. Pela Propriedade Universal do Produto Tensorial existe um único morfismo $*\colon Hom_k(C, A) \otimes Hom_k(C, A) \to Hom_k(C, A)$ tal que $*(f \otimes g) = f * g$. Ainda, definindo $\eta\colon k \to Hom_k(C, A)$ por $\eta(a) = a \triangleright (u \circ \epsilon)$, temos

$$\begin{aligned}
(* \circ (\eta \otimes id))(a \otimes f)(c) &= ((a \triangleright (u \circ \epsilon)) * f)(c) \\
&= a \triangleright u(\epsilon(c_1))f(c_2) \\
&= a \triangleright (\epsilon(c_1) \triangleright f(c_2)) \\
&= a \triangleright f(\epsilon(c_1)c_2) = a \triangleright f(c) = (a \triangleright f)(c),
\end{aligned}$$

e analogamente $* \circ (id \otimes \eta) = \triangleright$. Logo $Hom_k(C, A)$ é uma k-álgebra com $\eta(1_k) = u \circ \epsilon$.

Definição 1.2.11. Sejam $A \in Alg_k$ e $C \in CoAlg_k$. A **álgebra de convolução** de C e A é a k-álgebra $(Hom_k(C, A), *, \eta)$ construída acima.

Em particular, se um k-módulo H possui tanto uma estrutura de álgebra quanto de coálgebra - como $k[X]$, k^G, com G um grupo, e $M_n(k)$, com a estrutura usual de k-álgebra a estrutura de k-coálgebra do 1.2.8(2), tomando $X = \{e_{ij} : i, j = 1, \ldots, n\}$ - temos que $End_k(H) = Hom_k(H, H)$ possui a estrutura de álgebra de convolução, além da estrutura proveniente da composição.

A álgebra de convolução será muito útil no desenvolvimento de equações envolvendo álgebras de Hopf fracas, uma vez que diversas identidades podem ser facilmente traduzidas nesta álgebra. Como exemplo, do axioma da counidade, vale $\epsilon(c_1) \triangleright c_2 = c = c_1 \triangleleft \epsilon(c_2)$ para todo $c \in H$. Sendo H uma álgebra temos $u(\epsilon(c_1))c_2 = c = c_1 u(\epsilon(c_2))$, ou equivalentemente,

$$(u \circ \epsilon) * id_H = id_H = id_H * (u \circ \epsilon),$$

o que condiz com $\eta(1_k) = u \circ \epsilon$ ser a unidade de $End_k(H)$.

A noção de morfismos entre álgebras e coálgebras será necessária adiante.

Definição 1.2.12. Sejam $A, B \in Alg_k$ e $f\colon A \to B$ um morfismo de k-módulos. Então f é dito um **morfismo de álgebras** se satisfaz

$$f \circ \mu_A = \mu_B \circ (f \otimes f) \quad \text{e} \quad f \circ u_A = u_B,$$

e um **anti-morfismo de álgebras** se $f\colon A \to B^{op} = (B, \mu_B \circ \tau, u_B)$ for um morfismo de álgebras. De maneira dual, para $C, D \in CoAlg_k$ e $f\colon C \to D$ um morfismo de k-módulos, dizemos que f é um **morfismo de coálgebras** se satisfaz

$$(f \otimes f) \circ \Delta_C = \Delta_D \circ f \quad \text{e} \quad \epsilon_C = \epsilon_D \circ f,$$

e um **anti-morfismo de coálgebras** se $f\colon C \to D^{cop} = (D, \tau \circ \Delta_D, \epsilon_D)$ for um morfismo de coálgebras. Em ambos os casos, τ denota o isomorfismo canônico do produto tensorial.

A propriedade de um morfismo $f\colon A \to B$ ser de álgebras, ou $f\colon C \to D$ de coálgebras, pode ser representado através de diagramas comutativos, como:

morf. de álgebras

$$\begin{tikzcd} A \otimes A \arrow[r, "f \otimes f"] \arrow[d, "\mu_A"'] & B \otimes B \arrow[d, "\mu_B"] \\ A \arrow[r, "f"'] & B \end{tikzcd} \qquad \begin{tikzcd} A \arrow[rr, "f"] & & B \\ & k \arrow[ul, "u_A"] \arrow[ur, "u_B"'] & \end{tikzcd}$$

morf. de coálgebras

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[d, "\Delta_C"'] & D \arrow[d, "\Delta_D"] \\ C \otimes C \arrow[r, "f \otimes f"'] & D \otimes D \end{tikzcd} \qquad \begin{tikzcd} C \arrow[rr, "f"] \arrow[dr, "\epsilon_C"'] & & D \arrow[dl, "\epsilon_D"] \\ & k & \end{tikzcd}$$

Assim, a noção de morfismo de coálgebras é dual à noção de morfismo de álgebras.

1.3 Extensões de Ore

Nesta seção vamos motivar, definir e mostrar a existência das extensões de Ore, bem como algumas propriedades que serão úteis no decorrer deste texto. Os resultados desta seção foram originalmente publicados em [19] e, mais recentemente, em [11].

Seja A um anel. Então $A[X]$ é um A-módulo à esquerda livre com base $\{X^n : n \in \mathbb{N}\}$. Portanto, para todo $0 \neq p \in A[X]$, existe $d \in \mathbb{N}$ tal que $p = a_0 + a_1X + \cdots + a_dX^d$, com $a_d \neq 0$. Neste caso, denotaremos por $\deg(p) = d$ o **grau** de p. Quando $p = 0$ é o polinômio nulo, definimos $\deg(0) = -\infty$. Estamos interessados em munir $A[X]$ com um estrutura de anel, de forma que $i\colon A \to A[X]$, $r \mapsto rX^0$, seja um morfismo de anéis - portanto determina uma estrutura de extensão de A em $A[X]$ - e tal que vale a **regra do grau**: $\deg(pq) \leq \deg(p) + \deg(q)$, para quaisquer $p, q \in A[X]$.

Como $A[X] = \bigoplus_{n \in \mathbb{N}} AX^n$, para todo $r \in A$, existem $r_0, \ldots, r_n \in A$ tais que

$$Xr = r_0 + r_1X + \cdots + r_nX^n,$$

e, como $\deg(X) = 1$ e $\deg(r) = 0$, para valer a equação do grau, devemos ter $\deg(Xr) \leq 1$. Ou seja, $Xr = r_1X + r_0$, onde possivelmente $r_1 = 0$. Como tal escrita é única, vamos denotar $r_1 = \sigma(r)$ e $r_0 = \delta(r)$. Para que $1_{A[X]} = i(1_A) = 1_AX^0$, devem valer as igualdades

$$1_AX = X = X1_A = \sigma(1_A)X + \delta(1_A),$$

ou seja, $\sigma(1_A) = 1_A$ e $\delta(1_A) = 0$. Para que a multiplicação em $A[X]$ seja associativa, devemos ter

$$\begin{aligned}
\sigma(rs)X + \delta(rs) &= X(rs) = (Xr)s \\
&= (\sigma(r)X + \delta(r))s \\
&= \sigma(r)(Xs) + \delta(r)s \\
&= \sigma(r)(\sigma(s)X + \delta(s)) + \delta(r)s \\
&= \sigma(r)\sigma(s)X + \sigma(r)\delta(s) + \delta(r)s.
\end{aligned}$$

Portanto, devem ser iguais, $\sigma(rs) = \sigma(r)\sigma(s)$ e $\delta(rs) = \delta(r)s + \sigma(r)\delta(s)$. Para a compatibilidade com a soma, deve valer

$$\begin{aligned}
\sigma(r+s)X + \delta(r+s) &= X(r+s) = Xr + Xs \\
&= \sigma(r)X + \delta(r) + \sigma(s)X + \delta(s) \\
&= (\sigma(r) + \sigma(s))X + \delta(r) + \delta(s),
\end{aligned}$$

ou seja, σ e δ devem ser funções aditivas. Em particular, $\sigma\colon A \to A$ é um morfismo de anéis.

Definição 1.3.1. Sejam A um anel e $\sigma\colon A \to A$ um endomorfismo. Uma função aditiva $\delta\colon A \to A$ é chamada de **σ-derivação** se satisfaz $\delta(rs) = \delta(r)s + \sigma(r)\delta(s)$, $\forall r, s \in A$.

Apesar de termos deduzido que deve valer $\delta(1_A) = 0$, para que $i(1_A) = 1_{A[X]}$, não é necessário incluir esta condição na definição de σ-derivação, pois

$$\delta(1) = \delta(1^2) = \delta(1)1 + \sigma(1)\delta(1) = 2\delta(1),$$

de onde, subtraindo $\delta(1)$ da igualdade acima, obtemos novamente $\delta(1) = 0$. A discussão acima mostra propriedades necessárias para que um A-módulo à esquerda livre, com base enumerável e satisfazendo a regra do grau, seja uma extensão de A. O próximo resultado mostra que estas condições são suficientes.

Ao longo do próximo resultado, utilizaremos que todo grupo abeliano $(G, +)$ tem uma estrutura de $\mathbb{Z}$-módulo, dada por $ng = \sum_{i=1}^{n} g$, se $n > 0$, $ng = \sum_{i=1}^{n} -g$, se $n < 0$, e $0g = 0$, para todo $g \in G$. Em particular, se A é um anel, então $(A, +)$ e $(A[X], +)$ são $\mathbb{Z}$-módulos, e um morfismo de $\mathbb{Z}$-módulos é simplesmente uma função aditiva.

Proposição 1.3.2. *Sejam A um anel, σ um endomorfismo de A e δ uma σ-derivação. Então existe um anel R tal que:*

(i) Existe um monomorfismo de anéis $i\colon A \to R$;

(ii) Existe $y \in R$ tal que $\{y^n\colon n \in \mathbb{N}\}$ é base de R como A-módulo à esquerda;

(iii) Para todo $r \in A$, vale $yi(r) = i(\sigma(r))y + i(\delta(r))$.

Demonstração. Seja $E = End(A[X])$ o anel dos morfismos de grupos $A[X] \to A[X]$. Para cada $r \in A$, associe $i(r) \colon A[X] \to A[X]$, tal que $i(r)(p) = rp$. Então, pela bilinearidade da ação de A em $A[X]$, temos que $i(r) \in E$, e $i \colon A \to E$ é uma função aditiva. Mais ainda, $i(r) \equiv 0$ implica $0 = i(r)(1_A X^0) = rX^0 = r$, portanto i é injetor e, para quaisquer $r, s \in A$, vale $i(rs)(f) = (rs)f = r(sf) = (i(r) \circ i(s))(f)$. Logo i é um monomorfismo de anéis.

Defina $y \colon A[X] \to A[X]$ por $y(\sum a_n X^n) = \sum \sigma(a_n) X^{n+1} + \delta(a_n) X^n$. Então

$$\begin{aligned}
y\left(\sum_{n=0}^{N} a_n X^n + \sum_{n=0}^{M} b_n X^n\right) &= y\left(\sum_{n=0}^{\max\{N,M\}} (a_n + b_n) X^n\right)\\
&= \sum_{n=0}^{\max\{N,M\}} \sigma(a_n + b_n) X^{n+1} + \delta(a_n + b_n) X^n\\
&= \sum_{n=0}^{\max\{N,M\}} (\sigma(a_n) + \sigma(b_n)) X^{n+1} + (\delta(a_n) + \delta(b_n)) X^n\\
&= \sum_{n=0}^{N} \sigma(a_n) X^{n+1} + \delta(a_n) X^n + \sum_{n=0}^{M} \sigma(b_n) X^{n+1} + \delta(b_n) X^n\\
&= y\left(\sum_{n=0}^{N} a_n X^n\right) + y\left(\sum_{n=0}^{M} b_n X^n\right),
\end{aligned}$$

logo y é aditiva e, portanto, $y \in E$. Disso, para todo $f = \sum_{n=0}^{N} a_n X^n \in A[X]$, temos

$$\begin{aligned}
(y \circ i(a))(f) &= y\left(\sum_{n=0}^{N} a a_n X^n\right)\\
&= \sum_{n=0}^{N} \sigma(a a_n) X^{n+1} + \delta(a a_n) X^n\\
&= \sum_{n=0}^{N} \sigma(a)\sigma(a_n) X^{n+1} + (\delta(a) a_n + \sigma(a)\delta(a_n)) X^n\\
&= \sigma(a) \sum_{n=0}^{N} [\sigma(a_n) X^{n+1} + \delta(a_n) X^n] + \delta(a) \sum_{n=0}^{N} a_n X^n\\
&= (i(\sigma(a)) \circ y + i(\delta(a)))(f),
\end{aligned}$$

de onde $y \circ i(a) = i(\sigma(a)) \circ y + i(\delta(a))$ e, portanto, $yi(A) \subseteq i(A) + i(A)y$. Suponha que, para algum $n \geq 1$, vale $y^n i(A) \subseteq \sum_{j=0}^{n} i(A) y^j$. Então

$$y(y^n i(A)) \subseteq y \sum_{j=0}^{n} i(A) y^j = \sum_{j=0}^{n} (yi(A)) y^j \subseteq \sum_{j=0}^{n} (i(A) + i(A)y) y^j = \sum_{j=0}^{n+1} i(A) y^j.$$

Por indução, obtemos que a inclusão vale para todo $n \in \mathbb{N}$. Consequentemente

$$i(A) y^n \cdot i(A) y^m \subseteq i(A) \left(\sum_{j=0}^{n} i(A) y^j\right) y^m = \sum_{j=0}^{n} i(A) y^{m+j}.$$

Isso mostra que $R = \sum_{n\in\mathbb{N}} i(A)y^n$ é um subanel de E, com $i(A) \subseteq R$ e $y \in R$. Em particular, $i\colon A \to R$ satisfaz (i) e (iii). Resta mostrar a unicidade da escrita. Para isso, observe que $y(1_A) = \sigma(1_A)X + \delta(1_A) = 1_A X$ e suponha que, para algum $n \geq 0$, vale $y^n(1_A) = 1_A X^{n+1}$, então

$$y^{n+1}(1_A) = y(y^n(1_A)) = y(1_A X^{n+1}) = \sigma(1_A)X^{n+2} + \sigma(1_A)X^{n+1} = 1_A X^{n+2}.$$

Logo a igualdade vale para todo $n \in \mathbb{N}$. Agora, se $\sum_{n=0}^{N} i(a_n) \circ y^n \equiv 0$, então

$$0 = \left(\sum_{n=0}^{N} i(a_n) \circ y^n\right)(1_A) = \sum_{n=0}^{N}(i(a_n) \circ y^n)(1_A) = \sum_{n=0}^{N} a_n X^{n+1},$$

mas $A[X]$ é um A-módulo à esquerda livre com base $\{X^n \colon n \in \mathbb{N}\}$, de onde segue que $a_n = 0$, para todo $n \in \mathbb{N}$. Com isso $\{y^n \colon n \in \mathbb{N}\}$ é uma base para R como A-módulo à esquerda, de onde vale (ii). $\square$

No resultado acima mostramos a existência de um subanel R de $End(A[X])$ satisfazendo (i)-(iii). Alternativamente, poderíamos definir uma multiplicação no módulo livre $A[X]$ e mostrar que tal operação é associativa e unitária. Como R e $A[X]$ tem base enumerável, pela Proposição 1.1.5 teríamos que $R \simeq A[X]$ como A-módulos à esquerda. O próximo resultado, além de útil na demonstração dos resultados principais deste texto, nos permitirá obter um isomorfismo de anéis entre quaisquer anéis satisfazendo (i)-(iii).

Proposição 1.3.3 (Propriedade Universal das Extensões de Ore)**.** *Sejam A um anel, $\sigma \in End(A)$ e δ uma σ-derivação. Se (R, i, y) satisfaz a Proposição 1.3.2 e (S, j, x) é uma tripla tal que $j\colon A \to S$ é um morfismo de anéis (não necessariamente unitário) satisfazendo*

$$xj(r) = j(\sigma(r))x + j(\delta(r)), \quad \forall r \in A, \tag{1}$$

então existe um único morfismo de anéis $f\colon R \to S$ tal que $f \circ i = j$ e $f(y) = j(1_A)x$.

Demonstração. Defina $f\colon R \to S$ por

$$f\left(\sum_{n=0}^{N} i(r_n)y^n\right) = \sum_{n=0}^{N} j(r_n)x^n, \tag{2}$$

então, de $1_R = y^0$ e $1_S = x^0$, obtemos $(f \circ i)(r) = j(r)$ e $f(y) = f(i(1_A)y) = j(1_A)x$. Para mostrar que f é multiplicativa, dado $m = \sum i(r_n)y^n \in R$, temos

$$\begin{aligned}
f(ym) &= f\left(\sum_{n=0}^{N} yi(r_n)y^n\right) \\
&= f\left(\sum_{n=0}^{N}(i(\sigma(r_n))y + i(\delta(r_n)))y^n\right) && (iii) \\
&= \sum_{n=0}^{N} f(i(\sigma(r_n))y^{n+1}) + f(i(\delta(r_n))y^n) \\
&= \sum_{n=0}^{N} j(\sigma(r_n))x^{n+1} + j(\delta(r_n))x^n && (2)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{n=0}^{N} (j(\sigma(r_n))x + j(\delta(r_n)))x^n \\
&= \sum_{n=0}^{N} xj(r_n)x^n && (1) \\
&= xf(m).
\end{aligned}
$$

Suponha que, para $k \geq 1$, vale $f(y^k m) = x^k f(m)$. Então

$$f(y^{k+1}m) = f(yy^k m) = xf(y^k m) = xx^k f(m) = x^{k+1} f(m).$$

Por indução, obtemos

$$f(y^k m) = x^k f(m), \quad \forall k \in \mathbb{N}, \tag{3}$$

Agora, dado $s \in A$, por i e j serem morfismos de anéis, temos

$$f(i(s)m) = f\left(\sum_{n=0}^{N} i(sr_n)y^n\right) \overset{(2)}{=} \sum_{n=0}^{N} j(sr_n)x^n = j(s)f(m). \tag{4}$$

de onde, se $m' \in R$, então

$$
\begin{aligned}
f(mm') &= f\left(\sum_{n=0}^{N} (i(r_n)y^n)m'\right) \\
&= \sum_{n=0}^{N} f(i(r_n)(y^n m')) \\
&= \sum_{n=0}^{N} j(r_n)f(y^n m') && (4) \\
&= \sum_{n=0}^{N} j(r_n)x^n f(m') && (3) \\
&= \left(\sum_{n=0}^{N} j(r_n)x^n\right) f(m') \\
&= f\left(\sum_{n=0}^{N} i(r_n)y^n\right) f(m') \\
&= f(m)f(m').
\end{aligned}
$$

Logo f é multiplicativa. Para a unicidade de f, se $(j(1_A)x)^n = j(1_A)x^n$, para algum $n \geq 1$ - notando que $(f(1_A)x)^1 = j(1_A)x = j(1_A)x^1$ - então

$$
\begin{aligned}
(j(1_A)x)^{n+1} &= j(1_A)x(j(1_A)x)^n \\
&= j(1_A)xj(1_A)x^n && (h.i.) \\
&= j(1_A)[j(\sigma(1_A))x + j(\delta(1_A))]x^n && (1) \\
&= j(1_A)[j(1_A)x]x^n \\
&= j(1_A)x^{n+1}.
\end{aligned}
$$

Logo, por indução, obtemos $(j(1_A)x)^n = j(1_A)x^n$, para todo $n \in \mathbb{N}$. Com isso, se $f' \colon R \to S$ é um morfismo aditivo e multiplicativo satisfazendo $f' \circ i = j$ e $f'(y) = j(1_A)x$, então

$$\begin{aligned} f'\left(\sum_{n=0}^{N} i(r_n)y^n\right) &= \sum_{n=0}^{N}(f' \circ i)(r_n)f'(y)^n \\ &= \sum_{n=0}^{N} j(r_n)(j(1_A)x)^n \\ &= \sum_{n=0}^{N} j(r_n)j(1_A)x^n = f\left(\sum_{n=0}^{N} i(r_n)y^n\right), \end{aligned}$$

de onde $f' = f$. □

No enunciado da última proposição, apontamos que $j \colon A \to S$ é um morfismo de anéis não necessariamente unitário. Como $1_R = i(1_A)$ e $f \circ i = j$, se $j(1_A) = 1_S$, então $f(1_R) = j(1_A) = 1_S$, enquanto que, se $f(1_R) = 1_S$d, então $j(1_A) = f(1_R) = 1_S$. Ou seja, f é unitário se, e somente se, j for unitário, e neste caso $f(y) = j(1_A)x = x$ e f é um morfismo de A-módulos à esquerda, onde as estruturas de R e S são induzidas por i e j.

Com isso, se (R, i, y) e (S, j, x) satisfazem a Proposição 1.3.2 então, da Unicidade via Propriedade Universal, obtemos que $R \simeq S$, como A-módulos à esquerda e como anéis. Mais ainda, como existe um isomorfismo de A-módulos à esquerda $g \colon R \to A[X]$ tal que $g(y) = X$, podemos induzir uma multiplicação em $A[X]$ por $m(p, q) = g(g^{-1}(p)g^{-1}(q))$, de forma que: $(A[X], g \circ i, X)$ satisfaz a Proposição 1.3.2; $(g \circ i)(1_A) = g(1_R) = 1_{A[X]} = 1_A$ e, como g e i são morfismos de módulos, obtemos $(g \circ i)(r) = r$, para todo $r \in A$.

Definição 1.3.4. Sejam A um anel, $\sigma \in End(A)$ e δ uma σ-derivação. Uma **extensão de Ore** associada a σ e δ é uma tripla (R, j, X) satisfazendo a Proposição 1.3.2. Neste caso podemos assumir $A \subseteq R$ e vamos denotar $R = A[X; \sigma, \delta]$.

Exemplo 1.3.5. Abaixo listamos alguns exemplos de extensões de Ore.

(1) A identidade $id \colon A \to A$, $r \mapsto r$, é sempre um morfismo de anéis, e a aplicação nula $0 \colon A \to A$, $r \mapsto 0$, é uma σ-derivação para todo morfismo σ. Em particular, o anel de polinômios $A[X] = A[X; id, 0]$ é uma extensão de Ore.

(2) Sejam k um anel comutativo, $A = k[t]$, $q \in k \setminus \{0\}$ e $\sigma \colon A \to A$ tal que $t^n \mapsto q^n t^n$. Então $k[t][X; \sigma, 0]$ é uma extensão de Ore, onde $Xt = qtX$.

(3) Sejam $\sigma \in End(A)$, $q \in A$. Defina $\delta \colon A \to A$ por $\delta(r) = qr - \sigma(r)q$. Então δ é uma σ-derivação e $A[X; \sigma, \delta]$ é uma extensão de Ore, onde $Xr = \sigma(r)(X - q) + qr$.

(4) Seja $A = C^\infty(\mathbb{R})$ o anel das funções $\mathbb{R} \to \mathbb{R}$ infinitamente diferenciáveis. Considere $\frac{d}{dt} \colon A \to A$ o operador de derivação, $f \mapsto df/dt = f'$. Então δ é uma id_A-derivação e $C^\infty(\mathbb{R})[X; id, \frac{d}{dt}]$ é uma extensão de Ore, onde $f' = Xf - fX$.

Vamos finalizar esta seção com alguns resultados sobre o cálculo em extensões de Ore. Para o primeiro, como $X^n r \in A[X; \sigma, \delta]$, pela regra do grau, devem existir únicos $r_0, \ldots, r_n \in A$ tais que $X^n r = r_0 + r_1 X + \cdots + r_n X^n$. Os coeficientes r_j, $j = 0, \ldots, n$, podem ser determinados explicitamente via uma expressão combinatória, porém, uma versão mais simples deste resultado será suficiente para este trabalho.

Lema 1.3.6. *Sejam $A[X;\sigma,\delta]$ uma extensão de Ore, $r \in A$ e $n \in \mathbb{N}$. Então existem $r_1,\dots,r_{n-1} \in A$ tais que*

$$X^n r = \sigma^n(r)X^n + \delta^n(r) + \sum_{j=1}^{n-1} r_j X^j.$$

Demonstração. Por indução, se $n = 0$, então $X^0 r = r$, enquanto que o lado direito da igualdade enunciada possui apenas o termo livre, $\delta^0(r) = id(r) = r$. Supondo a fórmula válida para algum $n \geq 0$, obtemos

$$\begin{aligned}
X^{n+1}r &= X^n[Xr] = X^n[\sigma(r)X + \delta(r)] = [X^n\sigma(r)]X + X^n\delta(r) \\
&= \left[\sigma^n(\sigma(r))X^n + \delta^n(\sigma(r)) + \sum_{j=1}^{n-1}\sigma(r)_j X^j\right] X \qquad\qquad (h.i.) \\
&\quad + \sigma^n(\delta(r))X^n + \delta^n(\delta(r)) + \sum_{j=1}^{n-1}\delta(r)_j X^j \\
&= \sigma^{n+1}(r)X^{n+1} + \delta^{n+1}(r) \\
&\quad + \left[\delta^n(\sigma(r))X + \sigma^n(\delta(r))X^n + \sum_{j=1}^{n-1}\sigma(r)_j X^{j+1} + \sum_{j=1}^{n-1}\delta(r)_j)X^j\right].
\end{aligned}$$

Notando que o termo entre colchetes na última igualdade contém apenas termos com grau entre 1 e n, segue que podemos escrever

$$X^{n+1}r = \sigma^{n+1}(r)X^{n+1} + \delta^{n+1}(r) + \sum_{j=1}^{n} r_j X^j.$$

□

Em alguns momentos estaremos interessados apenas no coeficiente líder de um polinômio em $A[X;\sigma,\delta]$ - neste caso vamos denotar $p = \sum_{n=0}^{N} r_n X^n = r_N X^N + \mathcal{O}(X^{N-1})$ - ou no coeficiente linear - e neste caso escrevemos $p = r_0 + p'X$ onde $p' \in A[X;\sigma,\delta]$.

Seja $A[X;\sigma,\delta]$ uma extensão de Ore. Considere $\mathcal{U}(\delta)$ o A-submódulo à esquerda de ${}_AA$ gerado por $\delta(A)$, ou seja, o conjunto das somas finitas da forma $r\delta(s)$, $r,s \in A$. Então $\mathcal{U}(\delta)$ é um ideal à esquerda de A por definição, e como δ é uma σ-derivação, vale

$$r\delta(ss') = r(\delta(s)s' + \sigma(s)\delta(s')) = r\delta(s)s' + r\sigma(s)\delta(s'),$$

de onde $r\delta(s)s' = r\delta(ss') - r\sigma(s)\delta(s') \in \mathcal{U}(\delta)$. Logo $\mathcal{U}(\delta)$ é um ideal bilateral que, como ideal, é gerado por $\delta(A)$. Mais ainda, de $\delta(r\delta(s)) = \delta(r)\delta(s) + \sigma(r)\delta^2(s) \in \mathcal{U}(\delta)$, obtemos $\delta(\mathcal{U}(\delta)) \subseteq \mathcal{U}(\delta)$ - portanto $\mathcal{U}(\delta)$ é um ideal **δ-invariante**, também chamado **δ-ideal**.

Lema 1.3.7. *Sejam k um anel comutativo, A uma k-álgebra, $g \in A$, $A[X;\sigma,\delta]$ uma extensão de Ore de A e $\mathcal{U}(\delta)$ o ideal bilateral de A gerado por $\delta(A)$. Suponha que $A[X;\sigma,\delta]$ seja uma k-álgebra. Então, para todo $n \in \mathbb{N}$, existem $C_{i,j}^{(n)} \in A$ tais que*

$$(X \otimes 1 + g \otimes X)^n = \sum_{i,j=0}^{n} C_{i,j}^{(n)} X^i \otimes X^j,$$

onde $C_{n,0}^{(n)} = 1$, $C_{0,n}^{(n)} = g^n$ e, para todo $j < n$, $C_{j,0}^{(n)} = 0$ e $C_{0,j}^{(n)} \in \mathcal{U}(\delta)$.

Demonstração. Vamos obter os elementos $C_{i,j}^{(n)}$ destacados por indução. Se $n = 1$, temos

$$(X \otimes 1 + g \otimes X)^1 = 1X^1 \otimes X^0 + gX^0 \otimes X^1 + 0X^0 \otimes X^0,$$

portanto $C_{1,0}^{(1)} = 1$, $C_{0,1}^{(1)} = g$ e $C_{0,0}^{(1)} = 0 \in \mathcal{U}(\delta)$. Suponha o enunciado válido para algum $n \geq 1$, então

$$\begin{aligned}
&(X \otimes 1 + g \otimes X)^{n+1} \\
&= (X \otimes 1 + g \otimes X) \left(\sum_{i,j=0}^{n} C_{i,j}^{(n)} X^i \otimes X^j \right) \\
&= \sum_{i,j=0}^{n} X C_{i,j}^{(n)} X^i \otimes X^j + \sum_{i,j=0}^{n} g C_{i,j}^{(n)} X^i \otimes X X^j \\
&= \sum_{i,j=0}^{n} (\sigma(C_{i,j}^{(n)}) X + \delta(C_{i,j}^{(n)})) X^i \otimes X^j + \sum_{i,j=0}^{n} g C_{i,j}^{(n)} X^i \otimes X^{j+1} \\
&= \sum_{i,j=0}^{n} \sigma(C_{i,j}^{(n)}) X^{i+1} \otimes X^j + \sum_{i,j=0}^{n} \delta(C_{i,j}^{(n)}) X^i \otimes X^j + \sum_{i,j=0}^{n} g C_{i,j}^{(n)} X^i \otimes X^{j+1}.
\end{aligned}$$

Na expressão acima, o termo $X^{n+1} \otimes X^0$ ocorre apenas no somatório à esquerda quando $(i, j) = (n, 0)$, portanto $C_{n+1,0}^{(n+1)} = \sigma(C_{n,0}^{(n)}) = \sigma(1) = 1$. O termo $X^0 \otimes X^{n+1}$ ocorre apenas no somatório à direita quando $(i, j) = (0, n)$, portanto $C_{0,n+1}^{(n+1)} = gC_{0,n}^{(n)} = gg^n = g^{n+1}$. Para $l = 1, \ldots, n$, o termo $X^0 \otimes X^l$ ocorre no segundo somatório quando $(i, j) = (0, l)$, e no terceiro somatório quando $(i, j) = (0, l - 1)$, de onde

$$C_{0,l}^{(n+1)} = \delta(C_{0,l}^{(n)}) + gC_{0,l-1}^{(n)} \in \mathcal{U}(\delta) + g\mathcal{U}(\delta) = \mathcal{U}(\delta),$$

enquanto o termo $X^l \otimes X^0$ ocorre no primeiro somatório quando $(i, j) = (l - 1, 0)$, e no segundo somatório quando $(i, j) = (l, 0)$, portanto, de $\delta(1) = 0$, obtemos

$$C_{l,0}^{(n+1)} = \sigma(C_{l-1,0}^{(n)}) + \delta(C_{l,0}^{(n)}) = \sigma(0) + \delta([l = n]) = 0.$$

Por fim, $X^0 \otimes X^0$ ocorre somente no segundo somatório, com $C_{0,0}^{(n+1)} = \delta(C_{0,0}^{(n)}) = 0$. $\square$

No capítulo seguinte, bem como no lema acima, estaremos interessados nas extensões de Ore que possuem estrutura de álgebra. Mais precisamente, se $u \colon k \to A$ é o morfismo unidade e $i \colon A \to R = A[X; \sigma, \delta]$ é o monomorfismo de anéis da Proposição 1.3.2, queremos que a estrutura de k-álgebra em R seja definida pelo morfismo de anéis $i \circ u$.

Lema 1.3.8. *Sejam (A, u) uma álgebra sobre k e $R = A[X; \sigma, \delta]$ uma extensão de Ore de A com monomorfismo $i \colon A \to R$. Então $(R, i \circ u)$ é uma álgebra sobre k se, e somente se, σ e δ são morfismos de k-módulos.*

Demonstração. ($\Rightarrow$) A função $i \circ u$ é um morfismo de anéis, pois i e u o são. Se (R, iu) é uma álgebra sobre k, então $im(iu) \subseteq Z(R)$. Em particular, deve valer

$$i(u(a))X \overset{hip.}{=} Xi(u(a)) \overset{1.3.2}{=} i(\sigma(u(a)))X + i(\delta(u(a))).$$

Como $R \simeq \bigoplus_{n\in\mathbb{N}} AX^n$ e i é um monomorfismo, segue que $\sigma(u(a)) = u(a)$ e $\delta(u(a)) = 0$, para todo $a \in k$. Como σ é um morfismo de anéis, a condição $\sigma(u(a)) = u(a)$ implica

$$\sigma(u(a)r) = \sigma(u(a))\sigma(r) = u(a)\sigma(r), \quad \forall a \in k, r \in A.$$

Ou seja, σ deve ser um morfismo de módulos. Por outro lado, como δ é uma σ-derivação, a condição $\delta(u(a)) = 0$ implica

$$\delta(u(a)r) = \delta(u(a))r + \sigma(u(a))\delta(r) = u(a)\delta(r), \quad \forall a \in k, r \in A.$$

Portanto δ é um morfismo de módulos.

($\Leftarrow$) Suponha que $R = A[X;\sigma,\delta]$, onde σ e δ são morfismos de módulos. Então, para todo $a \in k$, valem

$$u(a) = u(a)\sigma(1_A) = \sigma(u(a)1_A) = \sigma(u(a)) \quad \text{e} \quad \delta(u(a)) = u(a)\delta(1_A) = 0.$$

De onde $Xi(u(a)) = i(\sigma(u(a)))X + i(\delta(u(a)) = i(u(a))X$. Ou seja, para todo $a \in k$, $i(u(a))$ comuta com X, e consequentemente com X^n, para todo $n \in \mathbb{N}$. Como $im(u) \subseteq Z(A)$,

$$i(u(a))i(r) = i(u(a)r) = i(ru(a)) = i(r)i(u(a)), \quad \forall r \in A.$$

Ou seja, $i(u(a))$ comuta com todo elemento da forma $i(r)$, e consequentemente com todo elemento da forma $i(r)X^n$, para todo $n \in \mathbb{N}$. Isso mostra que $im(i \circ u) \subseteq Z(R)$. $\square$

Ao longo desta seção, definimos e consideramos apenas extensões de Ore como módulos à esquerda livres de base $\{X^n : n \in \mathbb{N}\}$. Quando σ for um morfismo de anéis bijetor, ou seja, $\sigma \in Aut(A)$, podemos considerar $A[X;\sigma,\delta]$ como um A-módulo à direita com mesma base.

Proposição 1.3.9. *Seja $A[X;\sigma,\delta]$ uma extensão de Ore. Se $\sigma \in Aut(A)$, então $A[X;\sigma,\delta]$ é um A-módulo à direita livre de base $\{X^n : n \in \mathbb{N}\}$, via multiplicação.*

Demonstração. Vamos mostrar primeiro a unicidade da escrita do elemento nulo. Suponha que existem $r_0, \ldots, r_N \in A$, com $r_N \neq 0$, tais que $\sum X^n r_n = 0$, então

$$0 = \sum_{n=0}^{N} X^n r_n = \sum_{n=0}^{N} \sigma^n(r_n)X^n + \mathcal{O}(X^{n-1}) = \sigma^N(r_N)X^N + \mathcal{O}(X^{N-1}),$$

de onde $\sigma^N(r_N) = 0$. Como σ, e consequentemente σ^N, é injetiva, deve ser $r_N = 0$, o que é um absurdo. Portanto não é possível escrever o elemento nulo como uma combinação linear à direita não nula de $\{X^n : n \in \mathbb{N}\}$.

Para mostrar que todo elemento de $A[X;\sigma,\delta]$ pode ser escrito como combinação linear à direita, vamos utilizar indução em $n = \deg(p)$. Se $n = 0$ então existe $r_0 \in A$ tal que $p = r_0 = 1r_0$ e não há mais nada a mostrar. Suponha que, para algum $n > 0$, todo elemento $p \in R[X;\sigma,\delta]$ com $\deg(p) < n$, escrito na base à esquerda, pode ser escrito como uma combinação linear à direita de $\{X^n : n \in \mathbb{N}\}$.

Dado $f \in A[X;\sigma,\delta]$ com $\deg(f) = n$, escreva $f = \sum_{i=0}^{n} r_i X^i$ e

$$g := f - X^n\sigma^{-n}(r_n) = f - r_n X^n + \mathcal{O}(X^{n-1}) = \mathcal{O}(X^{n-1}),$$

ou seja, $\deg(g) < n$. Pela hipótese de indução, podemos escrever $g = \sum_{i=0}^{n-1} X^i s_i$. Substituindo g na definição acima, obtemos

$$f = X^n\sigma^{-n}(r_n) + \sum_{i=0}^{n-1} X^i s_i \in \sum_{i=0}^{n} X^i A$$

logo $A[X;\sigma,\delta]$ é gerado, como A-módulo à direita, por $\{X^n : n \in \mathbb{N}\}$. $\square$

Uma extensão de Ore R de A é uma maneira de estender a estrutura do anel A para um *"módulo de dimensão infinita"* de maneira controlada e tal que a inclusão $i\colon A \to R$, em geral, não satisfaz $im(i) \subseteq Z(R)$. Portanto, as extensões de Ore dão exemplos de extensões que não são álgebras.

No próximo capítulo estaremos interessados em estender não só a estrutura de anel, mas a estrutura de álgebra de Hopf fraca de uma k-álgebra A, k sendo um anel comutativo, para sua extensão de Ore R.

1.4 Álgebras de Hopf fracas

Nesta seção vamos definir álgebras de Hopf fracas e desenvolver identidades que serão úteis para se fazer cálculos nesse contexto, tendo como objetivo final dois resultados: mostrar que a antípoda de uma álgebra de Hopf fraca é um anti-morfismo de álgebras e de coálgebras; e caracterizar quando uma álgebra de Hopf fraca é uma álgebra de Hopf. As principais referências desta seção são [4] e [8]. Alguns resultados presentes nas referências anteriores, cuja demonstração foi apresentada apenas em dimensão finita, foram encontrados em sua forma mais geral em [7].

Para fins de comparação, vamos começar definindo e dando exemplos de álgebras de Hopf e, em seguida, passaremos ao estudo das álgebras de Hopf fracas. Nesta seção k denotará um anel comutativo.

Definição 1.4.1. Uma **álgebra de Hopf** é uma sêxtupla $(H, \mu, u, \Delta, \epsilon, S)$, onde:

(H1) (H, μ, u) é uma k-álgebra;

(H2) (H, Δ, ϵ) é uma k-coálgebra;

(H3) μ e u são morfismos de coálgebras, ou equivalentemente, Δ e ϵ são morfismos de álgebras;

(H4) $S \in End_k(H)$ satisfaz $S * id = u \circ \epsilon = id * S$.

Exemplo 1.4.2. Abaixo listamos algumas álgebras que possuem estrutura de álgebra de Hopf, e outras que não podem ser munidas de tal estrutura.

(1) O anel base k com a estrutura de álgebra trivial, (k, m, id), e a estrutura de coálgebra do Exemplo 1.2.8(1), é uma álgebra de Hopf com $S = id$.

(2) Sejam G um grupo e kG a álgebra de grupo do Exemplo 1.2.2(4) com a estrutura de coálgebra do Exemplo 1.2.8(2), então kG é uma de álgebra de Hopf com $S(g) = g^{-1}$, para todo $g \in G$.

(3) O anel $k[X]$ com a estrutura usual de álgebra de polinômios e a estrutura de coálgebra do Exemplo 1.2.8(3) satisfaz (H1)-(H3) da definição acima, mas não pode ser munido com uma estrutura de álgebra de Hopf, pois, neste caso, S deveria satisfazer

$$1_{k[X]} = (u \circ \epsilon)(X) = (S * id)(X) = S(X)X,$$

mas X não possui um inverso à esquerda no anel $k[X]$.

(4) O anel $k[X]$ com a estrutura usual de álgebra de polinômios e a estrutura de coálgebra do Exemplo 1.2.8(4) admite uma estrutura de álgebra de Hopf. Neste caso, $S(1) = 1$, e portanto

$$0 = (u \circ \epsilon)(X) = (S * id)(X) = S(X)1 + S(1)X,$$

de onde obtemos que a identidade (H4) é satisfeita para $S(X) = -X$. Veremos adiante que S é um anti-morfismo de álgebras, de onde, dado $n \in \mathbb{N}$, a identidade $S(X) = -X$ implicará em $S(X^n) = (S(X))^n = (-1)^n X$, determinando S para todo elemento de $k[X]$.

(5) Quando k é um anel simples (sem ideais bilaterais não triviais), a álgebra de matrizes $M_n(k)$, com $n > 1$, não admite nenhuma estrutura de coálgebra que satisfaça (H3). Neste caso, $M_n(k)$ também é simples e, para que $\epsilon\colon M_n(k) \to k$ seja um morfismo de álgebras, $ker(\epsilon)$ deve ser ideal bilateral. Se $\ker(\epsilon) = 0$, então $M_n(k) \simeq k$ como anéis, o que ocorre somente se $n = 1$, enquanto que $\ker(\epsilon) = M_n(k)$ implica em $c = (\epsilon \otimes id)\Delta(c) = 0$, $\forall c \in M_n(k)$, o que também é um absurdo.

Os exemplos (2) e (3) acima mostram que a comultiplicação de um elemento ser "a mais simples possível" - no sentido de não ser uma soma com mais de um termo - está associada com a inversibilidade do elemento, sendo (4) uma maneira de contornar a definição da comultiplicação para elementos não inversíveis, enquanto o exemplo (5) simplesmente mostra a incompatibilidade da estrutura matricial com a noção de álgebras de Hopf.

Existem diversas motivações distintas para a definição de álgebras de Hopf fracas, mas aqui estaremos interessados em definir uma estrutura mais geral que álgebras de Hopf, que englobe as álgebras de matrizes - e consequentemente, as álgebras de grupóides, como veremos adiante - e cuja expressão para comultiplicação de um elemento ser "simples" esteja "um pouco menos" relacionada a sua inversibilidade.

Definição 1.4.3. Uma **álgebra de Hopf fraca** é uma sextupla $(H, \mu, u, \Delta, \epsilon, S)$, onde:

(W1) (H, μ, u) é uma k-álgebra;

(W2) (H, Δ, ϵ) é uma k-coálgebra;

(W3) A comultiplicação Δ preserva a multiplicação de H para $H \otimes H$ e satisfaz

$$(\Delta(1) \otimes 1)(1 \otimes \Delta(1)) = \Delta_2(1) = (1 \otimes \Delta(1))(\Delta(1) \otimes 1);$$

(W4) A counidade ϵ satisfaz as identidades

$$\epsilon(abc) = \epsilon(ab_1)\epsilon(b_2c) = \epsilon(ab_2)\epsilon(b_1c), \quad \forall a, b, c \in H;$$

(W5) Denotando $\Delta(1) = 1_1 \otimes 1_2 \in H \otimes H$, a antípoda $S \in End_k(H)$ satisfaz

(a) $S * id * S = S$;

(b) $(S * id_H)(a) = 1_1\epsilon(a1_2)$, $\forall a \in H$;

(c) $(id_H * S)(a) = \epsilon(1_1a)1_2$, $\forall a \in H$.

Em [4], uma quíntupla $(H, \mu, u, \Delta, \epsilon)$ satisfazendo (W1)-(W4) é chamada **biálgebra fraca**, ou **WBA**, e para álgebras de Hopf fracas é utilizada a sigla **WHA**.

Antes de apresentar exemplos de WHA's será útil reescrever o axioma (W3) mais explicitamente. Considere duas escritas $\Delta(1)$ $\Delta(1) = 1_1 \otimes 1_2 = 1'_1 \otimes 1'_2$. Então, de (W3), são equivalentes

$$\begin{gathered}(\Delta(1) \otimes 1)(1 \otimes \Delta(1)) = \Delta_2(1) = (1 \otimes \Delta(1))(\Delta(1) \otimes 1),\\ (1_1 \otimes 1_2 \otimes 1)(1 \otimes 1'_1 \otimes 1'_2) = \Delta_2(1) = (1 \otimes 1_1 \otimes 1_2)(1'_1 \otimes 1'_2 \otimes 1),\\ 1_1 \otimes 1_2 1'_1 \otimes 1'_2 = 1_1 \otimes 1_2 \otimes 1_3 = 1'_1 \otimes 1_1 1'_2 \otimes 1_2,\end{gathered}$$

e trocando $1_1 \otimes 1_2$ com $1'_1 \otimes 1'_2$ na expressão à direita, obtemos ainda

$$1_1 \otimes 1_2 1'_1 \otimes 1'_2 = 1_1 \otimes 1'_1 1_2 \otimes 1'_2.$$

De forma prática, estas são as igualdades que interessam quando referenciamos (W3).

Exemplo 1.4.4. Abaixo listamos alguns exemplos de álgebras de Hopf fracas.

(1) Toda álgebra de Hopf é uma WHA.

Se Δ é um morfismo de álgebras, então preserva a multiplicação e $\Delta(1) = 1 \otimes 1$, de onde os três termos em (W3) se tornam $1 \otimes 1 \otimes 1$.

Se ϵ é um morfismo de álgebras, então $\epsilon(xy) = \epsilon(x)\epsilon(y)$ e, pelo axioma da counidade e por ϵ ser um morfismo de módulos, temos $\epsilon(b) = \epsilon((u \circ \epsilon)(b_1)b_2) = \epsilon(b_1)\epsilon(b_2)$. Logo

$$\epsilon(abc) = \epsilon(a)\epsilon(b)\epsilon(c) = \epsilon(a)\epsilon(b_1)\epsilon(b_2)\epsilon(c) = \epsilon(ab_1)\epsilon(b_2c).$$

A segunda identidade de (W4) segue da comutatividade de k.

Por fim, de $\Delta(1) = 1 \otimes 1$ temos $\epsilon(1_1a)1_2 = \epsilon(a) = 1_1\epsilon(a1_2)$, de onde (W5)(b) e (W5)(c) correspondem a (H4), enquanto (W5)(a) é satisfeito, pois a unidade da álgebra de convolução $End_k(H)$ é dada por $u \circ \epsilon$. Assim,

$$(S * id) * S = (u \circ \epsilon) * S = S.$$

(2) Para todo $n > 1$, a álgebra de matrizes $M_n(k)$ possui uma estrutura de WHA.

Vamos definir tal estrutura utilizando que $M_n(k)$ é um k-módulo livre de base $\{e_{ij} : i, j = 1, \ldots, n\}$, onde e_{ij} denota uma matriz elementar, e a Proposição 1.1.5(iii).

Defina $\Delta(e_{ij}) = e_{ij} \otimes e_{ij}$ e $\epsilon(e_{ij}) = 1$, para todos $i, j = 1, \ldots, n$. Então, pelo Exemplo 1.2.8(2), $(M_n(k), \Delta, \epsilon)$ é uma coálgebra. Para verificar (W3), temos que

$$\begin{aligned}\Delta(e_{ij})\Delta(e_{rs}) &= (e_{ij} \otimes e_{ij})(e_{rs} \otimes e_{rs})\\ &= e_{ij}e_{rs} \otimes e_{ij}e_{rs}\\ &= [j = r]e_{is} \otimes e_{is}\\ &= [j = r]\Delta(e_{is}) = \Delta(e_{ij}e_{rs}),\end{aligned}$$

e, como $\Delta(1) = \sum_{i=1}^n \Delta(e_{ii}) = \sum_{i=1}^n e_{ii} \otimes e_{ii}$, calculamos

$$(\Delta(1) \otimes 1)(1 \otimes \Delta(1)) = \sum_{i,j,r,s=1}^{n} (e_{ii} \otimes e_{ii} \otimes e_{jj})(e_{rr} \otimes e_{ss} \otimes e_{ss})$$

$$
\begin{aligned}
&= \sum_{i,j,r,s=1}^{n} e_{ii}e_{rr} \otimes e_{ii}e_{ss} \otimes e_{jj}e_{ss} \\
&= [i=r][i=s][j=s] \sum_{i,j,r,s=1}^{n} e_{ii} \otimes e_{ii} \otimes e_{jj} \\
&= \sum_{i=1}^{n} e_{ii} \otimes e_{ii} \otimes e_{ii} = \cdots = (1 \otimes \Delta(1))(\Delta(1) \otimes 1),
\end{aligned}
$$

e

$$\Delta_2(1) = \sum_{i=1}^{n} \Delta(e_{ii}) \otimes e_{ii} = \sum_{i=1}^{n} (e_{ii} \otimes e_{ii}) \otimes e_{ii}.$$

De $(e_{ij})_1 \otimes (e_{ij})_2 = \Delta(e_{ij}) = e_{ij} \otimes e_{ij}$, temos

$$
\begin{aligned}
\epsilon(e_{ij}e_{rs})\epsilon(e_{rs}e_{uv}) &= [j=r]\epsilon(e_{is})[s=u]\epsilon(e_{rv}) = [j=r][s=u] \\
&= [j=r][s=u]\epsilon(e_{iv}) = \epsilon(e_{ij}e_{rs}e_{uv}),
\end{aligned}
$$

logo (W4) é válida para os elementos da base de $M_n(k)$. Como ϵ é um morfismo, a identidade vale para todo elemento de $M_n(k)$. Por fim, definindo um morfismo $S\colon M_n(k) \to M_n(k)$ por $S(e_{ij}) = e_{ji}$, obtemos

$$
\begin{aligned}
(S * id_H)(e_{ij}) &= S(e_{ij})e_{ij} = e_{ji}e_{ij} = e_{jj}, \\
(id_H * S)(e_{ij}) &= e_{ij}S(e_{ij}) = e_{ij}e_{ji} = e_{ii},
\end{aligned}
$$

consequentemente, $((S * id_H) * S)(e_{ij}) = e_{jj}e_{ji} = e_{ji} = S(e_{ij})$, e também

$$1_1\epsilon(e_{ij}1_2) = \sum_{r=1}^{n} e_{rr}\epsilon(e_{ij}e_{rr}) = \sum_{r=1}^{n} [j=r]e_{rr} = e_{jj} = (S * id_H)(e_{ij}),$$

e

$$\epsilon(1_1e_{ij})1_2 = \sum_{r=1}^{n} \epsilon(e_{rr}e_{ij})e_{rr} = \sum_{r=1}^{n} [i=r]e_{rr} = e_{ii} = (id_H * S)(e_{ij}),$$

logo (W5) vale para a base de $M_n(k)$ e, portanto, para todos os elementos.

(3) Se H e L são WHA's, então $H \otimes L$ possui uma estrutura de WHA.

Pelos Lemas 1.2.4 e 1.2.9, sabemos que $H \otimes L$ tem uma estrutura de álgebra e de coálgebra. Denote $\Delta_H(1_H) = 1_1 \otimes 1_2 = 1'_1 \otimes 1'_2$ e $\Delta_L(1_L) = {}_11 \otimes {}_21 = {}_11' \otimes {}_21'$, e considere Γ a composição dos isomorfismos τ, de forma que

$$
\begin{aligned}
\Gamma\colon H \otimes L \otimes H \otimes L \otimes H \otimes L &\to H \otimes H \otimes H \otimes L \otimes L \otimes L, \\
\Gamma(a \otimes b \otimes a' \otimes b' \otimes a'' \otimes b'') &= a \otimes a' \otimes a'' \otimes b \otimes b' \otimes b'',
\end{aligned}
$$

então Γ é um morfismo inversível, de onde

$$
\begin{aligned}
&(\Delta(1_{H\otimes L}) \otimes 1_{H\otimes L})(1_{H\otimes L} \otimes \Delta(1_{H\otimes L})) \\
&= (1_1 \otimes {}_11 \otimes 1_2 \otimes {}_21 \otimes 1_H \otimes 1_L)(1_H \otimes 1_L \otimes 1'_1 \otimes {}_11' \otimes 1'_2 \otimes {}_21') \\
&= 1_1 \otimes {}_11 \otimes 1_21'_1 \otimes {}_21_11' \otimes 1'_2 \otimes {}_21' \\
&= \Gamma^{-1}((1_1 \otimes 1_21'_1 \otimes 1'_2) \otimes ({}_11 \otimes {}_21_11' \otimes {}_21'))
\end{aligned}
$$

$$\begin{aligned}
&= \Gamma^{-1}((1_1 \otimes 1_2 \otimes 1_3) \otimes ({}_11 \otimes {}_21 \otimes {}_31)) && (W3)\ p/\ H, L \\
&= 1_1 \otimes {}_11 \otimes 1_2 \otimes {}_21 \otimes 1_3 \otimes {}_31 \\
&= (1_1 \otimes {}_11) \otimes \Delta(1_2 \otimes {}_21) \\
&= ((id_{H\otimes L} \otimes \Delta) \circ \Delta)(1_H \otimes 1_L) = \Delta_2(1_{H\otimes L}),
\end{aligned}$$

e, analogamente, $(1_{H\otimes L} \otimes \Delta(1_{H\otimes L}))(\Delta(1_{H\otimes L}) \otimes 1_{H\otimes L}) = \Delta_2(1_{H\otimes L})$. Portanto vale (W3) em $H \otimes L$. Para (W4), como $im(\epsilon) \subseteq k$ e k é um anel comutativo, temos

$$\begin{aligned}
\epsilon((a \otimes b)(a' \otimes b')(a'' \otimes b'')) &= \epsilon(aa'a'' \otimes bb'b'') \\
&= \epsilon_H(aa'a'')\epsilon_L(bb'b'') \\
&= \epsilon_H(aa'_1)\epsilon_H(a'_2a'')\epsilon_L(bb'_1)\epsilon_L(b'_2b'') && (W4)\ p/\ H, L \\
&= \epsilon_H(aa'_1)\epsilon_L(bb'_1)\epsilon_H(a'_2a'')\epsilon_L(b'_2b'') && (k = k^{op}) \\
&= \epsilon(aa'_1 \otimes bb'_1)\epsilon(a'_2a'' \otimes b'_2b'') \\
&= \epsilon((a \otimes b)(a'_1 \otimes b'_1))\epsilon((a'_2 \otimes b'_2)(a'' \otimes b'')) \\
&= \epsilon((a \otimes b)(a' \otimes b')_1)\epsilon((a' \otimes b')_2(a'' \otimes b'')).
\end{aligned}$$

Analogamente, mostra-se que vale a identidade

$$\epsilon((a \otimes b)(a' \otimes b')(a'' \otimes b'')) = \epsilon((a \otimes b)(a' \otimes b')_2)\epsilon((a' \otimes b')_1(a \otimes b)).$$

Considerando o morfismo $S = S_H \otimes S_L \in End_k(H \otimes L)$, obtemos

$$\begin{aligned}
(S * id_{H\otimes L})(a \otimes b) &= S((a \otimes b)_1)(a \otimes b)_2 \\
&= S(a_1 \otimes b_1)(a_2 \otimes b_2) \\
&= (S_H(a_1) \otimes S_L(b_1))(a_2 \otimes b_2) \\
&= S_H(a_1)a_2 \otimes S_L(b_1)b_2 \\
&= 1_1\epsilon_H(a1_2) \otimes {}_11\epsilon_L(b\ {}_21) && (W5)(b)\ p/\ H, L \\
&= (1_1 \otimes {}_11)\epsilon_H(a1_2)\epsilon_L(b\ {}_21) \\
&= (1_1 \otimes {}_11)\epsilon(a1_2 \otimes b\ {}_21) \\
&= (1_1 \otimes {}_11)\epsilon((a \otimes b)(1_2 \otimes {}_21)) \\
&= (1_{H\otimes L})_1\epsilon((a \otimes b)(1_{H\otimes L})_2),
\end{aligned}$$

de onde vale (W5)(b) para $H \otimes L$. Analogamente, utilizando que vale o axioma (W5)(c) em H e L, mostra-se que vale (W5)(c) em $H \otimes L$. Por fim calculamos

$$\begin{aligned}
&(S * id_{H\otimes L} * S)(a \otimes b) \\
&= S((a \otimes b)_1)(a \otimes b)_2S((a \otimes b)_3) \\
&= S(a_1 \otimes b_1)(a_2 \otimes b_2)S(a_3 \otimes b_3) \\
&= (S_H(a_1) \otimes S_L(b_1))(a_2 \otimes b_2)(S_H(a_3) \otimes S_L(b_3)) \\
&= S_H(a_1)a_2S_H(a_3) \otimes S_L(b_1)b_2S_L(b_3) \\
&= S_H(a) \otimes S_L(b) && (W5)(a)\ p/\ H, L \\
&= S(a \otimes b).
\end{aligned}$$

Portanto $S * id_{H\otimes L} * S = S$ e vale (W5)(a) em $H \otimes L$.

(4) Sejam H uma álgebra de Hopf e ke um módulo livre com base $\{e\}$. Então o módulo $H' = ke \oplus H$ admite uma estrutura de álgebra de Hopf fraca sobre k, estendendo a estrutura de álgebra de Hopf de H.

Todo elemento $x \in H'$ pode ser escrito, de maneira única, como $x = re + a$, onde $r \in k$ e $a \in H$. Como H possui tanto estrutura de álgebra quanto de coálgebra, segue dos Lemas 1.2.5 e 1.2.10, com $g = 1_H$, que H' possui estrutura de álgebra e de coálgebra, definidas por

$$\begin{aligned} u(r) &= re, & (re+a)(se+b) &= rse + (rb + sa + ab), \\ \epsilon(re+a) &= 2r + \epsilon_H(a), & \Delta(re+a) &= r(1_H \otimes 1_H + f \otimes f) + \Delta_H(a), \end{aligned}$$

onde $f = e - 1_H$. Vamos verificar o axioma (W3), para isso, como Δ é morfismo de módulos, para verificar que Δ é multiplicativa, é suficiente mostrar que $\Delta(e) = \Delta(e)^2$ e $\Delta(a) = \Delta(e)\Delta(a) = \Delta(a)\Delta(e)$, de onde teremos

$$\begin{aligned} \Delta(re+a)\Delta(se+b) &= rs\Delta(e)^2 + r\Delta(e)\Delta(b) + s\Delta(a)\Delta(e) + \Delta(a)\Delta(b) \\ &= rs\Delta(e) + r\Delta(b) + s\Delta(a) + \Delta(ab) \\ &= \Delta(rse + (rb + sa + ab)) \\ &= \Delta((re+a)(se+b)). \end{aligned}$$

Como $f = e - 1_H = 1_{H'} - 1_H$ e 1_H é idempotente em H', temos que f é um idempotente ortogonal a $1_H \in H'$, ou seja, $1_H f = f 1_H = 0$ e $f^2 = f$, de onde $(1_H \otimes 1_H)(f \otimes f) = (f \otimes f)(1_H \otimes 1_H) = 0$, e portanto

$$\begin{aligned} \Delta(e)^2 &= (1_H \otimes 1_H + f \otimes f)^2 \\ &= (1_H \otimes 1_H)^2 + (f \otimes f)^2 \\ &= 1_H \otimes 1_H + f \otimes f \\ &= \Delta(e). \end{aligned}$$

Mais ainda, para todo $a \in H$, temos $fa = ea - 1_H a = a - a = 0$ e $af = 0$, logo $f \otimes f$ anula $H \otimes H$, à direita e à esquerda, portanto

$$\begin{aligned} \Delta(e)\Delta(a) &= (1_H \otimes 1_H)\Delta_H(a) + (f \otimes f)\Delta_H(a) = \Delta(a), \\ \Delta(a)\Delta(e) &= \Delta_H(a)(1_H \otimes 1_H) + \Delta_H(a)(f \otimes f) = \Delta(a). \end{aligned}$$

Isso mostra que Δ é multiplicativa. Ao mostrar que H' possui estrutura de coálgebra, notamos que $\Delta_2(e) = 1_H \otimes 1_H \otimes 1_H + f \otimes f \otimes f$. Por outro lado, de $1_H f = f 1_H = 0$ temos que $(x \otimes f \otimes y)(x' \otimes 1_H \otimes y') = (x' \otimes 1_H \otimes y')(x \otimes f \otimes y) = 0$, para quaisquer $x, x', y, y' \in H'$, de onde

$$\begin{aligned} (\Delta(e) \otimes e)(e \otimes \Delta(e)) &= (1_H \otimes 1_H \otimes e + f \otimes f \otimes e)(e \otimes 1_H \otimes 1_H + e \otimes f \otimes f) \\ &= 1_H \otimes 1_H \otimes 1_H + f \otimes f \otimes f = \Delta_2(e) \\ &= (e \otimes 1_H \otimes 1_H + e \otimes f \otimes f)(1_H \otimes 1_H \otimes e + f \otimes f \otimes e) \\ &= (e \otimes \Delta(e))(\Delta(e) \otimes e). \end{aligned}$$

Logo, vale (W3). Como toda álgebra de Hopf é uma álgebra de Hopf fraca, valem $\epsilon(a_1)\epsilon(a_2) = \epsilon(a)$ e $\epsilon(ab_1)\epsilon(b_2c) = \epsilon(abc) = \epsilon(ab_2)\epsilon(b_1c)$, para quaisquer $a, b, c \in H$. Como ϵ é morfismo de módulos e $\epsilon|_H = \epsilon_H$,

$$\epsilon((re+a)(se+b)_1)\epsilon((se+b)_2(pe+c))$$

$$
\begin{aligned}
&= \epsilon((re+a)s1_H)\epsilon(1_H(pe+c)) \\
&\quad + \epsilon((re+a)sf)\epsilon(f(pe+c)) \\
&\quad + \epsilon((re+a)b_1)\epsilon(b_2(pe+c)) \\
&= \epsilon(rs1_H + sa)\epsilon(p1_H + c) \\
&\quad + \epsilon(rsf)\epsilon(pf) && (fH = Hf = 0) \\
&\quad + \epsilon(rb_1 + ab_1)\epsilon(pb_2 + b_2c) \\
&= rsp + rs\epsilon(c) + sp\epsilon(a) + s\epsilon(a)\epsilon(c) && (\epsilon(1_H) = 1) \\
&\quad + rsp && (\epsilon(f) = 1) \\
&\quad + rp\epsilon(b) + r\epsilon(bc) + p\epsilon(ab) + \epsilon(abc) \\
&= 2rsp + sp\epsilon(a) + rp\epsilon(b) + rs\epsilon(c) \\
&\quad + p\epsilon(ab) + s\epsilon(ac) + r\epsilon(bc) + \epsilon(abc).
\end{aligned}
$$

Por outro lado,

$$
\begin{aligned}
&\epsilon((re+a)(se+b)(pe+c)) \\
&= \epsilon((rse + [rb + sa + ab])(pe+c)) \\
&= \epsilon(rspe + (rsc + p[rb + sa + ab] + [rb + sa + ab]c)) \\
&= \epsilon(rspe) + \epsilon(rsc) + \epsilon(prb) + \epsilon(psa) \\
&\quad + \epsilon(pab) + \epsilon(rbc) + \epsilon(sac) + \epsilon(abc) \\
&= 2rsp + rs\epsilon(c) + pr\epsilon(b) + ps\epsilon(a) \\
&\quad + p\epsilon(ab) + r\epsilon(bc) + s\epsilon(ac) + \epsilon(abc).
\end{aligned}
$$

Logo vale $\epsilon(xyz) = \epsilon(xy_1)\epsilon(y_2z)$, para quaisquer $x, y, z \in H'$. A demonstração de $\epsilon(xyz) = \epsilon(xy_2)\epsilon(y_1z)$ é análoga. Portanto vale (W4). Por fim, seja $S\colon H' \to H'$ definida por $S(re+a) = re + S_H(a)$. Então S é um morfismo de módulos, pois $S(s(re+a)) = S(sre + sa) = sre + sS_H(a) = sS(re+a)$. Como

$$\Delta_2(re+a) = r(1_H \otimes 1_H \otimes 1_H + f \otimes f \otimes f) + \Delta_2(a),$$

e $S(f) = S(e) - S(1_H) = e - 1_H = f$, temos que

$$
\begin{aligned}
(S * id_{H'} * S)(re+a) &= r[S(1_H)1_H S(1_H) + rS(f)fS(f)] + S(a_1)a_2S(a_3) \\
&= r[1_H + f] + S_H(a) \\
&= re + S_H(a) \\
&= S(re+a),
\end{aligned}
$$

de onde vale (W5)(a). Por fim, temos

$$
\begin{aligned}
(S * id_{H'})(re+a) &= r[S(1_H)1_H + S(f)f] + (S_H * id_H)(a) \\
&= r[1_H + f] + \epsilon_H(a)1_H \\
&= re + \epsilon_H(a)1_H \\
&= r[1_H + f] + \epsilon_H(a)1_H \\
&= r[1_H S(1_H) + fS(f)] + (id_H * S_H)(a) \\
&= (id_{H'} * S)(re+a),
\end{aligned}
$$

e

$$\begin{aligned}
e_1\epsilon((re+a)e_2) &= 1_H\epsilon((re+a)1_H) + f\epsilon((re+a)f) \\
&= 1_H\epsilon(r1_H + a) + f\epsilon(rf) && (Hf=0) \\
&= 1_H(r + \epsilon_H(a)) + fr \\
&= r[1_H + f] + \epsilon_H(a)1_H && (im(u) \subseteq Z(H')) \\
&= re + \epsilon_H(a)1_H \\
&= r[1_H + f] + \epsilon_H(a)1_H \\
&= r1_H + \epsilon(a)1_H + rf \\
&= \epsilon(r1_H + a)1_H + \epsilon(rf)f && (fH=0) \\
&= \epsilon(1_H(re+a))1_H + \epsilon(f(re+a))f \\
&= \epsilon(e_1(re+a))e_2.
\end{aligned}$$

Ou seja, $(S * id_{H'})(x) = (id_{H'} * S)(x) = e_1\epsilon(xe_2) = \epsilon(e_1x)e_2 = re + \epsilon_H(a)1_H$, para todo $x = re + a \in H'$. Portanto valem (W5)(b) e (W5)(c). Logo $(H', \mu, u, \Delta, \epsilon, S)$ é uma álgebra de Hopf fraca sobre k.

(5) Sejam $n \geq 1$ e $H = \bigoplus_{i,j=1}^{n} ke_{ij}$ o módulo livre sobre k com base $\{e_{ij} : i, j = 1, \ldots, n\}$. Então H é uma álgebra de Hopf fraca com

$$\mu(e_{ij} \otimes e_{rs}) = [i = r, j = s]e_{ij}, \quad u(1_k) = \sum_{i,j=1}^{n} e_{ij},$$

$$\epsilon(e_{ij}) = [i = j], \quad \Delta(e_{ij}) = \sum_{p=1}^{n} e_{ip} \otimes e_{pj} \quad \text{e} \quad S(e_{ij}) = e_{ji}.$$

A tripla (H, μ, u) é uma álgebra, pois

$$\begin{aligned}
\mu(\mu(e_{ij} \otimes e_{pq}) \otimes e_{rs}) &= [i = p, j = q]\mu(e_{ij} \otimes e_{rs}) \\
&= [i = p, j = q][i = r, j = s]e_{ij} \\
&= [i = p = r, j = q = s]e_{ij} \\
&= [p = r, q = s][i = p, j = q]e_{ij} \\
&= [p = r, q = s]\mu(e_{ij} \otimes e_{pq}) = \mu(e_{ij} \otimes \mu(e_{pq} \otimes e_{rs})),
\end{aligned}$$

e

$$\begin{aligned}
\mu(u(a) \otimes e_{ij}) &= \sum_{p,q=1}^{n} a \triangleright \mu(e_{pq} \otimes e_{ij}) = a \triangleright e_{ij}, \\
\mu(e_{ij} \otimes u(a)) &= \sum_{p,q=1}^{n} a \triangleright \mu(e_{ij} \otimes e_{pq}) = a \triangleright e_{ij}.
\end{aligned}$$

A tripla (H, Δ, ϵ) é uma coálgebra, pois

$$(\Delta \otimes id_H)\Delta(e_{ij}) = \sum_{p=1}^{n} \Delta(e_{ip}) \otimes e_{pj} = \sum_{p,q=1}^{n} (e_{iq} \otimes e_{qp}) \otimes e_{pj}$$

$$= \sum_{p,q=1}^{n} e_{iq} \otimes (e_{qp} \otimes e_{pj}) = \sum_{q=1}^{n} e_{iq} \otimes \Delta(e_{qj}) = (id_H \otimes \Delta)\Delta(e_{ij}),$$

e

$$\mu(\epsilon \otimes id_H)\Delta(e_{ij}) = \sum_{p=1}^{n} \epsilon(e_{ip})e_{pj} = \sum_{p=1}^{n} [p = i]e_{pj} = e_{ij},$$
$$\mu(id_H \otimes \epsilon)\Delta(e_{ij}) = \sum_{p=1}^{n} e_{ip}\epsilon(e_{pj}) = \sum_{p=1}^{n} [p = j]e_{ip} = e_{ij}.$$

Para (W3), verificamos que Δ é multiplicativo,

$$\begin{aligned}
\Delta(e_{ij})\Delta(e_{rs}) &= \left(\sum_{p=1}^{n} e_{ip} \otimes e_{pj}\right)\left(\sum_{q=1}^{n} e_{rq} \otimes e_{qs}\right) = \sum_{p,q=1}^{n} e_{ip}e_{rq} \otimes e_{pj}e_{qs} \\
&= [i = r, j = s] \sum_{p=1}^{n} e_{ip} \otimes e_{pj} = [i = r, j = s]\Delta(e_{ij}) = \Delta(e_{ij}e_{rs}),
\end{aligned}$$

enquanto que

$$\begin{aligned}
(\Delta(1_H) \otimes 1_H)(1_H \otimes \Delta(1_H)) &= \left(\sum_{i,j,p,r,s}^{n} e_{ip} \otimes e_{pj} \otimes e_{rs}\right)\left(\sum_{u,v,q,x,y}^{n} e_{uv} \otimes e_{xq} \otimes e_{qy}\right) \\
&= \sum_{\substack{i,j,p,r,s \\ u,v,q,x,y}}^{n} e_{ip}e_{uv} \otimes e_{pj}e_{xq} \otimes e_{rs}e_{qy} \\
&= \sum_{i,s,p,q}^{n} e_{ip} \otimes e_{pq} \otimes e_{qs} = \Delta_2(1_H).
\end{aligned}$$

Como H é comutativo, temos

$$(\Delta(1_H) \otimes 1_H)(1_H \otimes \Delta(1_H)) = (1_H \otimes \Delta(1_H))(\Delta(1_H) \otimes 1_H),$$

portanto vale (W3). Para verificar (W4), calculamos

$$\begin{aligned}
\epsilon(e_{ij}(e_{uv})_1)\epsilon((e_{uv})_2 e_{rs}) &= \sum_{p=1}^{n} \epsilon(e_{ij}e_{up})\epsilon(e_{pv}e_{rs}) \\
&= \sum_{p=1}^{n} \Big([i = u, j = p]\epsilon(e_{ij})\Big)\Big([p = r, v = s]\epsilon(e_{rs})\Big) \\
&= \sum_{p=1}^{n} \Big([i = u, j = p][i = j]\Big)\Big([p = r, v = s][r = s]\Big) \\
&= \Big([i = u, j = r][i = j]\Big)\Big([j = r, v = s][r = s]\Big) \\
&= [i = u = r, j = v = s][i = j] \\
&= [i = u = r, j = v = s]\epsilon(e_{ij}) \\
&= \epsilon(e_{ij}e_{uv}e_{rs}).
\end{aligned}$$

Analogamente, mostra-se que valem as igualdades

$$\epsilon(e_{ij}(e_{uv})_2)\epsilon((e_{uv})_1e_{rs}) = \epsilon(e_{ij}e_{uv}e_{rs}) = [i = j = u = v = r = s].$$

Portanto vale (W4). Para mostrar (W5), temos por um lado que

$$\epsilon(1_1e_{ij})1_2 = \sum_{r,s,p=1}^{n} \epsilon(e_{rp}e_{ij})e_{ps} = \sum_{s=1}^{n} \epsilon(e_{ij})e_{js} = \sum_{s=1}^{n}[i = j]e_{js},$$
$$1_1\epsilon(e_{ij}1_2) = \sum_{r,s,p=1}^{n} e_{rp}\epsilon(e_{ij}e_{ps}) = \sum_{r=1}^{n} \epsilon(e_{ij})e_{ri} = \sum_{r=1}^{n}[i = j]e_{ri}.$$

Por outro, calculamos

$$(id_H * S)(e_{ij}) = \sum_{p=1}^{n} e_{ip}S(e_{pj}) = \sum_{p=1}^{n} e_{ip}e_{jp} = \sum_{p=1}^{n}[i = j]e_{jp} = \epsilon(1_1e_{ij})1_2,$$
$$(S * id_H)(e_{ij}) = \sum_{p=1}^{n} S(e_{ip})e_{pj} = \sum_{p=1}^{n} e_{pi}e_{pj} = \sum_{p=1}^{n}[i = j]e_{pi} = 1_1\epsilon(e_{ij}1_2).$$

Portanto, valem (W5)(b) e (W5)(c). Por fim, temos

$$\begin{aligned}
((S * id_H) * S)(e_{ij}) &= \sum_{p,q=1}^{n} [S(e_{iq})e_{qp}]S(e_{pj}) \\
&= \sum_{p,q=1}^{n} [e_{qi}e_{qp}]e_{jp} \\
&= \sum_{q=1}^{n} e_{qi}e_{ji} \\
&= e_{ji} = S(e_{ij}).
\end{aligned}$$

De onde $(H, \mu, u, \Delta, \epsilon, S)$ é uma álgebra de Hopf fraca sobre k.

Como consequência dos exemplos (1)-(3) acima, podemos produzir novas álgebras de Hopf fracas a partir de álgebras de Hopf, tomando o produto tensorial por $M_n(k)$. No próximo capítulo mostraremos que, se $\mathcal{G}$ é um grupóide conexo, então a álgebra de grupóide $k\mathcal{G}$ é isomorfa a $kG \otimes M_n(k) \simeq M_n(kG)$ como álgebras de Hopf fracas, e esta caracterização tornará mais fácil o processo de determinar os caracteres de $k\mathcal{G}$, bem como outros elementos importantes para o resultado central deste texto.

O Exemplo 1.4.4(4) foi proposto em [5], no contexto de álgebras de Hopf fracas sobre corpos de característica zero, como um método de obter uma álgebra de Hopf fraca H' a partir de uma álgebra de Hopf H, aumentando a dimensão de H em 1. Este método foi chamado de "construção tipo de Kaplansky", assim, mencionaremos H' como uma **álgebra de Hopf fraca de Kaplansky**. O Exemplo 1.4.4(5) é um caso particular de uma "álgebra de face de Hayashi", geralmente apresentada como uma biálgebra fraca associada a um grafo orientado - vide [13, Example 2.6]. No caso em que o grafo não possui arestas, esta álgebra admite a estrutura de álgebra de Hopf fraca apresentada acima. Mencionaremos este exemplo como uma **álgebra de Hopf fraca de Hayashi**. No próximo capítulo, vamos calcular os caracteres e elementos group-like fracos das álgebras de Hopf fracas de

Kaplansky e de Hayashi.

Para o restante desta seção, $(H, \mu, u, \Delta, \epsilon, S)$ denotará uma álgebra de Hopf fraca sobre um anel comutativo k. No decorrer deste texto, serão essenciais as funções

$$\begin{array}{llll} \epsilon_t\colon H \to H & \epsilon_s\colon H \to H & \epsilon_t'\colon H \to H & \epsilon_s'\colon H \to H \\ \quad a \mapsto \epsilon(1_1 a)1_2 & \quad a \mapsto 1_1\epsilon(a1_2) & \quad a \mapsto \epsilon(a1_1)1_2 & \quad a \mapsto 1_1\epsilon(1_2 a) \end{array}$$

as quais são morfismos de k-módulos, por serem composições dos morfismos Δ, μ, ϵ e τ e da ação $\epsilon(a) \triangleright b = (u \circ \epsilon)(a)b$. No caso de H ser uma álgebra de Hopf, temos $\epsilon_t = \epsilon_s = \epsilon_t' = \epsilon_s' = u\epsilon$, e no contexto de álgebras de Hopf fracas, valem $\epsilon_t = id_H * S$ e $\epsilon_s = S * id_H$. Os resultados desta seção contém itens com afirmações *simétricas* sobre estes quatro morfismos, e suas demonstrações são muito semelhantes, portanto apresentaremos integralmente as demonstrações envolvendo ϵ_t, indicando as mudanças adequadas para os demais itens, sem prolongar o texto com suas demonstrações completas.

Lema 1.4.5. *Para quaisquer $a, b \in H$ valem:*

(i) $\epsilon_t \circ \epsilon_t = \epsilon_t$;

(ii) $\epsilon(a\epsilon_t(b)) = \epsilon(ab)$;

(iii) $\epsilon_t(a\epsilon_t(b)) = \epsilon_t(ab)$;

(iv) $\epsilon_s \circ \epsilon_s = \epsilon_s$;

(v) $\epsilon(\epsilon_s(a)b) = \epsilon(ab)$;

(vi) $\epsilon_s(\epsilon_s(a)b) = \epsilon_s(ab)$.

Demonstração. Pelo axioma (W3) temos $1_1 \otimes 1_2 1_1' \otimes 1_2' = 1_1 \otimes 1_2 \otimes 1_3$. Multiplicando por $a \otimes 1 \otimes 1$ à direita, obtemos $1_1 a \otimes 1_2 1_1' \otimes 1_2' = 1_1 a \otimes 1_2 \otimes 1_3$, de onde

$$\begin{aligned} (\epsilon_t \circ \epsilon_t)(a) &= \epsilon_t(\epsilon(1_1 a)1_2) \\ &= \epsilon(1_1 a)\epsilon_t(1_2) && (\epsilon_t \text{ morfismo}) \\ &= \epsilon(1_1 a)\epsilon(1_1' 1_2)1_2' \\ &= (\epsilon \otimes \epsilon \otimes id)(1_1 a \otimes 1_2 1_1' \otimes 1_2') && (W3) \\ &= (\epsilon \otimes \epsilon \otimes id)(1_1 a \otimes 1_2 \otimes 1_3) && (W3) \\ &= \epsilon(1_1 a)\epsilon(1_2)1_3 \\ &= \epsilon(1_1 a)1_2 && (u\epsilon * id = id) \\ &= \epsilon_t(a), \end{aligned}$$

isso mostra (i). A demonstração de (iv) é análoga, utilizamos que $im(u\epsilon) \subseteq Z(H)$, de onde $a\epsilon(b) = au\epsilon(b) = u\epsilon(b)a = \epsilon(b)a$. Como ϵ_s é um morfismo de k-módulos, segue que

$$\epsilon_s(a\epsilon(b)) = \epsilon_s(\epsilon(b)a) = \epsilon(b)\epsilon_s(a) = \epsilon_s(a)\epsilon(b).$$

Utilizando esta igualdade e que ϵ é k-linear, temos

$$\epsilon(a\epsilon_t(b)) = \epsilon(a\epsilon(1_1 b)1_2) = \epsilon(a1_2\epsilon(1_1 b)) = \epsilon(a1_2)\epsilon(1_1 b) \overset{(W4)}{=} \epsilon(ab),$$

logo, com a segunda igualdade de (W4), concluímos (ii). Para (v) utilizandos a primeira igualdade de (W4). Por fim utilizamos (ii) para obter (iii),

$$\epsilon_t(a\epsilon_t(b)) = \epsilon(1_1 a\epsilon_t(b))1_2 \overset{(ii)}{=} \epsilon(1_1 ab)1_2 = \epsilon_t(ab),$$

e analogamente, utilizando (v), obtemos (vi). ∎

Como consequência do Lema 1.4.5(i), se $a \in im(\epsilon_t)$, então existe $b \in H$ tal que $a = \epsilon_t(b)$, de onde obtemos $\epsilon_t(a) = (\epsilon_t \circ \epsilon_t)(b) = \epsilon_t(b) = a$. Reciprocamente, a igualdade $a = \epsilon_t(a)$ implica $a \in im(\epsilon_t)$. Por 1.4.5(iv) obtemos $a \in im(\epsilon_s)$ se, e somente se, $a = \epsilon_s(a)$. Com isso, vamos denotar

$$H_t = im(\epsilon_t) = \{a \in H\colon a = \epsilon_t(a)\} \quad \text{e} \quad H_s = im(\epsilon_s) = \{a \in H\colon a = \epsilon_s(a)\}.$$

Como ϵ_t e ϵ_s são morfismos de módulos, obtemos que H_t e H_s são submódulos de H. Ao longo desta seção vamos mostrar, como requisito para obter as propriedades da antípoda, que H_t e H_s são também subálgebras de H.

Lema 1.4.6. *Para $n \geq 2$, denotando $\Delta_{n-1}(1) = 1_1 \otimes \cdots \otimes 1_n$, temos:*

(i) $1_1 \otimes \cdots \otimes 1_n = 1_1 \otimes \cdots \otimes 1_{n-1} \otimes \epsilon_t(1_n)$*;*

(ii) $1_1 \otimes \cdots \otimes 1_n = \epsilon_s(1_1) \otimes 1_2 \otimes \cdots \otimes 1_n$*;*

(iii) $a \in H_t$ *se, e somente se,* $\Delta(a) = 1_1 a \otimes 1_2$*. Nesse caso* $\Delta(a) = a1_1 \otimes 1_2$*;*

(iv) $a \in H_s$ *se, e somente se,* $\Delta(a) = 1_1 \otimes a1_2$*. Nesse caso* $\Delta(a) = 1_1 \otimes 1_2 a$*.*

Demonstração. Com $n = 2$, utilizando o axioma da counidade e (W3), obtemos

$$\begin{aligned}
\Delta(1) &= 1_1 \otimes 1_2 \\
&= 1_1 \otimes \epsilon(1_2)1_3 && (id = u\epsilon * id) \\
&= (id \otimes \mu)(id \otimes u\epsilon \otimes id)(1_1 \otimes 1_2 \otimes 1_3) \\
&= (id \otimes \mu)(id \otimes u\epsilon \otimes id)(1_1 \otimes 1'_1 1_2 \otimes 1'_2) && (W3) \\
&= 1_1 \otimes \epsilon(1'_1 1_2)1'_2 \\
&= 1_1 \otimes \epsilon_t(1_2).
\end{aligned}$$

Para $n \geq 3$, utilizando o axioma da coassociatividade, temos

$$\begin{aligned}
\Delta_{n-1}(1) &= ((\Delta_{n-2} \otimes id_H) \circ \Delta)(1) \\
&= (\Delta_{n-2} \otimes id_H)(1_1 \otimes 1_2) \\
&= (\Delta_{n-2} \otimes id_H)(1_1 \otimes \epsilon_t(1_2)) && (n = 2) \\
&= 1_1 \otimes \cdots \otimes 1_{n-1} \otimes \epsilon_t(1_n),
\end{aligned}$$

portanto vale (i). A demonstração de (ii) utiliza $id = id * u\epsilon$ e (W3) quando $n = 2$, e $\Delta_{n-1} = (id_H \otimes \Delta_{n-2}) \circ \Delta$ quando $n \geq 3$.

Suponha $a \in H_t$, então

$$\begin{aligned}
\Delta(a) &= \Delta(\epsilon_t(a)) && 1.4.5(i) \\
&= \Delta(\epsilon(1_1 a)1_2) \\
&= \epsilon(1_1 a)\Delta(1_2) && (\Delta \text{ morfismo}) \\
&= \epsilon(1_1 a)1_2 \otimes 1_3 \\
&= (\mu \otimes id)(\epsilon \otimes id \otimes id)(1_1 a \otimes 1_2 \otimes 1_3) \\
&= (\mu \otimes id)(\epsilon \otimes id \otimes id)(1'_1 a \otimes 1_1 1'_2 \otimes 1_2) && (W3) \\
&= \epsilon(1'_1 a)1_1 1'_2 \otimes 1_2 \\
&= 1_1 \epsilon(1'_1 a)1'_2 \otimes 1_2 && (im(u\epsilon) \subseteq Z(H))
\end{aligned}$$

$$
\begin{aligned}
&= 1_1\epsilon_t(a) \otimes 1_2 \\
&= 1_1 a \otimes 1_2. && 1.4.5(i)
\end{aligned}
$$

Reciprocamente, se $\Delta(a) = 1_1 a \otimes 1_2$, então, aplicando $\mu \circ (u\epsilon \otimes id)$, obtemos

$$a = (u\epsilon * id)(a) = (\mu \circ (u\epsilon \otimes id) \circ \Delta)(a) = \epsilon(1_1 a)1_2 = \epsilon_t(a),$$

de onde $a \in H_t$. Retomando o cálculo anterior, temos

$$
\begin{aligned}
\Delta(a) &= (\mu \otimes id)(\epsilon \otimes id \otimes id)(1_1 a \otimes 1_2 \otimes 1_3) \\
&= (\mu \otimes id)(\epsilon \otimes id \otimes id)(1'_1 a \otimes 1'_2 1_1 \otimes 1_2) && (W3) \\
&= \epsilon(1'_1 a)1'_2 1_1 \otimes 1_2 \\
&= \epsilon_t(a)1_1 \otimes 1_2 \\
&= a1_1 \otimes 1_2, && 1.4.5(i)
\end{aligned}
$$

de onde vale (iii). A demontração de (iv) é análoga, utilizando que $\epsilon_s(a) = a$ se, e somente se, $a \in H_s$, e versões adequadas de (W3). $\square$

Os itens (i) e (ii) do lema acima, nas bibliografias referenciadas, são enunciados como $\Delta(1) \in H_s \otimes H_t$. Como $\epsilon_t \colon H \to H_t$ e $\epsilon_s \colon H \to H_s$ são morfismos de módulos, segue da Propriedade Universal do Produto Tensorial que $\epsilon_s \otimes \epsilon_t \colon H \otimes H \to H_s \otimes H_t$, dada por $(\epsilon_s \otimes \epsilon_t)(a \otimes b) = \epsilon_s(a) \otimes \epsilon_t(b)$, está bem definida. Utilizando os itens (i) e (ii) acima, obtemos que $\Delta(1) = 1_1 \otimes 1_2 = \epsilon_s(1_1) \otimes \epsilon_t(1_1) \in im(\epsilon_s \otimes \epsilon_t) \subseteq H_s \otimes H_t$. Porém, sempre que utilizarmos este resultado, estaremos interessados nas identidades (i) e (ii).

Lema 1.4.7. *Sejam $a, b \in H$, então:*

(i) $a_1 \otimes a_2 S(a_3) = 1_1 a \otimes 1_2$;

(ii) $a\epsilon_t(b) = \epsilon(a_1 b)a_2$;

(iii) $S(a_1)a_2 \otimes a_3 = 1_1 \otimes a1_2$;

(iv) $\epsilon_s(a)b = b_1\epsilon(ab_2)$.

Demonstração. Como Δ é multiplicativo, temos $\Delta(a) = \Delta(1)\Delta(a)$, ou seja, valem as identidades $a_1 \otimes a_2 = 1_1 a_1 \otimes 1_2 a_2$ e $1_1 a_1 \otimes 1_2 a_2 \otimes 1_3 = (1_1 a)_1 \otimes (1_1 a)_2 \otimes 1_2$, de onde

$$
\begin{aligned}
a_1 \otimes a_2 S(a_3) &= a_1 \otimes \epsilon(1_1 a_2)1_2 && (W5)(c) \\
&= a_1\epsilon(1_1 a_2) \otimes 1_2 && (im(\epsilon) \subseteq k) \\
&= 1'_1 a_1 \epsilon(1_1 1'_2 a_2) \otimes 1_2 \\
&= ((\mu \circ (id_H \otimes \epsilon)) \otimes id_H)((1'_1 \otimes 1_1 1'_2 \otimes 1_2)(a_1 \otimes a_2 \otimes 1_H)) \\
&= ((\mu \circ (id_H \otimes \epsilon)) \otimes id_H)((1_1 \otimes 1_2 \otimes 1_3)(a_1 \otimes a_2 \otimes 1_H)) && (W3) \\
&= ((\mu \circ (id_H \otimes \epsilon)) \otimes id_H)(1_1 a_1 \otimes 1_2 a_2 \otimes 1_3) \\
&= ((\mu \circ (id_H \otimes \epsilon)) \otimes id_H)((1_1 a)_1 \otimes (1_1 a)_2 \otimes 1_2) \\
&= (1_1 a)_1 \epsilon((1_1 a)_2) \otimes 1_2 \\
&= 1_1 a \otimes 1_2, && (id * u\epsilon = id)
\end{aligned}
$$

portanto vale (i). O cálculo de (iii) é análogo utilizando (W5)(b), (W3) e $u\epsilon * id = id$.

Para (ii) e (iv), lembramos que H é um k-módulo via $r \triangleright a = u(r)a$, de onde vale a igualdade $\epsilon(b) \triangleright a = (u \circ \epsilon)(b)a$, a qual denotamos por $\epsilon(b)a$. Assim, temos

$$a\epsilon_t(b) = a\epsilon(1_1 b)1_2$$

$$
\begin{aligned}
&= \epsilon(a_1)a_2\epsilon(1_1b)1_2 && (id = u\epsilon * id)\\
&= \epsilon(a_1)\epsilon(1_1b)a_21_2 && (im(u\epsilon) \subseteq Z(H))\\
&= \mu_2(\epsilon \otimes \epsilon \otimes id_H)((a_1 \otimes 1_1 \otimes a_21_2)(1_H \otimes b \otimes 1_H))\\
&= \mu_2(\epsilon \otimes \epsilon \otimes id_H)((a_1 \otimes S(a_2)a_3 \otimes a_4)(1_H \otimes b \otimes 1_H)) && (iii)\\
&= \epsilon(a_1)\epsilon(S(a_2)a_3b)a_4\\
&= \epsilon(a_1)\epsilon(\epsilon_s(a_2)b)a_3 && (W5)(b)\\
&= \epsilon(a_1)\epsilon(a_2b)a_3 && 1.4.5(v)\\
&= \epsilon(\epsilon(a_1)a_2b)a_3 && (\epsilon \text{ morfismo})\\
&= \epsilon(a_1b)a_2, && (u\epsilon * id = id)
\end{aligned}
$$

portanto vale (ii). A demonstração de (iv) utiliza $id = id * u\epsilon$, (i) deste lema, (W5)(c), o Lema 1.4.5(ii) e, por fim, novamente $id * u\epsilon = id$. □

Como observado anteriormente, H_s e H_t são submódulos de H, pois são imagem dos morfismos ϵ_s e ϵ_t. Pelo axioma da counidade, obtemos $1_H \in H_s$ e $1_H \in H_t$, pois

$$\epsilon_s(1_H) = 1_1\epsilon(1_H1_2) = 1_1\epsilon(1_2) = 1_H = \epsilon(1_1)1_2 = \epsilon(1_11_H)1_2 = \epsilon_t(1_H).$$

Com o lema acima, podemos provar que estes submódulos são subálgebras de H.

Proposição 1.4.8. *Os subconjuntos $H_s, H_t \subseteq H$ são subálgebras de H. Mais ainda, para quaisquer $s \in H_s$ e $t \in H_t$, vale $st = ts$.*

Demonstração. Sejam $s \in H_s$ e $t \in H_t$, então

$$
\begin{aligned}
st &= \epsilon_s(s)\epsilon_t(t) && 1.4.5(i)\\
&= 1'_1\epsilon(s1'_2)\epsilon(1_1t)1_2\\
&= \epsilon(1_1t)1'_11_2\epsilon(s1'_2) && (im(u\epsilon) \subseteq Z(H))\\
&= \mu_2(\epsilon \otimes id \otimes \epsilon)((1 \otimes 1 \otimes s)(1_1 \otimes 1'_11_2 \otimes 1'_2)(t \otimes 1 \otimes 1))\\
&= \mu_2(\epsilon \otimes id \otimes \epsilon)((1 \otimes 1 \otimes s)(1_1 \otimes 1_21'_1 \otimes 1'_2)(t \otimes 1 \otimes 1)) && (W3)\\
&= \epsilon(1_1t)1_21'_1\epsilon(s1'_2)\\
&= \epsilon_t(t)\epsilon_s(s)\\
&= ts. && 1.4.5(i)
\end{aligned}
$$

Isto prova a segunda afirmação enunciada. Pela observação anterior, resta mostrar que, dados $a, b \in H_t$, vale $ab \in H_t$, e analogamente para H_s. Para isso, calculamos

$$
\begin{aligned}
ab &= a\epsilon_t(b) && 1.4.5(i)\\
&= \epsilon(a_1b)a_2 && 1.4.7(ii)\\
&= \mu((\epsilon \circ \mu) \otimes id)(\tau \otimes id_H)(b \otimes \Delta(a))\\
&= \mu((\epsilon \circ \mu) \otimes id)(\tau \otimes id_H)(b \otimes 1_1a \otimes 1_2) && 1.4.6(iii)\\
&= \epsilon(1_1ab)1_2\\
&= \epsilon_t(ab) \in H_t,
\end{aligned}
$$

enquanto, para $a, b \in H_s$, utilizamos 1.4.7(iv) e 1.4.6(iv), obtendo $ab \in H_s$. □

O último lema desta seção relaciona os morfismos ϵ_t, ϵ'_t, ϵ_s, ϵ'_s e S.

Lema 1.4.9. *Para todo $a, b \in H$ valem:*

(i) $\epsilon_t(\epsilon_t(a)b) = \epsilon_t(a)\epsilon_t(b)$;

(ii) $\epsilon_t(a) = (\epsilon'_t \circ S)(a) = \epsilon(S(a)1_1)1_2$;

(iii) $\epsilon_t(a) = S(1_1)\epsilon(1_2a)$;

(iv) $\epsilon_t \circ S = \epsilon_t \circ \epsilon_s = S \circ \epsilon_s$;

(v) $\epsilon_s(a\epsilon_s(b)) = \epsilon_s(a)\epsilon_s(b)$;

(vi) $\epsilon_s(a) = (\epsilon'_s \circ S)(a) = 1_1\epsilon(1_2S(a))$;

(vii) $\epsilon_s(a) = \epsilon(a1_1)S(1_2)$;

(viii) $\epsilon_s \circ S = \epsilon_s \circ \epsilon_t = S \circ \epsilon_t$.

Demonstração. Pela Proposição 1.4.8, temos que, se $a, b \in H_t$, então $ab \in H_t$. Em particular, para quaisquer $a, b \in H$, temos $\epsilon_t(a)\epsilon_t(b) \in H_t$. Portanto $\epsilon_t(a)\epsilon_t(b) = \epsilon_t(\epsilon_t(a)\epsilon_t(b))$. Logo

$$\begin{aligned} \epsilon_t(\epsilon_t(a)b) &= \epsilon_t(\epsilon_t(a)\epsilon_t(b)) && 1.4.5(iii) \\ &= \epsilon_t(a)\epsilon_t(b), && 1.4.8 \end{aligned}$$

de onde concluímos (i). A demonstração de (v) utiliza 1.4.5(vi) e a Proposição 1.4.8.

Pelo Lema 1.4.6(ii), temos $1_1 \otimes 1_2 = \epsilon_s(1_1) \otimes 1_2$. Multiplicando por $\epsilon_t(a) \otimes 1_H$ à direita, obtemos $1_1\epsilon_t(a) \otimes 1_2 = \epsilon_s(1_1)\epsilon_t(a) \otimes 1_2$ e, pela Proposição 1.4.8, vale $\epsilon_s(1_1)\epsilon_t(a) \otimes 1_2 = \epsilon_t(a)\epsilon_s(1_1) \otimes 1_2$. Aplicando novamente o Lema 1.4.6(ii), temos $1_1\epsilon_t(a) \otimes 1_2 = \epsilon_t(a)1_1 \otimes 1_2$. Com isso

$$\begin{aligned} \epsilon_t(a) &= \epsilon(1_1a)1_2 \\ &= \epsilon(1_1\epsilon_t(a))1_2 && 1.4.5(ii) \\ &= \mu(\epsilon \otimes id)(1_1\epsilon_t(a) \otimes 1_2) \\ &= \mu(\epsilon \otimes id)(\epsilon_t(a)1_1 \otimes 1_2) && 1.4.8 \\ &= \epsilon(\epsilon_t(a)1_1)1_2 \\ &= \epsilon(a_1S(a_2)1_1)1_2 && (W5)(c) \\ &= \epsilon(\epsilon_s(a_1)S(a_2)1_1)1_2 && 1.4.5(v) \\ &= \epsilon(S(a_1)a_2S(a_3)1_1)1_2 && (W5)(b) \\ &= \epsilon(S(a)1_1)1_2 && (W5)(a) \\ &= (\epsilon'_t \circ S)(a), \end{aligned}$$

e, portanto, vale (ii). A demonstração de (vi) utiliza os Lemas 1.4.5(v), 1.4.6(i) e a Proposição 1.4.8 para obter $1_1 \otimes \epsilon_s(a)1_2 = 1_1 \otimes 1_2\epsilon_s(a)$ e, em seguida, (W5)(b), o Lema 1.4.5(ii), (W5)(c) e (W5)(a).

Pelo Lema 1.4.6(ii), temos $1_1 \otimes 1_2 \otimes 1_3 = \epsilon_s(1_1) \otimes 1_2 \otimes 1_3$. Multiplicando por $1_H \otimes 1_H \otimes a$ à direita e aplicando $id_H \otimes S \otimes \epsilon$, obtemos $1_1 \otimes S(1_2) \otimes \epsilon(1_3a) = \epsilon_s(1_1) \otimes S(1_2) \otimes \epsilon(1_3a)$. Consequentemente, vale $\epsilon_s(1_1)S(1_2)\epsilon(1_3a) = 1_1S(1_2)\epsilon(1_3a)$, portanto

$$\begin{aligned} S(1_1)\epsilon(1_2a) &= S(1_1)1_2S(1_3)\epsilon(1_4a) && (W5)(a) \\ &= \epsilon_s(1_1)S(1_2)\epsilon(1_3a) && (W5)(b) \\ &= 1_1S(1_2)\epsilon(1_3a) && 1.4.6(ii) \\ &= \epsilon_t(1_1)\epsilon(1_2a) && (W5)(c) \\ &= \epsilon(1'_11_1)1'_2\epsilon(1_2a) \\ &= \epsilon(1'_11_1)\epsilon(1_2a)1'_2 && im(u\epsilon) \subseteq Z(H) \\ &= \epsilon(1'_1a)1'_2 && (W4) \\ &= \epsilon_t(a), \end{aligned}$$

de onde vale (iii). A demonstração de (vii) utiliza (W5)(a), (W5)(c) e o Lema 1.4.6(i) para obter a identidade $\epsilon(a1_1)S(1_2)1_3 = \epsilon(a1_1)S(1_2)\epsilon_t(1_3)$, e em seguida (W5)(b), $im(u\epsilon) \subseteq Z(H)$ e (W4).

Por fim calculamos

$$\begin{aligned}
(\epsilon_t \circ S)(a) &= \epsilon_t(S(a_1)a_2S(a_3)) && (W5)(a)\\
&= \epsilon_t(S(a_1)\epsilon_t(a_2)) && (W5)(c)\\
&= \epsilon_t(S(a_1)a_2) && 1.4.5(iii)\\
&= (\epsilon_t \circ \epsilon_s)(a), && (W5)(b)
\end{aligned}$$

e também

$$\begin{aligned}
(\epsilon_t \circ S)(a) &= S(1_1)\epsilon(1_2S(a)) && (iii)\\
&= S(1_1\epsilon(1_2S(a))) && S \text{ morfismo}\\
&= S(\epsilon_s' \circ S)(a) && \\
&= (S \circ \epsilon_s)(a), && (vi)
\end{aligned}$$

de onde vale (iv). Analogamente, utilizando (W5)(a), (W5)(b), o Lema 1.4.5 (vi) e (W5)(c), mostramos $\epsilon_s \circ S = \epsilon_s \circ \epsilon_t$, e com (vii) e (ii), obtemos $\epsilon_s \circ S = S \circ \epsilon_t$, concluindo (viii). □

Para mostrar que a antípoda é um anti-morfismo, observamos que, se X é um conjunto munido de uma operação binária associativa $*$, e $f, g, h \in X$, então um elemento $x \in X$ satisfazendo o sistema de equações

$$\begin{cases} x * f * x = x, \\ x * f = g, \\ f * x = h. \end{cases} \tag{$\star$}$$

se existir, será único. De fato, se $x, y \in X$ satisfazem as igualdades acima, então

$$x = (x * f) * x = g * x = (y * f) * x = y * (f * x) = y * h = y * (f * y) = y.$$

Vamos utilizar esta observação com $X = Hom_k(H \otimes H, H)$ e $X = Hom_k(H, H \otimes H)$, juntamente do produto convolução.

Proposição 1.4.10. *A antípoda S de uma WHA é um anti-morfismo de álgebras e de coálgebras. Mais precisamente, para quaisquer $a, b \in H$ valem:*

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

(ii) $S(1_H) = 1_H$;

(iii) $\Delta(S(a)) = S(a_2) \otimes S(a_1)$;

(iv) $(\epsilon \circ S)(a) = \epsilon(a)$.

Demonstração. Considere $x = S \circ m, y = m \circ \tau \circ (S \otimes S) \in Hom_k(H \otimes H, H)$, então

$$x(a \otimes b) = S(ab) \quad \text{e} \quad y(a \otimes b) = S(b)S(a),$$

logo, para (i), é suficiente mostrar que x e y satisfazem um sistema do tipo ($\star$) na álgebra de convolução $Hom_k(H \otimes H, H)$. Com $f = m$, $g = \epsilon_s \circ m$ e $h = \epsilon_t \circ m$, obtemos

$$x(a \otimes b) = S(ab)$$

$$
\begin{aligned}
&= S((ab)_1)(ab)_2S((ab)_3) && (W5)(a)\\
&= S(a_1b_1)a_2b_2S(a_3b_3)\\
&= (x * m * x)(a \otimes b),
\end{aligned}
$$

e

$$
\begin{aligned}
(m * x)(a \otimes b) &= a_1b_1S(a_2b_2)\\
&= (ab)_1S((ab)_2)\\
&= \epsilon_t(ab) && (W5)(c)\\
&= (\epsilon_t \circ m)(a \otimes b),
\end{aligned}
$$

enquanto que, de (W5)(b), têm-se $x * m = \epsilon_s \circ m$. Logo x satisfaz o sistema $(\star)$ para $(f, g, h) = (m, \epsilon_s \circ m, \epsilon_t \circ m)$. Por outro lado,

$$
\begin{aligned}
(y * m * y)(a \otimes b) &= S(b_1)S(a_1)a_2b_2S(b_3)S(a_3)\\
&= S(b_1)\epsilon_s(a_1)\epsilon_t(b_2)S(a_2) && (W5)(b),(c)\\
&= S(b_1)\epsilon_t(b_2)\epsilon_s(a_1)S(a_2) && 1.4.8\\
&= S(b_1)b_2S(b_3)S(a_1)a_2S(a_2) && (W5)(b),(c)\\
&= S(b)S(a) && (W5)(a)\\
&= y(a \otimes b),
\end{aligned}
$$

e

$$
\begin{aligned}
(m * y)(a \otimes b) &= a_1b_1S(b_2)S(a_2)\\
&= a_1\epsilon_t(b)S(a_2) && (W5)(c)\\
&= \epsilon(a_1b)a_2S(a_3) && 1.4.7(ii)\\
&= \epsilon(a_1b)\epsilon_t(a_2) && (W5)(c)\\
&= \epsilon(a_1b)\epsilon(1_1a_2)1_2\\
&= \epsilon(1_1a_2)\epsilon(a_1b)1_2 && im(u\epsilon) \subseteq Z(H)\\
&= \epsilon(1_1ab)1_2 && (W4)\\
&= \epsilon_t(ab)\\
&= (\epsilon_t \circ m)(a \otimes b),
\end{aligned}
$$

e,analogamente, utilizando (W5)(b), 1.4.7(iv), (W5)(b) e (W4), mostra-se $y * m = \epsilon_s \circ m$. Logo y satisfaz $(\star)$ para $(f, g, h) = (m, \epsilon_s \circ m, \epsilon_t \circ m)$. Pela observação anterior, é único o elemento satisfazendo este sistema, portanto $x = y$. Logo vale (i). De

$$
\begin{aligned}
S(1) &= S(1_1)1_2S(1_3) && (W5)(a)\\
&= \epsilon_s(1_1)S(1_2) && (W5)(b)\\
&= m(id_H \otimes S)(\epsilon_s(1_1) \otimes 1_2)\\
&= m(id_H \otimes S)(1_1 \otimes 1_2) && 1.4.6(ii)\\
&= 1_1S(1_2)\\
&= \epsilon_t(1_H) && (W5)(c)\\
&= 1_H, && 1_H \in H_t, 1.4.5(i)
\end{aligned}
$$

obtemos (ii). Portanto $S\colon H \to H$ é um anti-morfismo de álgebras.

Agora, considere $x = \Delta \circ S, y = (S \otimes S) \circ \tau \circ \Delta \in Hom_k(H, H \otimes H)$, então

$$x(a) = S(a)_1 \otimes S(a)_2 \quad \text{e} \quad y(a) = S(a_2) \otimes S(a_1),$$

portanto, para mostrar (iii), é suficiente mostrar que x e y satisfazem um sistema do tipo ($\star$). Escolha $f = \Delta$, $g = \Delta \circ \epsilon_s$ e $h = \Delta \circ \epsilon_t$, então

$$\begin{aligned} x(a) &= \Delta(S(a)) \\ &= \Delta(S(a_1)a_2S(a_3)) && (W5)(a) \\ &= \Delta(S(a_1))\Delta(a_2)\Delta(S(a_3)) && (W3) \\ &= (x * \Delta * x)(a), \end{aligned}$$

e

$$\begin{aligned} (\Delta * x)(a) &= \Delta(a_1)\Delta(S(a_2)) \\ &= \Delta(a_1S(a_2)) && (W3) \\ &= \Delta(\epsilon_t(a)) && (W5)(c) \\ &= (\Delta \circ \epsilon_t)(a), \end{aligned}$$

e, utilizando (W3) com (W5)(b), mostra-se $x * \Delta = \Delta \circ \epsilon_s$. Portanto, x satisfaz o sistema ($\star$) para $(f, g, h) = (\Delta, \Delta \circ \epsilon_s, \Delta \circ \epsilon_t)$. Por outro lado, temos

$$\begin{aligned} (\Delta * y)(a) &= a_1S(a_4) \otimes a_2S(a_3) \\ &= a_1S(a_3) \otimes \epsilon(1_1a_2)1_2 && (W5)(c) \\ &= a_1\epsilon(1_1a_2)S(a_3) \otimes 1_2 && (im(u\epsilon) \subseteq Z(H), im(\epsilon) \subseteq k) \\ &= \epsilon_s(1_1)a_1S(a_2) \otimes 1_2 && 1.4.7(iv) \\ &= \epsilon_s(1_1)\epsilon_t(a) \otimes 1_2 && (W5)(c) \\ &= (\epsilon_s(1_1) \otimes 1_2)(\epsilon_t(a) \otimes 1_H) \\ &= (1_1 \otimes 1_2)(\epsilon_t(a) \otimes 1_H) && 1.4.6(ii) \\ &= 1_1\epsilon_t(a) \otimes 1_2 \\ &= \Delta(\epsilon_t(a)) && 1.4.6(iii) \\ &= (\Delta \circ \epsilon_t)(a), \end{aligned}$$

enquanto que, de (W5)(b), 1.4.7(ii), (W5)(b), 1.4.6(i) e 1.4.6(iv), obtemos $y * \Delta = \Delta \circ \epsilon_s$. Para mostrar que $y * \Delta * y = y$, temos por 1.4.6(ii) que $1_1 \otimes 1_2 = \epsilon_s(1_1) \otimes 1_2$, de onde, aplicando $S \otimes id_H$ e utilizando 1.4.9(iv), obtemos $S(1_1) \otimes 1_2 = \epsilon_t(\epsilon_s(1_1)) \otimes 1_2$. Usando novamente 1.4.6(ii), resulta $S(1_1) \otimes 1_2 = \epsilon_t(1_1) \otimes 1_2$, logo

$$\begin{aligned} S(1_1) \otimes S(1_2) &= (id_H \otimes S)(S(1_1) \otimes 1_2) \\ &= (id_H \otimes S)(\epsilon_t(1_1) \otimes 1_2) \\ &= \epsilon_t(1_1) \otimes S(1_2) \\ &= \epsilon(1'_1 1_1)1'_2 \otimes S(1_2) \\ &= 1'_2 \otimes \epsilon(1'_1 1_1)S(1_2) && (im(\epsilon) \subseteq k) \\ &= 1'_2 \otimes \epsilon_s(1'_1) && 1.4.9(vii) \\ &= \tau(\epsilon_s(1'_1) \otimes 1'_2) \\ &= \tau(1'_1 \otimes 1'_2) && 1.4.6(ii) \end{aligned}$$

$$= 1'_2 \otimes 1'_1,$$

ou seja, vale a identidade

$$S(1_1) \otimes S(1_2) = 1_2 \otimes 1_1. \qquad (**)$$

Com isso, calculamos

$$\begin{aligned}
(y * \Delta * y)(a) &= (y * (\Delta \circ \epsilon_t))(a) \\
&= (S(a_2) \otimes S(a_1))\Delta(\epsilon_t(a_3)) \\
&= (S(a_2) \otimes S(a_1))(\epsilon_t(a_3)1_1 \otimes 1_2) && 1.4.6(iii) \\
&= S(a_2)\epsilon_t(a_3)1_1 \otimes S(a_1)1_2 \\
&= S(a_2)a_3S(a_4)1_1 \otimes S(a_1)1_2 && (W5)(c) \\
&= S(a_2)1_1 \otimes S(a_1)1_2 && (W5)(a) \\
&= S(a_2)S(1_2) \otimes S(a_1)S(1_1) && (**) \\
&= S(1_2a_2) \otimes S(1_1a_1) && (i) \\
&= ((S \otimes S) \circ \tau)(\Delta(1)\Delta(a)) \\
&= ((S \otimes S) \circ \tau)\Delta(a) && (W3) \\
&= S(a_2) \otimes S(a_1) \\
&= y(a),
\end{aligned}$$

portanto y satisfaz $(\star)$ para $(f, g, h) = (\Delta, \Delta \circ \epsilon_s, \Delta \circ \epsilon_t)$ e, pela unicidade da solução do sistema, $x = y$, logo vale (iii). Por fim, temos

$$\begin{aligned}
(\epsilon \circ S)(a) &= \epsilon(S(a_1)a_2S(a_3)) && (W5)(a) \\
&= \epsilon(\epsilon_s(a_1)S(a_2)) && (W5)(b) \\
&= \epsilon(a_1S(a_2)) && 1.4.5(v) \\
&= \epsilon(1_H\epsilon_t(a)) && (W5)(c) \\
&= \epsilon(a), && 1.4.5(ii)
\end{aligned}$$

de onde vale (iv). Logo S é um anti-morfismo de coálgebras. $\square$

O último resultado dessa seção caracteriza quando uma álgebra de Hopf fraca é uma álgebra de Hopf, no sentido da Definição 1.4.1. Nas referências citadas, este resultado é enunciado como uma equivalência de seis itens, incluindo o item $H_t = H_s = im(u\epsilon)$.

Quando k é um corpo, a hipótese adicional sobre u que aparece na proposição a seguir é automaticamente satisfeita, e neste caso mostra-se que, se $H_t = H_s = k1_H$, como $\Delta(1_H) \in H_s \otimes H_t$ e $\Delta(1_H) = \Delta(1_H)^2$, deve valer

$$\Delta(1_H) = \alpha(1_H \otimes 1_H) = \alpha^2(1_H \otimes 1_H) \quad \therefore \quad \alpha = \alpha^2,$$

de onde $\alpha \in \{0, 1_k\}$ e portanto $\alpha = 1_k$. Logo $H_t = H_s = k1_H$ implica $\Delta(1_H) = 1_H \otimes 1_H$.

No contexto de uma WHA sobre um anel comutativo, não vale em geral que $\alpha = \alpha^2$ implica $\alpha \in \{0, 1_k\}$, portanto o último item da equivalência foi retirado, sendo substituído por uma demonstração direta de $S * id_H = u\epsilon = id_H * S$ implicar $\Delta(1_H) = 1_H \otimes 1_H$.

Proposição 1.4.11. *Seja H uma álgebra de Hopf fraca. São equivalentes:*

(i) $\Delta(1_H) = 1_H \otimes 1_H$*;*

(ii) $\epsilon(ab) = \epsilon(a)\epsilon(b)$*;*

(iii) $S * id_H = u \circ \epsilon$*;*

(iv) $id_H * S = u \circ \epsilon$*.*

Se u for injetiva, então H é uma álgebra de Hopf se, e somente se, vale (i)-(iv).

Demonstração. Se $1_1 \otimes 1_2 = \Delta(1) = 1_H \otimes 1_H$, então

$$\begin{aligned}
\epsilon(ab) &= \epsilon(a1b) \\
&= \epsilon(a1_1)\epsilon(1_2b) && (W4) \\
&= \epsilon(a1_H)\epsilon(1_Hb) \\
&= \epsilon(a)\epsilon(b),
\end{aligned}$$

logo (i) implica (ii). Se ϵ é multiplicativa,

$$\begin{aligned}
(S * id_H)(a) &= 1_1\epsilon(a1_2) && (W5)(b) \\
&= 1_1\epsilon(a)\epsilon(1_2) && (ii) \\
&= 1_1\epsilon(1_2)\epsilon(a) && (im(u) \subseteq Z(H)) \\
&= 1_H\epsilon(a) && (id * u\epsilon = id) \\
&= (u \circ \epsilon)(a),
\end{aligned}$$

portanto (ii) implica (iii). Se $S * id_H = u \circ \epsilon$, temos

$$\begin{aligned}
(id_H * S)(a) &= \epsilon(1_1a)1_2 && (W5)(c) \\
&= (S * id_H))(1_1a)1_2 && (iii) \\
&= S(1_1a_1)1_2a_21_3 \\
&= S(a_1)S(1_1)1_2a_21_3 && 1.4.10(i) \\
&= S(a_1)\epsilon(1_1)a_21_2 && (iii) \\
&= S(a_1)a_2\epsilon(1_1)1_2 && (im(u) \subseteq Z(H)) \\
&= \epsilon(a)1_H && (u\epsilon * id = id, (iii)) \\
&= (u \circ \epsilon)(a),
\end{aligned}$$

de onde (iii) implica (iv). Analogamente, utilizando (W5)(b), a Proposição 1.4.10(i) e $id * u\epsilon = id$, mostra-se que (iv) implica (iii). Supondo $S * id_H = u \circ \epsilon = id_H * S$, então

$$u(\epsilon(1_H)) = \epsilon_t(1_H) = 1_H, \qquad (iv), 1.4.8$$

com isso, obtemos

$$\begin{aligned}
\Delta(1_H) &= 1_1 \otimes 1_2 \\
&= \epsilon_s(1_1) \otimes 1_2 && 1.4.6(ii) \\
&= (\epsilon_s \otimes id_H)(1_1 \otimes 1_2) \\
&= (\epsilon_s \otimes id_H)(1_1 \otimes \epsilon_t(1_2)) && 1.4.6(i) \\
&= \epsilon_s(1_1) \otimes \epsilon_t(1_2) \\
&= \epsilon(1_1)1_H \otimes \epsilon(1_2)1_H && (iii), (iv) \\
&= \epsilon(1_1\epsilon(1_2))1_H \otimes 1_H && (im(\epsilon) \subseteq k) \\
&= \epsilon(1_H)1_H \otimes 1_H && (id * u\epsilon = id)
\end{aligned}$$

$$= 1_H \otimes 1_H, \qquad\qquad (u\epsilon(1_H) = 1_H)$$

ou seja, (iii) com (iv) implicam (i).

Por fim, se H é uma WHA com u injetiva e valem (i)-(iv), então $u(\epsilon(1_H)) = 1_H = u(1_k)$, portanto $\epsilon(1_H) = 1_k$ e H é uma álgebra de Hopf - o axioma (W3) com (i) diz que Δ é morfismo de álgebras e (ii) com $\epsilon(1_H) = 1_k$ diz que ϵ é morfismo de álgebras, logo vale (W3), e (iii)-(iv) são (H4) - enquanto que, se H é uma álgebra de Hopf, pela Definição 1.4.1 valem (i)-(iv). □

Observamos que, no contexto de álgebras de Hopf fracas sobre anéis comutativos, a hipótese sobre a injetividade de u é essencial para concluirmos que (i)-(uv) implicam H ser uma álgebra de Hopf. De fato, considerando a estrutura de $\mathbb{Z}_6$-álgebra em $\mathbb{Z}_2$ definida por $u(1_{\mathbb{Z}_6}) = 1_{\mathbb{Z}_2}$, a estrutura de coálgebra dada por $\Delta(1_{\mathbb{Z}_2}) = 1_{\mathbb{Z}_2} \otimes 1_{\mathbb{Z}_2}$ e $\epsilon(1_{\mathbb{Z}_2}) = 3_{\mathbb{Z}_6}$ e a antípoda $S(1_{\mathbb{Z}_2}) = 1_{\mathbb{Z}_2}$, então $(\mathbb{Z}_2, \mu, u, \Delta, \epsilon, S)$ é uma álgebra de Hopf fraca sobre $\mathbb{Z}_6$ satisfazendo (i)-(iv). Mas $\mathbb{Z}_2$ não é uma álgebra de Hopf sobre $\mathbb{Z}_6$, pois ϵ não é unitário. Nesse caso $ker(u) = \{0, 2, 4\} \neq 0$, ou seja, u não é injetora.

No próximo capítulo utilizaremos a Proposição 1.4.11 para motivar a generalização das definições de elemento group-like e elemento primitivo para o contexto de álgebras de Hopf fracas.

Capítulo 2

Extensões de Hopf-Ore primitivas fracas

Neste capítulo vamos falar brevemente sobre o Teorema de Panov em álgebras de Hopf, definir e apresentar os resultados necessários sobre elementos group-like fracos, elementos primitivos fracos e caracteres fracos em álgebras de Hopf fracas. Ao final, apresentaremos a demonstração da generalização do Teorema de Panov para álgebras de Hopf fracas e a caracterização das extensões de Hopf-Ore primitivas fracas para as álgebras de Hopf fracas de Kaplansky e de Hayashi.

2.1 Teorema de Panov para álgebras de Hopf

Nesta seção vamos falar sobre a caracterização das extensões de Hopf-Ore, publicada por Panov em [20], apresentando a noção de elementos group-like, elementos primitivos e caracteres em álgebras de Hopf. Para esta seção, $(H, \mu, u, \Delta, \epsilon, S)$ denotará uma álgebra de Hopf sobre um anel comutativo k.

Apesar dos resultados desta seção serem casos particulares dos resultados que serão apresentados no restante do capítulo, mostraremos algumas construções e propriedades, para fim de motivação e comparação com as generalizações para o contexto de álgebras de Hopf fracas.

Na Seção 1.3, vimos que, dado um anel A, é possível obter uma extensão (R, i) de A de forma que i seja injetiva, $R \simeq \bigoplus_{n\in\mathbb{N}} AX^n$ e $\deg(pq) \leq \deg(p) + \deg(q)$, para todo $p, q \in R$, se, e somente se, $R = A[X; \sigma, \delta]$, onde $\sigma\colon A \to A$ é um endomorfismo de anéis unitários e $\delta\colon A \to A$ é uma σ-derivação.

No contexto do artigo de Panov, estamos interessados em saber quando uma extensão de Ore $H[X; \sigma, \delta]$ possui uma estrutura de álgebra de Hopf sobre k, estendendo a estrutura de H. Em vista da Definição 1.4.1 e da Propriedade Universal das Extensões de Ore, é suficiente determinar a imagem de X para estender os morfismos Δ, ϵ e S.

Definição 2.1.1. Sejam H e $R = H[X; \sigma, \delta]$ álgebras de Hopf sobre k. Dizemos que R é uma **extensão de Hopf-Ore (primitiva)** de H se $\Delta(X) = g \otimes X + X \otimes h$, onde $g, h \in H$, e H é uma subálgebra de Hopf de R.

Se R é uma extensão de Hopf-Ore de H, vale o axioma da coassociatividade em R, de onde devem valer as igualdades

$$\begin{array}{c}(\Delta \otimes id_R)\Delta(X) = g_1 \otimes g_2 \otimes X + g \otimes X \otimes h + X \otimes h \otimes h \\ \parallel \\ (id_R \otimes \Delta)\Delta(X) = g \otimes g \otimes X + g \otimes X \otimes h + X \otimes h_1 \otimes h_2.\end{array}$$

Como R é um H-módulo à esquerda com base $\{X^n \colon n \in \mathbb{N}\}$, utilizando a Proposição 1.2.6, obtemos que $R \otimes R \otimes R$ é um $(H \otimes H \otimes H)$-módulo à esquerda livre, portanto

$$\Delta(g) \otimes 1_H = g_1 \otimes g_2 \otimes 1_H = g \otimes g \otimes 1_H.$$

Aplicando $id_H \otimes \mu$ na igualdade acima, segue que $\Delta(g) = g \otimes g$. Analogamente, mostra-se que $\Delta(h) = h \otimes h$. Se fosse $g = 0$, então, pelo axioma da counidade em R, teríamos

$$X = (u\epsilon \otimes id_R)\Delta(X) = \epsilon(X)h \in H,$$

o que contradiz R ser um H-módulo à esquerda livre com base $\{X^n \colon n \in \mathbb{N}\}$. Portanto $g \neq 0$. Pelo axioma da counidade em H, vale $g = (u\epsilon \otimes id_H)\Delta(g) = u\epsilon(g)g$. No contexto de álgebras de Hopf sobre um corpo k, esta identidade implica em $u(1_k - \epsilon(g))g = 0$. Como $g \neq 0$ e u é injetiva, resta que $\epsilon(g) = 1_k$ e, portanto, $u\epsilon(g) = 1_H$. De forma análoga, mostra-se que $h \neq 0$ e, sendo k um corpo, valem $\epsilon(h) = 1_k$ e $u\epsilon(h) = 1_H$.

Definição 2.1.2. Seja H uma álgebra de Hopf sobre um anel comutativo k. Um elemento $g \in H$ é chamado **group-like** se $\Delta(g) = g \otimes g$ e $\epsilon(g) = 1_k$. O conjunto dos elementos group-like de H será denotado por $G(H)$.

Como consequência da condição $\epsilon(g) = 1_k$, temos $g \neq 0$ e, utilizando os axioma da antípoda, obtemos

$$gS(g) = (id_H * S)(g) = u\epsilon(g) = 1_H \quad \text{e} \quad S(g)g = (S * id_H)(g) = u\epsilon(g) = 1_H,$$

de onde todo elemento group-like é inversível, com $g^{-1} = S(g)$. Mais ainda, como Δ e ϵ são morfismos de anéis, dados $g, h \in G(H)$, temos

$$\Delta(gh) = \Delta(g)\Delta(h) = (g \otimes g)(h \otimes h) = gh \otimes gh \quad \text{e} \quad \epsilon(gh) = \epsilon(g)\epsilon(h) = 1_k,$$

e como S é um anti-morfismo de coálgebras, vale $\Delta(S(g)) = (S \otimes S)\tau\Delta(g) = S(g) \otimes S(g)$. Ou seja, $g, h \in G(H)$ implica em $gh, g^{-1} \in G(H)$, logo $G(H)$ é um grupo.

Definição 2.1.3. Seja H uma álgebra de Hopf sobre um anel comutativo k. Um elemento $X \in H$ é chamado (g, h)-**primitivo** se $\Delta(X) = g \otimes X + X \otimes h$, com $g, h \in G(H)$.

Seja $X \in H$ um elemento (g, h)-primitivo. Pelo axioma da counidade, temos

$$X = (u\epsilon \otimes id_H)\Delta(X) = X + u\epsilon(X)h \quad \therefore \quad u\epsilon(X)h = 0.$$

Como h é um elemento group-like, portanto inversível, obtemos $u\epsilon(X) = 0$. Nesse caso,

$$0 = u\epsilon(X) = (S * id_H)(X) = S(g)X + S(X)h \quad \therefore \quad S(X) = -S(g)XS(h).$$

Como última observação antes de apresentar o Teorema de Panov, a fim de caracterizar as extensões de Hopf-Ore geradas por um elemento (g, h)-primitivo, é suficiente considerar as extensões geradas por um elemento $(g, 1)$-primitivo.

Proposição 2.1.4. *Seja $R = H[X; \sigma, \delta]$ uma extensão de Hopf-Ore onde X é um elemento (g, h)-primitivo. Então existem um elemento $(r, 1)$-primitivo $Y \in R$ e nirfusnis $\sigma', \delta' \colon H \to H$, tais que $R = H[Y; \sigma', \delta']$.*

Demonstração. Defina $Y = XS(h) \in R$. Então, como Δ é um morfismo de álgebras, obtemos

$$\begin{aligned}\Delta(Y) &= \Delta(X)\Delta(S(h)) \\ &= (g \otimes X + X \otimes h)(S(h) \otimes S(h)) \\ &= gS(h) \otimes XS(h) + XS(h) \otimes hS(h) \\ &= gh^{-1} \otimes Y + Y \otimes 1.\end{aligned}$$

Portanto, tomando $r = gh^{-1} \in G(H)$, segue que Y é um elemento $(r, 1)$-primitivo. Como $R = H[X; \sigma, \delta]$, para todo $a \in H$, vale

$$Ya = XS(h)a = \sigma(S(h)a)X + \delta(S(h)a).$$

Por outro lado, se $\sigma', \delta' \colon H \to H$ são morfismos tais que $Ya = \sigma'(a)Y + \delta'(a)$, então

$$Ya = \sigma'(a)Y + \delta'(a) = \sigma'(a)XS(h) + \delta'(a) = \sigma'(a)\sigma(S(h))X + \sigma'(a)\delta(S(h)) + \delta'(a).$$

Igualando as duas escritas de Ya e utilizando que R é uma H-módulo à esquerda livre de base $\{X^n \colon n \in \mathbb{N}\}$, obtemos

$$\sigma'(a)\sigma(S(h)) = \sigma(S(h)a) \quad \text{e} \quad \delta'(a) + \sigma'(a)\delta(S(h)) = \delta(S(h)a).$$

Como σ é morfismo de anéis e $S(h) = h^{-1}$, as igualdades acima equivalem a

$$\sigma'(a) = \sigma(S(h)ah) \quad \text{e} \quad \delta'(a) = \delta(S(h)a) - \sigma(S(h)ah)\delta(S(h)).$$

As funções σ' e δ' definidas pelas expressões acima são, respectivamente, um morfismo de anéis unitários e uma σ'-derivação. Para ver que $R = H[Y; \sigma', \delta']$, vamos utilizar a Propriedade Universal das Extensões de Ore. Considere $j \colon H \to H[Y; \sigma', \delta']$ o morfismo inclusão, $j(a) = a$, para todo $a \in H$, e $x = Yh = XS(h)h = X \in H[Y; \sigma', \delta']$. Então

$$\begin{aligned}xj(a) &= Yha \\ &= \sigma'(ha)Y + \delta'(ha) \\ &= \sigma(S(h)hah)Y + \delta(S(h)ha) - \sigma(S(h)hah)\delta(S(h)) \\ &= \sigma(ah)Y + \delta(a) - \sigma(ah)\delta(S(h)) \\ &= \sigma(ah)(Y - \delta(S(h))) + \delta(a).\end{aligned}$$

Por outro lado, como $\delta(1) = 0$, temos

$$\begin{aligned}j(\sigma(a))x + j(\delta(a)) &= \sigma(a)Yh + \delta(a) \\ &= \sigma(a)(\sigma'(h)Y + \delta'(h)) + \delta(a) \\ &= \sigma(a)(\sigma(S(h)hh)Y + \delta(S(h)h) - \sigma(S(h)hh)\delta(S(h))) + \delta(a) \\ &= \sigma(a)(\sigma(h)Y + \delta(1_H) - \sigma(h)\delta(S(h))) + \delta(a) \\ &= \sigma(a)\sigma(h)(Y - \delta(S(h))) + \delta(a),\end{aligned}$$

de onde $xj(a) = j(\sigma(a))x + j(\delta(a))$. Logo, existe um morfismo de anéis $j' \colon R \to H[Y; \sigma', \delta']$ tal que $j'(a) = a$, para todo $a \in H$, e $j'(X) = Yh = X$. Desta forma, j' é uma inclusão - portanto injetora - e $j'(a_n(XS(h))^n) = a_n(XS(h))^n = a_nY^n$, para todo $n \in \mathbb{N}$, de onde j' é sobrejetora. Isso mostra que $R = H[Y; \sigma', \delta']$. $\square$

Com isso, a caracterização das extensões de Hopf-Ore, a menos de uma mudança de parâmetros explicitamente determinada, fica completa a partir da caracterização das extensões geradas por elementos $(g,1)$-primitivos. Por fim, um morfismo de álgebras $\chi\colon H \to k$ é chamado **caracter** de H.

Teorema 2.1.5 (Teorema de Panov). *$R = H[X;\sigma,\delta]$ é uma extensão de Hopf-Ore onde X um elemento $(r,1)$-primitivo se, e somente se, existe um caracter χ de H tal que, para todo $a \in H$, valem*

(i) $\sigma(a) = \chi(a_1)a_2 = ra_1S(r)\chi(a_2)$;

(ii) $\Delta(\delta(a)) = \delta(a_1) \otimes a_2 + ra_1 \otimes \delta(a_2)$.

Pode-se mostrar que, se R é uma extensão de Hopf-Ore de H, nas condições do Teorema de Panov, então devem valer as identidades

$$rS(a)S(r) = \sigma(S(\sigma(a))) \quad \text{e} \quad S(\delta(a)) = S(r)\delta(S(\sigma(a)). \tag{iii}$$

Reciprocamente, para que a antípoda $S \in End_k(H)$ admita uma extensão $S \in End_k(R)$, a qual é obtida pela Propriedade Universal das Extensões de Ore considerando o morfismo de álgebras $S\colon H \to H^{op}$, as identidades em (iii) são necessárias. Mas, neste caso, (iii) pode ser obtidos de (i) e (ii). Assim, as condições em (iii) são necessárias e suficientes para o Toerema de Panov, mas sua menção é redundante.

O Teorema de Panov, bem como outros resultado de [20] envolvendo a classificação de extensões de Hopf-Ore de álgebras de Hopf cocomutativas (quando $\Delta = \tau \circ \Delta$), são obtidos como corolários de resultados formulados no contexto de álgebras de Hopf fracas em [16], os quais serão apresentados ao decorrer do texto.

2.2 Elementos group-like fracos e primitivos fracos

Nesta seção vamos motivar a generalização das noções de elemento group-like e primitivo, utilizadas no Teorema de Panov, e as propriedades necessárias para a demonstração do resultado central deste texto. As referências para esta seção são [8] e [16]. Para o restante deste capítulo, $(H,\mu,u,\Delta,\epsilon,S)$ denotará uma álgebra de Hopf fraca sobre um anel comutativo k.

Seguindo a ideia em [20], estamos interessados em munir uma extensão de Ore $R = H[X;\sigma,\delta]$ com uma estrutura de álgebra de Hopf fraca, contendo H como subálgebra de Hopf fraca, e de modo que X seja um elemento $(g,1)$-primitivo. Em particular, a comultiplicação $\Delta\colon R \to R \otimes R$ deve ser um morfismo multiplicativo, de onde

$$g \otimes X + X \otimes 1 = \Delta(X) = \Delta(1)\Delta(X) = \Delta(1)(g \otimes X) + \Delta(1)(X \otimes 1).$$

Como R é um H-módulo à esquerda livre de base $\{X^n\colon n \in \mathbb{N}\}$, aplicando a Proposição 1.2.6 e comparando os coeficientes de $X \otimes 1$, obtemos $\Delta(1) = 1 \otimes 1$. Pela Proposição 1.4.11, se u for injetiva, então H deverá ser uma álgebra de Hopf. Portanto a noção de elemento primitivo, definida em álgebras de Hopf, é muito restritiva para o contexto de álgebras de Hopf fracas.

Lema 2.2.1. *Sejam $R = H[X;\sigma,\delta]$, $g_1, g_2 \in H$ e $\Delta\colon R \to R \otimes R$ um morfismo multiplicativo satisfazendo $\Delta(X) = \Delta(1)(g_1 \otimes X + X \otimes g_2) = (g_1 \otimes X + X \otimes g_2)\Delta(1)$ e $\Delta|_H = \Delta_H$. Então Δ satisfaz o axioma da coassociatividade se, e somente se, valem $\Delta(g_i) = \Delta(1)(g_i \otimes g_i) = (g_i \otimes g_i)\Delta(1)$, $i = 1,2$.*

Demonstração. Utilizando que $\Delta(X) = \Delta(1)(g_1 \otimes X + X \otimes g_2)$, para que o morfismo Δ seja coassociativo, devem ser iguais

$$\begin{aligned}
(\Delta \otimes id_R)\Delta(X) &= \Delta(1_1 g_1) \otimes 1_2 X + \Delta(1_1 X) \otimes 1_2 g_2 \\
&= \Delta(1_1)\Delta(g_1) \otimes 1_2 X + \Delta(1_1)\Delta(X) \otimes 1_2 g_2 && (\Delta \text{ mult.}) \\
&= (1_1 \otimes 1_2 \otimes 1_3)(\Delta(g_1) \otimes X + g_1 \otimes X \otimes g_2 + X \otimes g_2 \otimes g_2) \\
&= \Delta_2(1)(\Delta(g_1) \otimes X + g_1 \otimes X \otimes g_2 + X \otimes g_2 \otimes g_2),
\end{aligned}$$

e

$$\begin{aligned}
(id_R \otimes \Delta)\Delta(X) &= 1_1 g_1 \otimes \Delta(1_2 X) + 1_1 X \otimes \Delta(1_2 g_2) \\
&= 1_1 g_1 \otimes \Delta(1_2)\Delta(X) + 1_1 X \otimes \Delta(1_2)\Delta(g_2) && (\Delta \text{ mult.}) \\
&= (1_1 \otimes 1_2 \otimes 1_3)(g_1 \otimes g_1 \otimes X + g_1 \otimes X \otimes g_2 + X \otimes \Delta(g_2)) \\
&= \Delta_2(1)(g_1 \otimes g_1 \otimes X + g_1 \otimes X \otimes g_2 + X \otimes \Delta(g_2)).
\end{aligned}$$

Pela Proposição 1.2.6, podemos comparar os coeficientes de $1 \otimes 1 \otimes X$ e $X \otimes 1 \otimes 1$, obtendo que, se Δ é coassociativa, então

$$\Delta_2(1_H)(\Delta(g_1) \otimes 1_H) = \Delta_2(1_H)(g_1 \otimes g_1 \otimes 1_H), \tag{i}$$
$$\Delta_2(1_H)(1_H \otimes \Delta(g_2)) = \Delta_2(1_H)(1_H \otimes g_2 \otimes g_2). \tag{ii}$$

Aplicando $id_{H\otimes H} \otimes \epsilon$ - e o isomorfismo $H \otimes k \simeq H$ - à primeira igualdade, obtemos

$$\begin{aligned}
& (1_1 \otimes 1_2)\Delta(g_1) u\epsilon(1_3) = 1_1 g_1 \otimes 1_2 g_1 u\epsilon(1_3) \\
\Longleftrightarrow \quad & (1_1 \otimes 1_2 \epsilon(1_3))\Delta(g_1) = 1_1 g_1 \otimes 1_2 \epsilon(1_3) g_1 && (im(u) \subseteq Z(H), im(\epsilon) \subseteq k) \\
\Longleftrightarrow \quad & \Delta(g_1) = \Delta(1)\Delta(g_1) = \Delta(1)(g_1 \otimes g_1). && (id * u\epsilon = id)
\end{aligned}$$

De forma análoga, aplicando $\epsilon \otimes id_{H\otimes H}$ em (ii), obtemos $\Delta(g_2) = \Delta(1)(g_2 \otimes g_2)$. Repetindo o argumento acima para $\Delta(X) = (g_1 \otimes X + X \otimes g_2)\Delta(1)$, mostra-se que, se Δ é coassociativa, então $\Delta(g_i) = (g_i \otimes g_i)\Delta(1)$, $i = 1, 2$.

Reciprocamente, se $\Delta(g_i) = \Delta(1)(g_i \otimes g_i) = (g_i \otimes g_i)\Delta(1)$, $i = 1, 2$, então

$$\begin{aligned}
\Delta_2(1)(1 \otimes \Delta(g_i)) &= (1_1 \otimes \Delta(1_2))(1 \otimes 1'_1 g_i \otimes 1'_2 g_i) \\
&= (1_1 \otimes \Delta(1_2))(1 \otimes \Delta(1))(1 \otimes g_i \otimes g_i) \\
&= (1_1 \otimes \Delta(1_2)\Delta(1))(1 \otimes g_i \otimes g_i) \\
&= (1_1 \otimes \Delta(1_2))(1 \otimes g_i \otimes g_i) && (\Delta \text{ mult.}) \\
&= \Delta_2(1)(1 \otimes g_i \otimes g_i),
\end{aligned}$$

e

$$\begin{aligned}
\Delta_2(1)(\Delta(g_i) \otimes 1) &= (\Delta(1_1) \otimes 1_2)(1'_1 g_i \otimes 1'_2 g_i \otimes 1) \\
&= (\Delta(1_1) \otimes 1_2)(\Delta(1) \otimes 1)(g_i \otimes g_i \otimes 1) \\
&= (\Delta(1_1)\Delta(1) \otimes 1_2)(g_i \otimes g_i \otimes 1) \\
&= (\Delta(1_1) \otimes 1_2)(g_i \otimes g_i \otimes 1) && (\Delta \text{ mult.}) \\
&= \Delta_2(1)(g_i \otimes g_i \otimes 1).
\end{aligned}$$

Portanto valem (i) e (ii). Logo Δ é coassociativa. $\square$

Em vista do lema acima, temos a seguinte definição.

Definição 2.2.2. Seja H uma álgebra de Hopf fraca sobre um anel comutativo k. Então:

(i) Um elemento $g \in H$ é chamado **group-like fraco** se

$$\Delta(g) = \Delta(1)(g \otimes g) = (g \otimes g)\Delta(1).$$

O conjunto dos elementos group-like fracos de H é denotado $G_w(H)$.

(ii) Para $g, h \in H$, um elemento $X \in H$ é chamado (g, h)**-primitivo fraco** se

$$\Delta(X) = \Delta(1)(g \otimes X + X \otimes h) = (g \otimes X + X \otimes h)\Delta(1).$$

Algumas observações sobre a definição de elemento group-like fraco: se um elemento $g \in H$ é group-like - no sentido de $\Delta(g) = g \otimes g$ - então ele é group-like fraco, pois Δ é multiplicativa, de onde

$$\Delta(1)(g \otimes g) = \Delta(1)\Delta(g) = \Delta(g) = \Delta(g)\Delta(1) = (g \otimes g)\Delta(1).$$

Assim, a noção de elemento group-like fraco é uma generalização da noção de elemento group-like, e da mesma forma para os elementos primitivos. A unidade 1_H é um elemento group-like se, e somente se, $\Delta(1_H) = 1_H \otimes 1_H$. Neste caso, se u for injetiva, então H deve ser uma álgebra de Hopf. Por outro lado, como $1_{H\otimes H} = 1_H \otimes 1_H$, a unidade 1_H é sempre um elemento group-like fraco. Apesar da definição de elemento (g, h)-primitivo fraco pedir apenas $g, h \in H$, o lema anterior mostra que, se existe um elemento (g, h)-primitivo fraco, então g e h devem ser elementos group-like fracos.

Na Seção 2.1, a definição de elemento group-like pede que $u\epsilon(g) = 1_H$, de forma que, no contexto de álgebras de Hopf, os elementos group-like são inversíveis. No contexto de álgebras de Hopf fraca, um elemento é chamado group-like se satisfaz as identidades de elementos group-like fracos e possui alguma propriedade de inversibilidade - por exemplo, em [4, Definition 4.11] é exigido que $S(g)g = 1$ - enquanto que, na álgebra de matrizes $M_n(k)$ com a estrutura do exemplo 1.4.4(2), as matrizes elementares e_{ij}, $i, j = 1, \ldots, n$, são elementos group-like fracos satisfazendo $u\epsilon(e_{ij}) = 1$, mas não são inversíveis.

Exemplo 2.2.3. Sejam H uma álgebra de Hopf e $H' = ke \oplus H$ a álgebra de Hopf fraca de Kaplansky, com operações definidas por

$$\begin{aligned} u(r) &= re, & (re + a)(se + b) &= rse + (rb + sa + ab), \\ \epsilon(re + a) &= 2r + \epsilon_H(a), & \Delta(re + a) &= r(1_H \otimes 1_H + f \otimes f) + \Delta_H(a), \end{aligned}$$

onde $f = e - 1_H$, e antípoda definida por $S(re + a) = re + S_H(a)$. Vamos mostrar que

$$G_w(H') = \{rf + a \colon r^2 = r, a \in G_w(H)\}.$$

Vamos mostrar que $re + a \in G_w(H')$ se, e somente se, $r^2 = r \in k$ e $a \in H$ satisfaz

$$\Delta_H(a) = a \otimes a + r(a \otimes 1_H + 1_H \otimes a). \qquad (*)$$

Em seguida, mostraremos que $a \in H$ satisfaz $(*)$ se, e somente se, $a + r1_H = b \in G_w(H)$. Assim, os elementos de $G_w(H')$ serão da forma $re + a = re + (b - r1_H) = rf + b$.

Como $\Delta(e)$ é um elemento central em $H' \otimes H'$, é suficiente considerar os elementos $x \in H'$ tais que $\Delta(x) = \Delta(e)(x \otimes x)$. Se $re + a \in G_w(H')$, então

$$\begin{aligned}
\Delta(re+a) &= \Delta(e)([re+a] \otimes [re+a]) \\
&= (1_H \otimes 1_H + f \otimes f)(r^2 e \otimes e + re \otimes a + ra \otimes e + a \otimes a) \\
&= r^2 1_H \otimes 1_H + r1_H \otimes a + ra \otimes 1_H + a \otimes a + r^2 f \otimes f \qquad (fH = Hf = 0) \\
&= r^2 \Delta(e) + r(a \otimes 1_H + 1_H \otimes a) + a \otimes a.
\end{aligned}$$

Pelo axioma da counidade, segue que $re + a = r^2 e + r(\epsilon_H(a)1_H + a) + \epsilon_H(a)a$, ou ainda,

$$(r^2 - r)e + [r\epsilon_H(a)1_H + \epsilon_H(a)a + (r - 1_H)a] = 0.$$

Como o termo entre colchetes pertence a H e $H' = ke \oplus H$, deve ser $r^2 - r = 0$. Logo

$$\begin{aligned}
r\Delta(e) + \Delta_H(a) &= \Delta(re+a) \\
&= r^2\Delta(e) + r(a \otimes 1_H + 1_H \otimes a) + a \otimes a \\
&= r\Delta(e) + r(a \otimes 1_H + 1_H \otimes a) + a \otimes a.
\end{aligned}$$

Subtraíndo $r\Delta(e)$ da igualdade acima, obtemos que a satisfaz $(*)$. Reciprocamente, suponha que $r^2 = r$ e $a \in H$ satisfaz $(*)$, então

$$\begin{aligned}
\Delta(e)([re+a] \otimes [re+a]) &= \Delta(e)(r^2 e \otimes e + r(a \otimes e + e \otimes a) + a \otimes a) \\
&= r^2\Delta(e) + r(a \otimes 1_H + 1_H \otimes a) + a \otimes a \\
&= r\Delta(e) + \Delta_H(a) \\
&= \Delta(re+a).
\end{aligned}$$

Portanto $re + a \in G_w(H')$. Agora, suponha que $a \in G_w(H)$ e $r^2 = r$, então

$$\begin{aligned}
&(a - r1_H) \otimes (a - r1_H) + r[(a - r1_H) \otimes 1_H + 1_H \otimes (a - r1_H)] \\
&= [a \otimes a - a \otimes r1_H - r1_H \otimes a + r1_H \otimes r1_H] \\
&\quad + r[a \otimes 1_H - r1_H \otimes 1_H] + r[1_H \otimes a - 1_H \otimes r1_H] \\
&= [a \otimes a - ra \otimes 1_H - r1_H \otimes a + r^2 1_H \otimes 1_H] \\
&\quad + [ra \otimes 1_H - r^2 1_H \otimes 1_H] + [r1_H \otimes a - r^2 1_H \otimes 1_H] \\
&= a \otimes a - r^2 1_H \otimes 1_H \\
&= \Delta_H(a - r1_H),
\end{aligned}$$

de onde $a - r1_H$ satisfaz $(*)$. Por outro lado, se $a \in H$ satisfaz $(*)$, então

$$\begin{aligned}
(a + r1_H) \otimes (a + r1_H) &= a \otimes a + a \otimes r1_H + r1_H \otimes a + r1_H \otimes r1_H \\
&= a \otimes a + ra \otimes 1_H + r1_H \otimes a + r^2 1_H \otimes 1_H \\
&= a \otimes a + r[a \otimes 1_H + 1_H \otimes a] + r1_H \otimes 1_H \\
&= \Delta_H(a + r1_H),
\end{aligned}$$

de onde $a + r1_H \in G_w(H)$, ou ainda, deve valer $a = b - r1_H$, para algum $b \in G_w(H)$.

Exemplo 2.2.4. Sejam $n \geq 1$ e $H = \bigoplus_{i,j=1}^{n} ke_{ij}$ a álgebra de Hopf fraca de Hayashi, com morfismos definidos por

$$\mu(e_{ij} \otimes e_{rs}) = [i = r, j = s]e_{ij}, \quad u(1_k) = \sum_{i,j=1}^{n} e_{ij},$$

$$\epsilon(e_{ij}) = [i = j], \quad \Delta(e_{ij}) = \sum_{p=1}^{n} e_{ip} \otimes e_{pj} \quad \text{e} \quad S(e_{ij}) = e_{ji}.$$

Vamos mostrar que $x = \sum_{i,j=1}^{n} a_{ij}e_{ij} \in H$ é um elemento group-like fraco se, e somente se, existe um idempotente $e \in k$ e elementos $\lambda_1, \ldots, \lambda_n \in \mathcal{U}(ke)$ tais que $a_{ij} = \lambda_i \lambda_j^*$, onde λ_j^* denota o inverso de λ_j no anel unitário ke.

Como H é comutativa, $\Delta(1_H)(x \otimes x) = (x \otimes x)\Delta(1_H)$, para todo $x \in H$. Denotando $x = \sum_{i,j=1}^{n} a_{ij}e_{ij}$, temos

$$\Delta(1_H)(x \otimes x) = \left(\sum_{u,v,p=1}^{n} e_{up} \otimes e_{pv}\right)\left(\sum_{i,j,r,s=1}^{n} a_{is}a_{rj}[e_{is} \otimes e_{rj}]\right) = \sum_{i,j,p=1}^{n} a_{ip}a_{pj}[e_{ip} \otimes e_{pj}].$$

Enquanto que $\Delta(x) = \sum_{i,j,p=1}^{n} a_{ij}[e_{ip} \otimes e_{pj}]$. Assim, $x \in G_w(H)$ se, e somente se,

$$a_{ip}a_{pj} = a_{ij}, \quad \forall i, j, p = 1, \ldots, n.$$

Em particular, tomando $p = 1$ e $j = i$, temos $a_{ii} = a_{i1}a_{1i} = a_{1i}a_{i1} = a_{11}$ e $a_{11} = a_{11}^2$. Seja $e := a_{11} \in k$, então e é um idempotente e, tomando $p = j = i$, vale

$$a_{ij} = a_{ij}a_{jj} = a_{ij}a_{11} = a_{ij}e \in ke, \quad \forall i, j = 1, \ldots, n.$$

Note que ke é um ideal bilateral unitário de k, assim, ke é um anel com unidade $1_{ke} = e$. De $e = a_{ii} = a_{i1}a_{1i}$, temos que a_{1i} é um inverso de a_{i1} em ke. Denote $a_{i1} = \lambda_i$ e $a_{1i} = \lambda_i^* \in ke$, então $a_{ij} = \lambda_i\lambda_j^* \in ke$.

Reciprocamente, sejam $e \in k$ um idempotente e $\lambda_1, \ldots, \lambda_n \in \mathcal{U}(ke)$. Denote o inverso de λ_i em ke por λ_i^* e considere $a_{ij} = \lambda_i\lambda_j^*$. Então $x = \sum_{i,j=1}^{n} a_{ij}e_{ij}$ é um elemento group-like fraco de H, pois $a_{ip}a_{pj} = \lambda_i\lambda_p^*\lambda_p\lambda_j^* = \lambda_i e \lambda_j^* = \lambda_i\lambda_j^* = a_{ij}$.

Vamos apresentar algumas propriedades dos elementos group-like fracos.

Lema 2.2.5. *Seja $g \in G_w(H)$. Então:*

(i) g é inversível à direita se, e somente se, $\epsilon_t(g) = 1_H$ se, e somente se, $gS(g) = 1_H$.

(ii) g é inversível à esquerda se, e somente se, $\epsilon_s(g) = 1_H$ se, e somente se, $S(g)g = 1_H$.

Demonstração. Se $g \in G_w(H)$, então $\Delta(g) = 1_1g \otimes 1_2g$. Pelo axioma da counidade, segue que $g = (u\epsilon * id_H)(g) = \epsilon(1_1g)1_2g$. Com isso, se existe $h \in H$ tal que $gh = 1_H$, então

$$\epsilon_t(g) = \epsilon_t(g)gh = \epsilon(1_1g)1_2gh = gh = 1_H.$$

Se $\epsilon_t(g) = 1_H$, então, lembrando que $1_H \in H_t$, e portanto $1_H = \epsilon_t(1_H)$, temos

$$\begin{aligned}
1_H &= \epsilon_t(g) \\
&= (id_H * S)(g) && (W5)(c) \\
&= g1_1S(g1_2) \\
&= g1_1S(1_2)S(g) && 1.4.10(i) \\
&= g\epsilon_t(1_H)S(g) && (W5)(c) \\
&= gS(g).
\end{aligned}$$

Por fim, se $gS(g) = 1_H$, então g é inversível à direita. Isso mostra (i). A demonstração de (ii) é análoga, utilizando $\Delta(g) = g1_1 \otimes g1_2$, (W5)(b) e $1_H = \epsilon_s(1_H)$. □

No contexto de álgebras de Hopf definidas sobre um corpo k, sabemos que $G(H)$, com a multiplicação de H, tem estrutura de grupo. Tendo em vista que elementos group-like fracos não são necessariamente inversíveis, tal propriedade não é mais possível, Ainda assim, podemos garantir que $G_w(H)$ é um conjunto com unidade, fechado para a multiplicação e invariante por S. Pela observação após a Definição 2.2.2, sabemos que $1_H \in G_w(H)$. Agora, dados $g, h \in G_w(H)$, temos

$$\begin{aligned}
\Delta(gh) &= \Delta(g)\Delta(h) && (W3)\\
&= \Big(\Delta(1)(g \otimes g)\Big)\Big(\Delta(1)(h \otimes h)\Big)\\
&= \Delta(1)\Big((g \otimes g)\Delta(1)\Big)(h \otimes h)\\
&= \Delta(1)\Big(\Delta(1)(g \otimes g)\Big)(h \otimes h)\\
&= \Delta(1)(g \otimes g)(h \otimes h) && (W3)\\
&= \Delta(1)(gh \otimes gh).
\end{aligned}$$

Analogamente $\Delta(gh) = (gh \otimes gh)\Delta(1)$, portanto $gh \in G_w(H)$. Como S é um anti-morfismo de álgebras e de coálgebras, obtemos

$$\begin{aligned}
\Delta(S(g)) &= S(g)_1 \otimes S(g)_2\\
&= S(g_2) \otimes S(g_1) && 1.4.10(iii)\\
&= S(1_2 g) \otimes S(1_1 g)\\
&= S(g)S(1_2) \otimes S(g)S(1_1) && 1.4.10(i)\\
&= (S(g) \otimes S(g))(S(1_2) \otimes S(1_1))\\
&= (S(g) \otimes S(g))\Delta(S(1_H)) && 1.4.10(iii)\\
&= (S(g) \otimes S(g))\Delta(1_H).
\end{aligned}$$

Analogamente, utilizando $\Delta(g) = g1_1 \otimes g1_2$, mostra-se que $\Delta(S(g)) = \Delta(1_H)(S(g) \otimes S(g))$. Portanto $S(g) \in G_w(H)$. Em particular, o conjunto dos elementos group-like fracos inversíveis é um grupo com a multiplicação de H.

O próximo resultado não requer a noção de elemento group-like fraco, mas será utilizado com elementos group-like fracos, juntamente do Lema 2.2.5.

Lema 2.2.6. *Seja $g \in H$. Então:*

(i) São equivalentes:

- *(a)* $\epsilon_t(g) = 1_H$*;*
- *(b)* $\epsilon(ag^n) = \epsilon(a), \forall n \in \mathbb{N}, a \in H$*;*
- *(c)* $\epsilon'_s(g) = 1_H$*.*

(ii) São equivalentes:

- *(a)* $\epsilon_s(g) = 1_H$*;*
- *(b)* $\epsilon(g^n a) = \epsilon(a), \forall n \in \mathbb{N}, a \in H$*;*
- *(c)* $\epsilon'_t(g) = 1_H$*.*

Demonstração. Vamos provar (i). A demonstração de (ii) é análoga, utilizando os resultados correspondentes da Seção 1.4. Suponha que vale a propriedade em (b). Então

$$\epsilon_t(g) = \epsilon(1_1 g)1_2 = \epsilon(1_1)1_2 = 1_H \quad \text{e} \quad \epsilon'_s(g) = 1_1\epsilon(1_2 g) = 1_1\epsilon(1_2) = 1_H,$$

ou seja, valem (a) e (c). Suponha (a), vamos provar que vale (b) utilizando indução. Para $n = 0$ o resultado é trivial, enquanto que, para $n = 1$, temos

$$\epsilon(ag) = \epsilon(a1_2)\epsilon(1_1 g) \qquad (W4)$$

$$\begin{aligned} &= \epsilon(a\epsilon(1_1 g)1_2) && (\epsilon \text{ morfismo}) \\ &= \epsilon(a\epsilon_t(g)) \\ &= \epsilon(a). && (\mathit{hip.}) \end{aligned}$$

Supondo que vale (b) para algum $n \geq 1$, então

$$\begin{aligned} \epsilon(ag^{n+1}) &= \epsilon((ag^n)g) \\ &= \epsilon(ag^n) && (n = 1) \\ &= \epsilon(a). && (\mathit{h.i.}) \end{aligned}$$

Portanto (a) implica (b). A demonstração de (c) implica (b) se faz por indução de forma análoga à (a) implica (b), utilizando $\epsilon(ag) = \epsilon(a1_1)\epsilon(1_2 g)$. □

Vamos tratar agora dos elementos primitivos fracos. Na seção anterior mostramos que, no contexto de álgebras de Hopf, se X é um elemento primitivo de H, então $u\epsilon(X) = 0$. Consequentemente, como $u\epsilon$ é multiplicativo, obtemos $u\epsilon(HXH) = 0$ e, se u for injetiva, $\epsilon(HXH) = 0$.

Lema 2.2.7. *Seja $X \in H$. Então:*

(i) $\epsilon(aX) = 0$ para todo $a \in H$ se, e somente se, $\epsilon_t(X) = 0$ se, e somente se, $\epsilon'_s(X) = 0$;

(ii) $\epsilon(Xa) = 0$ para todo $a \in H$ se, e somente se, $\epsilon_s(X) = 0$ se, e somente se, $\epsilon'_t(X) = 0$.

Demonstração. Se $\epsilon(aX) = 0$ para todo $a \in H$, então

$$\epsilon_t(X) = \epsilon(1_1 X)1_2 = 0 \cdot 1_2 = 0 \quad \text{e} \quad \epsilon'_s(X) = 1_1\epsilon(1_2 X) = 1_1 \cdot 0 = 0.$$

Reciprocamente, se $\epsilon_t(X) = 0$, então

$$\begin{aligned} \epsilon(aX) &= \epsilon(a1_2)\epsilon(1_1 X) && (W4) \\ &= \epsilon(a\epsilon(1_1 X)1_2) && (\epsilon \text{ morfismo}) \\ &= \epsilon(a\epsilon_t(X)) \\ &= \epsilon(a \cdot 0) = 0, \end{aligned}$$

enquanto que $\epsilon'_s(X) = 0$ implica

$$\begin{aligned} \epsilon(aX) &= \epsilon(a1_1)\epsilon(1_2 X) && (W4) \\ &= \epsilon(a1_1\epsilon(1_2 X)) && (\epsilon \text{ morfismo}) \\ &= \epsilon(a\epsilon'_s(X)) \\ &= \epsilon(a \cdot 0) = 0. \end{aligned}$$

Isso mostra (i). A demonstração de (ii) é análoga. □

Continuando a comparação com a Seção 2.1, vimos que um elemento (g, h)-primitivo X, em consequência dos axiomas da antípoda e da inversibilidade dos elementos group-like, deve satisfazer $S(X) = -S(g)XS(h)$.

Lema 2.2.8. *Seja $X \in H$ um elemento (g, h)-primitivo fraco. Então:*

(i) Se $\epsilon_s(X) = 0$ e $\epsilon_t(h) = 1_H$, então $S(X) = -S(g)XS(h)$;

(ii) Se $\epsilon_t(X) = 0$ e $\epsilon_s(g) = 1_H$, então $S(X) = -S(g)XS(h)$.

Demonstração. Vamos mostrar (i). Lembrando que $1_H \in H_s$, de onde $1_H = \epsilon_s(1_H)$, temos

$$\begin{aligned}
\epsilon_s(X) &= S(X_1)X_2 && (W5)(b)\\
&= S(1_1 g)1_2 X + S(1_1 X)1_2 h \\
&= S(g)S(1_1)1_2 X + S(X)S(1_1)1_2 h && 1.4.10(i)\\
&= S(g)\epsilon_s(1_H)X + S(X)\epsilon_s(1_H)h && (W5)(b)\\
&= S(g)X + S(X)h.
\end{aligned}$$

Se $\epsilon_s(X) = 0$, então $S(x)h = -S(g)X$. Se $\epsilon_t(h) = 1$, segue do Lema 2.2.5 que $hS(h) = 1_H$, e consequentemente $S(x) = -S(g)XS(h)$. A demonstração de (ii) é análoga, utilizando $\Delta(X) = (g \otimes X + X \otimes h)\Delta(1)$, (W5)(c) e $1_H \in H_t$. □

Para o último resultado desta seção, vamos relacionar a inversibilidade lateral dos elementos g e h com a propriedade de um elemento (g,h)-primitivo fraco ser anulado por ϵ_t ou ϵ_s, o qual será usado em conjunto com o Lema 2.2.7 para a demonstração dos resultados principais deste texto.

Lema 2.2.9. *Seja $X \in H$ um elemento (g,h)-primitivo fraco. Então:*

(i) Se $\epsilon_t(g) = 1_H$ e $\epsilon_t(h) = 1_H$, então $\epsilon_t(X) = 0$;

(ii) Se $\epsilon_s(g) = 1_H$ e $\epsilon_s(h) = 1_H$, então $\epsilon_s(X) = 0$.

Demonstração. Segue do axioma da counidade que

$$X = (u\epsilon * id_H)(X) = \epsilon(1_1 g)1_2 X + \epsilon(1_1 X)1_2 h = \epsilon_t(g)X + \epsilon_t(X)h.$$

Se $\epsilon_t(g) = 1_H$, a igualdade acima equivale a $\epsilon_t(X)h = 0$. Se $\epsilon_t(h) = 1_H$, segue do Lema 2.2.5 que $hS(h) = 1_H$, logo $\epsilon_t(X) = 0$. Isso mostra (i). De maneira análoga, utilizando $id_H * u\epsilon = id_H$, mostra-se que $X = g\epsilon_s(X) + X\epsilon_s(h)$. Portanto $\epsilon_s(g) = 1_H$ e $\epsilon_s(h) = 1_H$ implicam $\epsilon_s(X) = 0$, demonstrando (ii). □

Gostaríamos de observar que, apesar da definição de elemento group-like fraco não exigir qualquer tipo de inversibilidade, os resultados desta seção, que tentam reobter as propriedades conhecidas no contexto de álgebras de Hopf, dependem da inversibilidade lateral dos elementos group-like fracos envolvidos.

Tendo em vista o Lema 2.2.1 e o parágrafo inicial da Seção 2.1, mesmo no contexto de álgebras de Hopf, para construir extensões de Hopf-Ore geradas por um elemento primitivo, seria suficiente considerar elementos satisfazendo $\Delta(g) = g \otimes g$ e $g \neq 0$, mas utiliza-se para a definição de elemento group-like que, quando k é um corpo, deve valer $\epsilon(g) = 1$. Pelo Lema 2.2.5, isto equivale a exigir que tais elementos sejam inversíveis.

Em contraste com o contexto de álgebras de Hopf fracas, onde, a princípio, a inversibilidade à esquerda e à direita de elementos group-like fracos são independentes, no contexto de álgebras de Hopf vale $\epsilon_t = u\epsilon = \epsilon_s$, de onde um elemento group-like fraco ou é inversível, ou não possui inversos laterais, ou seja, $G(H) = G_w(H) \cap \mathcal{U}(H)$.

Encerraremos esta seção mostrando que, se um anel comutativo A possui idempotentes não triviais, então a estrutura de álgebra de Hopf trivial em A contém elementos satisfazendo $\Delta(g) = g \otimes g$ e $g \neq 0$, mas que não são inversíveis. Ao final do capítulo veremos que, apesar deste exemplo, o Teorema de Panov para álgebras de Hopf não fica incompleto por assumir a inversibilidade dos elementos group-like fracos.

Exemplo 2.2.10. No contexto de álgebras de Hopf sobre anéis comutativos, podem existir elementos group-like fraco que não são inversíveis.

Seja A um anel comutativo. Considere a estrutura de álgebra de Hopf trivial em A, dada pelo Exemplo 1.4.2(1). Seja $g \in G_w(A)$, então

$$g \otimes g = \Delta(1_A)(g \otimes g) = \Delta(g) = g \otimes 1_A.$$

Aplicando μ à igualdade acima, obtemos que $g^2 = g$. Portanto todo elemento group-like fraco de A é um idempotente. Reciprocamente, se $g \in A$ é um idempotente, então

$$\Delta(g) = g \otimes 1_A = gg \otimes 1_A = g \otimes g,$$

onde, na última igualdade, utilizamos que $(a, b) \mapsto a \otimes b$ é uma aplicação A-bilinear. Isso mostra que, em A, os elementos group-like fracos são os elementos idempotentes. Por fim, se $e \in A$ é um idempotente não trivial, então $\epsilon_t(e) = \epsilon_s(e) = \epsilon(e) = e \neq 1_A$. Pela contrapositiva do Lema 2.2.5, segue que e não possui inversos laterais. Em particular, no anel comutativo $H = A \oplus A$, visto como álgebra de Hopf sobre H, o elemento $(1_A, 0) \in H$ é um elemento group-like fraco não inversíveis.

2.3 Caracteres fracos e coderivações

Nesta seção vamos apresentar algumas propriedades de caracteres fracos e coderivações em álgebras de Hopf fracas, as quais serão necessárias para o desenvolvimento dos resultados principais deste texto. As referências para esta seção são [8] e [16].

No contexto de álgebras de Hopf, o Teorema de Panov caracteriza as extensões de Hopf-Ore $H[X; \sigma, \delta]$ de uma álgebra de Hopf H em termos dos **caracteres** de H, ou seja, utilizando os morfismos de álgebras $H \to k$, no sentido da Definição 1.2.12. Nesse caso, a counidade $\epsilon \colon H \to k$ é sempre um caracter de H, o qual é utilizado pelo teorema quando $\sigma = id_H$. No contexto de álgebras de Hopf fracas, a counidade não é necessariamente um morfismo de álgebras, mas ainda vale $id_H(a) = u\epsilon(a_1)a_2$, para todo $a \in H$.

Definição 2.3.1. Seja H uma álgebra de Hopf fraca sobre um anel comutativo k. Dizemos que um morfismo de módulos $\chi \in Hom_k(H, k)$ é um **caracter à esquerda fraco** se $\tau^l_\chi = u\chi * id_H \in End_k(H)$ é um morfismo de álgebras. O morfismo τ^l_χ é chamado **twist à esquerda** por χ. O conjunto dos caracteres à esquerda fracos de H será denotado por $X^l_w(H)$.

Analogamente, chamaremos de **caracter à direita fraco** todo morfismo de módulos $\chi \in Hom_k(H, k)$ tal que o **twist à direita** por χ, definido por $\tau^r_\chi = id_H * u\chi \in End_k(H)$, é um morfismo de álgebras. O conjunto dos caracteres à direita fracos será denotado por $X^r_w(H)$.

Exemplo 2.3.2. Seja H uma álgebra de Hopf e $H' = ke \oplus H$ a álgebra de Hopf fraca de Kaplansky, com operações definidas por

$$u(r) = re, \qquad (re + a)(se + b) = rse + (rb + sa + ab),$$
$$\epsilon(re + a) = 2r + \epsilon_H(a), \qquad \Delta(re + a) = r(1_H \otimes 1_H + f \otimes f) + \Delta_H(a),$$

onde $f = e - 1_H$, e antípoda definida por $S(re + a) = re + S_H(a)$. Vamos mostrar que

$$\chi \in X_w^l(H') \iff \chi|_H \in X_w^l(H) \quad \text{e} \quad \chi(e) = \chi|_H(1_H) + 1_k.$$

Como $H' = ke \oplus H \in {}_k\mathfrak{M}$, se $f \in Hom_k(H', k)$ é um morfismo de módulos, então $f|_H \colon H \to k$ é um morfismo de módulos, enquanto que, se $g \in Hom_k(H, k)$ é um morfismo de módulos e $x \in k$, então $f_{(g,x)}(re + a) := rx + g(a)$ define um morfismo de módulos $f_{(g,x)} \colon H' \to k$. Mais ainda, se $f \in Hom_k(H', k)$, então

$$f_{(f|H,f(e))}(re + a) = rf(e) + f|_H(a) = f(re + a),$$

e, para quaisquer $g \in Hom_k(H, k)$ e $x \in k$, temos

$$f_{(g,x)}|_H(a) = f_{g,x}(0e + a) = 0x + g(a) = g(a).$$

Ou seja, $Hom_k(H', k) \simeq k \times Hom_k(H, k)$, como conjuntos. Seja $\chi \in X_w^l(H')$, então

$$\begin{aligned} e &= \tau_\chi^l(e) \\ &= u\chi(1_H)1_H + u\chi(f)f \\ &= \chi(1_H)e1_H + \chi(f)ef \\ &= \chi(1_H)1_H + \chi(f)f \\ &= [\chi(1_H) - \chi(f)]1_H + \chi(f)e. \end{aligned}$$

Como $e \in H'$ tem escrita única, $e = 1_k e + 0_H$, segue que $\chi(f) = 1_k$ e

$$0 = [\chi(1_H) - \chi(f)]1_H = u_H(\chi(1_H) - 1_k) \implies u\chi(1_H) = u(1_k).$$

Com isso, $\chi(e) = \chi(1_H) + \chi(f) = \chi(1_H) + 1_k$ e $\tau_\chi^l(1_H) = u\chi(1_H)1_H = u(1_k)1_H = 1_H$. O morfismo $\tau_{\chi|_H}^l = (\tau_\chi^l)|_H \colon H \to H$ é multiplicativo, pois a multiplicação de H' estende a multiplicação de H. Logo $\chi|_H$ é um caracter à esquerda fraco de H.

Reciprocamente, se $\xi \in X_w^l(H)$, então $\chi(re + a) = r(\xi(1_H) + 1_k) + \xi(a)$ define um morfismo de módulos. Temos que $\tau_\chi^l \colon H' \to k$ é unitário, pois

$$\begin{aligned} \tau_\chi^l(e) &= u\chi(1_H)1_H + u\chi(f)f \\ &= u\xi(1_H)1_H + u(\chi(e) - \chi(1_H))f \\ &= u_H\xi(1_H)1_H + u(1_k)f \\ &= \tau_\xi^l(1_H) + ef \\ &= 1_H + f = e. \end{aligned}$$

Como $\tau_\chi^l(a) = \tau_\xi^l(a)$, segue que $\tau_\chi^l(a)\tau_\chi^l(b) = \tau_\chi^l(ab)$, para todo $a, b \in H$. Logo

$$\begin{aligned} \tau_\chi^l(re + a)\tau_\chi^l(se + b) &= \tau_\chi^l(re)\tau_\chi^l(se) + \tau_\chi^l(re)\tau_\chi^l(b) + \tau_\chi^l(a)\tau_\chi^l(se) + \tau_\chi^l(a)\tau_\chi^l(b) \\ &= re \cdot se + re\tau_\chi^l(b) + \tau_\chi^l(a)se + \tau_\chi^l(a)\tau_\chi^l(b) \\ &= rse + r\tau_\chi^l(b) + s\tau_\chi^l(a) + \tau_\chi^l(ab) \\ &= \tau_\chi^l(rse) + \tau_\chi^l(rb) + \tau_\chi^l(sa) + \tau_\chi^l(ab) \\ &= \tau_\chi^l(rse + [rb + sa + ab]) \\ &= \tau_\chi^l((re + a)(se + b)). \end{aligned}$$

Ou seja, τ_χ^l é multiplicativo. Portanto $\chi \in X_w^l(H')$.

Exemplo 2.3.3. Sejam $n \geq 1$ e $H = \bigoplus_{i,j=1}^{n} ke_{ij}$ a álgebra de Hopf fraca de Hayashi, com morfismos definidos por

$$\mu(e_{ij} \otimes e_{rs}) = [i = r, j = s]e_{ij}, \quad u(1_k) = \sum_{i,j=1}^{n} e_{ij},$$

$$\epsilon(e_{ij}) = [i = j], \quad \Delta(e_{ij}) = \sum_{p=1}^{n} e_{ip} \otimes e_{pj} \quad \text{e} \quad S(e_{ij}) = e_{ji}.$$

Vamos mostrar que $\chi \in Hom_k(H, k)$ é um caracter à esquerda fraco de H se, e somente se, para cada $j = 1, \ldots, n$, o conjunto $\{\chi(e_{ij}) \colon i = 1, \ldots, n\}$ é formado por idempotentes ortogonais tais que $\sum_{i=1}^{n} \chi(e_{ij}) = 1_k$.

Seja $\chi \in Hom_k(H, k)$ e considere $\tau_\chi^l(e_{ij}) = (u\chi * id_H)(e_{ij})$, então

$$\tau_\chi^l(e_{ij}e_{rs}) = [i = r, j = s]\tau_\chi^l(e_{ij}) = [i = r, j = s]\sum_{p=1}^{n} \chi(e_{ip})e_{pj}.$$

Enquanto que,

$$\tau_\chi^l(e_{ij})\tau_\chi^l(e_{rs}) = \left(\sum_{p=1}^{n} \chi(e_{ip})e_{pj}\right)\left(\sum_{q=1}^{n} \chi(e_{rq})e_{qs}\right) = [j = s]\sum_{p=1}^{n} \chi(e_{ip})\chi(e_{rp})e_{pj}.$$

Portanto, τ_χ^l é multiplicativo se, e somente se, para cada $p = 1, \ldots, n$, vale $\chi(e_{ip})\chi(e_{rp}) = [i = r]\chi(e_{ip})$, ou seja, se o conjunto $\{\chi(e_{1p}), \ldots, \chi(e_{np})\}$ é formado por idempotentes dois a dois ortogonais. Por outro lado, temos

$$\tau_\chi^l(1_H) = \sum_{i,j=1}^{n} \tau_\chi^l(e_{ij}) = \sum_{i,j,p=1}^{n} \chi(e_{ip})e_{pj} = \sum_{p,j=1}^{n}\left(\sum_{i=1}^{n} \chi(e_{ip})\right)e_{pj},$$

de onde vale $\tau_\chi^l(1_H) = 1_H = \sum_{p,j=1}^{n} e_{ij}$ se, e somente se, $\sum_{i=1}^{n} \chi(e_{ip}) = 1_k$, para todo $p = 1, \ldots, n$. Assim, $\chi \in X_w^l(H)$ se, e somente se, para cada $j = 1, \ldots, n$, o conjunto $\{\chi(e_{ij}) \colon i = 1, \ldots, n\}$ é formado por idempotentes ortogonais cuja soma é 1_k.

No contexto de álgebras de Hopf, todo caracter é um caracter à esquerda fraco, pois

$$\tau_\chi^l(ab) = u\chi(a_1b_1)a_2b_2 = u\chi(a_1)a_2u\chi(b_1)b_2 = \tau_\chi^l(a)\tau_\chi^l(b),$$

e $\tau_\chi^l(1_H) = u\chi(1_H)1_H = 1_H^2 = 1_H$. Pelo Exemplo 2.3.2, todo caracter ξ de H define um caracter à esquerda fraco χ de $ke \oplus H$, satisfazendo $\chi(e) = \xi(1_H) + 1_k = 2 \in k$.

De modo geral, todo resultado que apresentaremos para $X_w^l(H)$ possui um resultado correspondente para $X_w^r(H)$, cuja demonstração é essencialmente igual. Assim, apresentaremos as demonstrações completas para $X_w^l(H)$, indicando as alterações necessárias pra $X_w^r(H)$.

Lema 2.3.4. *Seja $\chi \in X_w^l(H)$. Então:*

(i) $\chi * \xi \in X_w^l(H)$, para todo $\xi \in X_w^l(H)$;

(ii) $\tau^l_\chi(s) = s$, *para todo* $s \in H_s$*;*

(iii) Se χ *é inversível na álgebra de convolução* $Hom_k(H,k)$ *e* $\chi^{-1} = \xi$*, então* $\xi \in X^l_w(H)$ *e* $(\tau^l_\chi)^{-1} = \tau^l_\xi$*;*

(iv) Se $(\tau^l_\chi)^{-1} = \sigma$*, então* $\chi * \epsilon\sigma = \epsilon$*.*

Demonstração. Para todo morfismo de módulos $\xi \in Hom_k(H,k)$, temos que $u\xi \colon H \to H$ é um morfismo de módulos, logo $\tau^l_\xi = u\xi * id_H \colon H \to H$ é um morfismo de módulos. Sejam $\xi \in X^l_w(H)$ e $a \in H$, então

$$\begin{aligned}
\tau^l_{\chi*\xi}(a) &= (u(\chi * \xi))(a_1)a_2 \\
&= (u\chi * u\xi)(a_1)a_2 \\
&= u\chi(a_1)u\xi(a_2)a_3 \\
&= u\chi(a_1)\tau^l_\xi(a_2) \\
&= \tau^l_\xi(u\chi(a_1)a_2) && (\tau^l_\xi \text{ morf.}) \\
&= (\tau^l_\xi \circ \tau^l_\chi)(a).
\end{aligned}$$

Como a composição de morfismos de álgebras é um morfismo de álgebras, vale (i). Seja $s \in H_s$, pelo Lema 1.4.6(iv), temos que $\Delta(s) = 1_1 \otimes 1_2 s$, de onde

$$\tau^l_\chi(s) = u\chi(s_1)s_2 = u\chi(1_1)1_2 s = \tau^l_\chi(1_H)s = s.$$

Portanto vale (ii). Se ξ é o inverso de χ na álgebra de convolução $Hom_k(H,k)$, pela identidade obtida no item (i), temos que

$$\tau^l_\xi \circ \tau^l_\chi = \tau^l_{\chi*\xi} = \tau^l_{u\epsilon} = u\epsilon * id_H = id_H \quad \text{e} \quad \tau^l_\chi \circ \tau^l_\xi = \tau^l_{\xi*\chi} = \tau^l_{u\epsilon} = u\epsilon * id_H = id_H.$$

Ou seja, τ^l_ξ é o inverso de τ^l_χ, portanto um morfismo de álgebras. Logo, vale (iii). Por fim, se $\sigma = (\tau^l_\chi)^{-1}$, então σ é, em particular, um morfismo de módulos, logo, $\epsilon\sigma \colon H \to k$ é um morfismo de módulos, e vale

$$(\chi * \epsilon\sigma)(a) = \chi(a_1)(\epsilon \circ \sigma)(a_2) = (\epsilon \circ \sigma)(\chi(a_1)a_2) = (\epsilon \circ \sigma \circ \tau^l_\chi)(a) = \epsilon(a).$$

De onde obtemos (iv). □

Lema 2.3.5. *Seja* $\chi \in X^r_w(H)$*. Então:*

(i) $\chi * \xi \in X^r_w(H)$*, para todo* $\xi \in X^r_w(H)$*;*

(ii) $\tau^r_\chi(t) = t$*, para todo* $t \in H_t$*;*

(iii) Se χ *é inversível na álgebra de convolução* $Hom_k(H,k)$ *e* $\chi^{-1} = \xi$*, então* $\xi \in X^r_w(H)$ *e* $(\tau^r_\chi)^{-1} = \tau^r_\xi$*;*

(iv) Se $(\tau^r_\chi)^{-1} = \sigma$*, então* $\epsilon\sigma * \chi = \epsilon$*.*

Demonstração. (ideia) Análogo ao lema anterior. Mostra-se que $\tau^r_{\chi*\xi} = \tau^r_\chi \circ \tau^r_\xi$, o que prova (i). Para $t \in H_t$, do Lema 1.4.6(iii) segue que $\tau^r_\chi(t) = t1_1 u\chi(1_2) = t$, de onde vale (ii). O item (iii) utiliza a igualdade $\tau^r_{\chi*\xi} = \tau^r_\chi \circ \tau^r_\xi$. O item (iv) segue de $\epsilon\sigma * \chi = \epsilon \circ \sigma \circ \tau^r_\chi = \epsilon$. □

Quando H é cocomutativa, temos $\tau_\chi^l(a) = u\chi(a_1)a_2 = u\chi(a_2)a_1 = a_1u\chi(a_2) = \tau_\chi^r(a)$, de onde segue que τ_χ^r é um automorfismo se, e somente se, χ for inversível na álgebra de convolução $Hom_k(H, k)$.

Lema 2.3.6. *Seja $\sigma \in End_k(H)$. Então:*

(i) $\Delta \circ \sigma = (\sigma \otimes id_H) \circ \Delta$ se, e somente se, existe $\chi \in Hom_k(H, k)$ tal que $\sigma = \tau_\chi^l$;

(ii) $\Delta \circ \sigma = (id_H \otimes \sigma) \circ \Delta$ se, e somente se, existe $\chi \in Hom_k(H, k)$ tal que $\sigma = \tau_\chi^r$.

Em ambos os casos, pode-se considerar $\chi = \epsilon \circ \sigma$.

Demonstração. Suponha que $\sigma = \tau_\chi^l$, então

$$\Delta(\sigma(a)) = \Delta(u\chi(a_1)a_2) = u\chi(a_1)a_2 \otimes a_3 = \tau_\chi^l(a_1) \otimes a_2 = (\sigma \otimes id_H)\Delta(a),$$

onde, na segunda igualdade, utilizamos que $im(\chi) \subseteq k$ e Δ é morfismo de módulos. Reciprocamente, se $\Delta \circ \sigma = (\sigma \otimes id_H) \circ \Delta$, definindo $\chi = \epsilon \circ \sigma \in Hom_k(H, k)$, temos

$$\begin{aligned}
\tau_\chi^l(a) &= u\chi(a_1)a_2 \\
&= u\epsilon\sigma(a_1)a_2 \\
&= \mu(u\epsilon \otimes id_H)(\sigma \otimes id_H)\Delta(a) \\
&= \mu(u\epsilon \otimes id_H)\Delta\sigma(a) \\
&= (u\epsilon * id_H)(\sigma(a)) \\
&= \sigma(a), & (u\epsilon = 1_{End_k(H)})
\end{aligned}$$

de onde vale (i). A demonstração de (ii) é análoga. □

No contexto de álgebras de Hopf, se χ é um caracter à esquerda (resp. à direita) fraco de H, então, pelo resultado acima, $\chi = \epsilon \circ \sigma$, onde σ é um morfismo de álgebras. Como ϵ é um morfismo de álgebras, segue que χ é um morfismo de álgebras. Assim, χ é um caracter à esquerda fraco se, e somente se, é um caracter se, e somente se, é um caracter à direita fraco. Com isso, denotando o conjunto dos caracteres de uma álgebra de Hopf H por $X(H)$, podemos reescrever o Exemplo 2.3.2 como

$$\chi \in X_w(ke \oplus H) \iff \chi|_H \in X(H) \quad \text{e} \quad \chi(e) = 2.$$

Definição 2.3.7. Sejam $g, h \in G_w(H)$. Um morfismo de módulos $\delta\colon H \to H$ é uma (g, h)**-coderivação** se $\Delta(\delta(a)) = ga_1 \otimes \delta(a_2) + \delta(a_1) \otimes ha_2$, para todo $a \in H$.

Apesar da definição acima considerar δ apenas um morfismo de módulos, na próxima seção, estaremos interessados particularmente em $(g, 1_H)$-coderivações que são τ_χ^l-derivações, onde $\epsilon_t(g) = 1_H$ e $\chi \in X_w^l(H)$.

Exemplo 2.3.8. Sejam H uma álgebra de Hopf e $H' = ke \oplus H$ a álgebra de Hopf fraca de Kaplansky, com operações

$$\begin{aligned}
u(r) &= re, & (re + a)(se + b) &= rse + (rb + sa + ab), \\
\epsilon(re + a) &= 2r + \epsilon_H(a), & \Delta(re + a) &= r(1_H \otimes 1_H + f \otimes f) + \Delta_H(a),
\end{aligned}$$

onde $f = e - 1_H$, e antípoda definida por $S(re + a) = re + S_H(a)$. Sejam $\chi \in X_w^l(H')$ e $g = sf + b \in G_w(H')$. Vamos mostrar que $\delta \in End_k(H')$ é uma τ_χ^l-derivação e uma

(g, e)-coderivação se, e somente se, $\delta|_H$ é uma $\tau^l_\chi|_H$-derivação e uma $(b, 1_H)$-coderivação. Mais ainda, mostramos que g é inversível à esquerda se, e somente se, $s = 1_k$ e $u\epsilon(b) = 1_H$.

Primeiramente, como δ é um morfismo de módulos e uma derivação, dado $x = re+a \in H'$, temos

$$\delta(x) = r\delta(e) + \delta(a) = \delta(a).$$

Pelo Exemplo 2.3.2, temos que $\chi|_H \in X^l_w(H)$, de onde $\tau^l_\chi(1_H) = 1_H$. Como $1_H \in Z(H')$,

$$\delta(1_H) = \delta(1_H^2) = \delta(1_H)1_H + \tau^l_\chi(1_H)\delta(1_H) = 2 \cdot 1_H\delta(1_H).$$

Multiplicando por 1_H e subtraindo $1_H\delta(1_H)$ da igualdade acima, obtemos $1_H\delta(1_H) = 0$. Por outro lado, denotando $\delta(x) = r_xe + a_x \in H'$, para cada $x \in H$, temos

$$0 = 1_H\delta(1_H) = 1_H(r_{1_H}e + a_{1_H}) = r_{1_H}1_H + a_{1_H} \quad \therefore \quad \delta(1_H) = r_{1_H}e - r_{1_H}1_H = r_{1_H}f.$$

Mas $fH = Hf = 0$, de onde $r_{1_H}e - r_{1_H}1_H = \delta(1_H) = 2 \cdot 1_H\delta(1_H) = 2r_{1_H}1_Hf = 0$. Como a escrita de $0 \in H'$ em termos de e e H é única, segue que $r_{1_H} = 0$, portanto $\delta(1_H) = 0$. Com isso, calculamos

$$r_xe + a_x = \delta(x) = \delta(x1_H) = \delta(x)1_H + \tau^l_\chi(x)\delta(1_H) = (r_xe + a_x)1_H = r_x1_H + a_x.$$

Ou seja, $r_xe - r_x1_H = 0$, portanto $r_x = 0$. Isso mostra que $\delta(H) \subseteq H$, de onde $\delta|_H$ é uma $\tau^l_\chi|_H$-derivação. Do Exemplo 2.2.3, todo $g \in G_w(H)$ é da forma $g = sf + b$, onde $s \in k$ é um idempotente e $b \in G_w(H)$. Lembrando que $fH = Hf = 0$, $f^2 = f$ e $\epsilon(f) = 1$, calculamos

$$\begin{aligned}
\epsilon_t(g) &= \epsilon_t(sf + b) \\
&= \epsilon(1_H(sf + b))1_H + \epsilon(f(sf + b))f \\
&= \epsilon(b)1_H + \epsilon(sf^2)f \\
&= \epsilon(b)1_H + sf \\
&= se + \epsilon(b)1_H - s1_H \\
&= se + [u_H\epsilon(b) - u_H(s)].
\end{aligned}$$

Com isso, $\epsilon_t(se + b) = e$ se, e somente se, $s = 1_k$ e $u\epsilon(b) = u\epsilon(s) = u\epsilon(1_k) = 1_H$. Por fim, como δ é uma (g, e)-coderivação e $g = f + b$, temos

$$\begin{aligned}
\Delta(\delta(x)) &= (f + b)x_1 \otimes \delta(x_2) + \delta(x_1) \otimes ex_2 \\
&= bx_1 \otimes \delta(x_2) + \delta(x_1) \otimes 1_Hx_2,
\end{aligned}$$

de onde $\delta|_H$ é uma $(b, 1_H)$-coderivação.

Reciprocamente, sejam $\xi \in X^l_w(H)$, $b \in G_w(H)$ e $\delta'\colon H \to H$ uma τ^l_ξ-derivação que é uma $(b, 1_H)$-coderivação. Pelo Exemplo 2.3.2, definindo $\chi\colon H' \to k$ por $\chi(re + a) = 2e + \xi(a)$, temos que $\chi \in X^l_w(H')$ e $\chi|_H = \xi$. Defina $\delta\colon H' \to H'$ por $\delta(re + a) = \delta'(a)$. Assim, $\delta \in Hom_k(H', H')$, $\delta|_H = \delta'$ e, para quaisquer $re + a, te + c \in H'$, temos

$$\begin{aligned}
&\delta(re + a)(te + c) + \tau^l_\chi(re + a)\delta(te + c) \\
&= \delta'(a)(te + c) + [re + \tau^l_\xi(a)]\delta'(c) \\
&= t\delta'(a) + \delta'(a)c + r\delta'(c) + \tau^l_\xi(a)\delta'(c)
\end{aligned}$$

$$\begin{aligned}
&= \delta'(ta + rc) + \delta'(a)c + \tau^l_\xi(a)\delta'(c)\\
&= \delta'(ta + rc) + \delta'(ac)\\
&= \delta'(ta + rc + ac)\\
&= \delta(rte + [ta + rc + ac])\\
&= \delta([re + a][te + c]),
\end{aligned}$$

logo δ é uma τ^l_χ-derivação. Pelo Exemplo 2.2.3, para todo idempotente $s \in k$, temos $sf + b \in G_w(H')$. Como $fH = 0$ e, para todo $a \in H$, $ea = a = 1_H a$, temos

$$\begin{aligned}
\Delta(\delta(re + a)) &= \Delta(\delta'(a))\\
&= ba_1 \otimes \delta(a_2) + \delta(a_1) \otimes 1_H a_2\\
&= (sf + b)a_1 \otimes \delta(a_2) + \delta(a_1) \otimes ea_2,
\end{aligned}$$

logo δ é uma $(sf + b, e)$-coderivação.

Exemplo 2.3.9. Sejam $n \geq 2$ e $H = \bigoplus_{i,j=1}^n ke_{ij}$ a álgebra de Hopf fraca de Hayashi, com morfismos definidos por

$$\mu(e_{ij} \otimes e_{rs}) = [i = r, j = s]e_{ij}, \quad u(1_k) = \sum_{i,j=1}^n e_{ij},$$

$$\epsilon(e_{ij}) = [i = j], \quad \Delta(e_{ij}) = \sum_{p=1}^n e_{ip} \otimes e_{pj} \quad \text{e} \quad S(e_{ij}) = e_{ji}.$$

Seja $\chi \in X^l_w(H)$. Vamos mostrar que $\delta \in End_k(H)$ é uma τ^l_χ-derivação se, e somente se, existem $d_{rs} \in k$ tais que $\chi(e_{rr})d_{rs} = 0$ e $\delta(e_{ij}) = d_{ij}e_{ij} - \sum_{r=1}^n \chi(e_{ir})d_{rj}e_{rj}$. Mais ainda, se $g \in G_w(H)$ satisfaz $\epsilon_t(g) = 1_H$ e δ é uma $(g, 1_H)$-coderivação, então $\delta \equiv 0$.

Pelo Exemplo 2.3.3, se $\chi \in X^l_w(H)$ então, para cada $j = 1, \ldots, n$, $\{\chi(e_{ij})\colon i = 1, \ldots, n\}$ é uma família de idempotentes ortogonais tais que $\chi(e_{1j}) + \cdots + \chi(e_{nj}) = 1_k$. Seja $\delta \in End_k(H)$ uma τ^l_χ-derivação e denote $\delta(e_{ij}) = \sum_{r,s=1}^n d^{ij}_{rs}e_{rs}$. Então

$$\begin{aligned}
\delta(e_{ij}) &= \delta(e_{ij}e_{ij}) = \delta(e_{ij})e_{ij} + \tau^l_\chi(e_{ij})\delta(e_{ij})\\
&= \left(\sum_{r,s=1}^n d^{ij}_{rs}e_{rs}\right) e_{ij} + \left(\sum_{p=1}^n \chi(e_{ip})e_{pj}\right)\left(\sum_{r,s=1}^n d^{ij}_{rs}e_{rs}\right) = d^{ij}_{ij}e_{ij} + \sum_{p=1}^n \chi(e_{ip})d^{ij}_{pj}e_{pj}.
\end{aligned}$$

Comparando as escritas de $\delta(e_{ij})$, obtemos que: $d^{ij}_{rs} = 0$, para todo $s \neq j$; $d^{ij}_{rj} = \chi(e_{ir})d^{ij}_{rj}$, para todo $r \neq i$; e $d^{ij}_{ij} = d^{ij}_{ij} + \chi(e_{ii})d^{ij}_{ij}$, de onde $\chi(e_{ii})d^{ij}_{ij} = 0$. Fixe $u \neq i$, então

$$\begin{aligned}
0 &= \delta(e_{ij}e_{uj}) = \delta(e_{ij})e_{uj} + \tau^l_\chi(e_{ij})\delta(e_{uj})\\
&= \sum_{r=1}^n d^{ij}_{rj}e_{rj} \cdot e_{uj} + \sum_{p,r=1}^n \chi(e_{ip})e_{pj} \cdot d^{uj}_{rj}e_{rj}\\
&= d^{ij}_{uj}e_{uj} + \sum_{p=1}^n \chi(e_{ip})d^{uj}_{pj}e_{pj}\\
&= d^{ij}_{uj}e_{uj} + \chi(e_{iu})d^{uj}_{uj}e_{uj} + \sum_{p\neq u} \chi(e_{ip})\chi(e_{up})d^{uj}_{pj}e_{pj}
\end{aligned}$$

$$= (d^{ij}_{uj} + \chi(e_{iu})d^{uj}_{uj})e_{uj},$$

onde a última igualdade segue de $\chi(e_{1j}), \ldots, \chi(e_{nj})$ serem idempotentes ortogonais. Assim, temos que $d^{ij}_{uj} + \chi(e_{iu})d^{uj}_{uj} = 0$, para todo $u \neq i$, ou ainda, $d^{ij}_{uj} = -\chi(e_{iu})d^{uj}_{uj}$. Como $\chi(e_{ii})d^{ij}_{ij} = 0$, temos que

$$\delta(e_{ij}) = d^{ij}_{ij}e_{ij} - \sum_{r=1}^{n} \chi(e_{ir})d^{rj}_{rj}e_{rj}, \quad \chi(e_{pj})d^{pj}_{pj} = 0, \forall i, j, p = 1, \ldots, n.$$

Reciprocamente, para cada $i, j = 1, \ldots, n$, escolha $d_{ij} \in k$ tal que $\chi(e_{ij})d_{ij} = 0$. Defina $\delta \in End_k(H)$ por $\delta(e_{ij}) = d_{ij}e_{ij} - \sum_{r=1}^{n} \chi(e_{ir})d_{rj}e_{rj}$, então

$$\begin{aligned}
&\delta(e_{ij})e_{uv} + \tau^l_\chi(e_{ij})\delta(e_{uv}) \\
&= \left(d_{ij}e_{ij} - \sum_{r=1}^{n} \chi(e_{ir})d_{rj}e_{rj}\right) e_{uv} + \left(\sum_{p=1}^{n} \chi(e_{ip})e_{pj}\right)\left(d_{uv}e_{uv} - \sum_{r=1}^{n} \chi(e_{ur})d_{rv}e_{rv}\right) \\
&= [j = v]\left([i = u]d_{ij}e_{ij} - \chi(e_{iu})d_{uj}e_{uj} + \chi(e_{iu})d_{uj}e_{uj} - \sum_{r=1}^{n} \chi(e_{ir})\chi(e_{ur})d_{rj}e_{rj}\right) \\
&= [j = v]\left([i = u]d_{ij}e_{ij} - \sum_{r=1}^{n}[i = u]\chi(e_{ir})d_{rj}e_{rj}\right) \\
&= [i = u, j = v]\left(d_{ij}e_{ij} - \sum_{r=1}^{n} \chi(e_{ir})d_{rj}e_{rj}\right) \\
&= [i = u, j = v]\delta(e_{ij}) \\
&= \delta(e_{ij}e_{uv}),
\end{aligned}$$

ou seja, δ é uma τ^l_χ-derivação. Nesse caso, temos que

$$\Delta(\delta(e_{ij})) = \sum_{p=1}^{n}\left(d_{ij}[e_{ip} \otimes e_{pj}] - \sum_{r=1}^{n} \chi(e_{ir})d_{rj}[e_{rp} \otimes e_{pj}]\right).$$

Por outro lado, se δ é uma $(g, 1_H)$-coderivação, então

$$\begin{aligned}
&\Delta(\delta(e_{ij})) = \sum_{p=1}^{n} ge_{ip} \otimes \delta(e_{pj}) + \delta(e_{ip}) \otimes e_{pj} \\
&= \sum_{p=1}^{n} ge_{ip} \otimes \left(d_{pj}e_{pj} - \sum_{r=1}^{n} \chi(e_{pr})d_{rj}e_{rj}\right) + \left(d_{ip}e_{ip} - \sum_{r=1}^{n} \chi(e_{ir})d_{rp}e_{rp}\right) \otimes e_{pj} \\
&= \sum_{p=1}^{n}\left(ge_{ip} \otimes d_{pj}e_{pj} + d_{ip}e_{ip} \otimes e_{pj} - \sum_{r=1}^{n}(ge_{ip} \otimes \chi(e_{pr})d_{rj}e_{rj} + \chi(e_{ir})d_{rp}e_{rp} \otimes e_{pj})\right).
\end{aligned}$$

Pelo Exemplo 2.2.4, se $g \in H$ é um elemento group-like fraco, então existem um idempotente $e \in k$ e escalares $\lambda_1, \ldots, \lambda_n \in \mathcal{U}(ke)$ tais que $g = \sum_{i,j=1}^{n} \lambda_i\lambda^*_j e_{ij}$, onde λ^*_j denota o inverso de λ_j em ke. Com isso, calculamos

$$\epsilon_t(g) = \sum_{i,j=1}^{n} \lambda_i\lambda^*_j\epsilon_t(e_{ij}) = \sum_{i,j,p,r,s=1}^{n} \lambda_i\lambda^*_j\epsilon(e_{rp}e_{ij})e_{ps} = \sum_{i,s=1}^{n} \lambda_i\lambda^*_i e_{is} = \sum_{i,s=1}^{n} ee_{is}.$$

Assim, $\epsilon_t(g) = 1_H$ se, e somente se, $e = 1_k$. Consequentemente, $\lambda_1, \dots, \lambda_n \in \mathcal{U}(k)$ e $\lambda_j^* = \lambda_j^{-1}$, e daí $ge_{ip} = \lambda_i \lambda_p^{-1} e_{ip}$. Substituindo na escrita de $\Delta(\delta(e_{ij}))$, obtemos que δ é uma $(g, 1_H)$-coderivação se, e somente se,

$$\begin{aligned}
&\sum_{p=1}^{n} \left(d_{ij}[e_{ip} \otimes e_{pj}] - \sum_{r=1}^{n} \chi(e_{ir}) d_{rj}[e_{rp} \otimes e_{pj}] \right) \\
&= \sum_{p=1}^{n} \Big(\lambda_i \lambda_p^{-1} d_{pj}[e_{ip} \otimes e_{pj}] + d_{ip}[e_{ip} \otimes e_{pj}] \\
&\quad - \sum_{r=1}^{n} \left(\lambda_i \lambda_p^{-1} \chi(e_{pr}) d_{rj}[e_{ip} \otimes e_{rj}] + \chi(e_{ir}) d_{rp}[e_{rp} \otimes e_{pj}] \right) \Big).
\end{aligned}$$

Cancelando o termo em comum no segundo somatório e colocando em evidência o somando $e_{ip} \otimes e_{pj}$, segue que δ é uma $(g, 1_H)$-coderivação se, e somente se,

$$\sum_{p=1}^{n} d_{ij}[e_{ip} \otimes e_{pj}] = \sum_{p=1}^{n} \Big((\lambda_i \lambda_p^{-1} d_{pj} + d_{ip})[e_{ip} \otimes e_{pj}] - \sum_{r=1}^{n} \lambda_i \lambda_p^{-1} \chi(e_{pr}) d_{rj}[e_{ip} \otimes e_{rj}] \Big).$$

Se $r \neq p$, então o termo $e_{ip} \otimes e_{rj}$ aparece apenas no lado direito da igualdade, assim, deve ser $\lambda_i \lambda_p^{-1} \chi(e_{pr}) d_{rj} = 0$. Como $\lambda_1, \dots, \lambda_n \in k$ são inversíveis, segue que $\chi(e_{pr}) d_{rj} = 0$, para todo $p \neq r$. Mas $\chi(e_{rr}) d_{rj} = 0$, pois δ é uma τ_χ^l-derivação, e $\chi(e_{1r}) + \cdots + \chi(e_{nr}) = 1_k$, pois χ é um caracter à esquerda fraco de H. De onde

$$d_{rj} = [\chi(e_{1r}) + \cdots + \chi(e_{nr})] d_{rj} = \chi(e_{1r}) d_{rj} + \cdots + \chi(e_{nr}) d_{rj} = 0, \quad \forall r, j = 1, \dots, n.$$

Portanto a única τ_χ^l-derivação que é uma $(g, 1_H)$-coderivação, quando $\epsilon_t(g) = 1$, é o morfismo nulo, $\delta \equiv 0$.

Apresentaremos agora algumas propriedades de coderivações.

Lema 2.3.10. *Seja δ uma (g, h)-coderivação. Se $\epsilon_s(g) = \epsilon_s(h) = 1$, então $\epsilon \circ \delta = 0$.*

Demonstração. Como δ é uma (g, h)-coderivação, temos

$$\begin{aligned}
\delta(a) &= (id_H * u\epsilon)(\delta(a)) && (id_H * u\epsilon = id_H) \\
&= ga_1 u\epsilon(\delta(a_2)) + \delta(a_1) u\epsilon(ha_2) \\
&= ga_1 u\epsilon(\delta(a_2)) + \delta(a_1) u\epsilon(a_2) && 2.2.6(ii) \\
&= ga_1 u\epsilon(\delta(a_2)) + \delta(a_1 u\epsilon(a_2)) && (\delta \text{ morf.}) \\
&= ga_1 u\epsilon(\delta(a_2)) + \delta(a), && (id_H * u\epsilon = id_H)
\end{aligned}$$

subtraindo $\delta(a)$ da igualdade acima, obtemos $ga_1 u\epsilon(\delta(a_2)) = 0$. Aplicando ϵ, segue que

$$\begin{aligned}
0 &= \epsilon(ga_1 u\epsilon(\delta(a_2))) \\
&= \epsilon(ga_1)\epsilon(\delta(a_2)) && (\epsilon \text{ morf.}) \\
&= \epsilon(a_1)\epsilon(\delta(a_2)) && 2.2.6(ii) \\
&= \epsilon(\delta(u\epsilon(a_1)a_2)) && (\epsilon\delta \text{ morf.}) \\
&= \epsilon(\delta(a)). && (u\epsilon * id_H = id_H)
\end{aligned}$$

Logo $\epsilon \circ \delta \equiv 0$. $\square$

Lembramos que, conforme observando antes do Lema 1.3.7, dada uma σ-derivação δ de H, o submódulo à esquerda de ${}_HH$ gerado por $im(\delta)$, denotado $\mathcal{U}(\delta)$, é um ideal bilateral que satisfaz $\delta(\mathcal{U}(\delta)) \subseteq \mathcal{U}(\delta)$.

Lema 2.3.11. *Seja δ uma (g, h)-coderivação que é uma τ^l_χ-derivação, onde χ é um caracter à esquerda fraco de H. Se $\epsilon \circ \delta \equiv 0$ e $\delta(H_s) = 0$, então $\epsilon(\mathcal{U}(\delta)) = 0$.*

Demonstração. Como $\chi \in X^l_w(H)$, segue do Lema 2.3.4 que $\tau^l_\chi(\epsilon_s(a)) = \epsilon_s(a)$, para todo $a \in H$. Como δ é uma τ^l_χ-derivação, obtemos

$$\delta(\epsilon_s(a)b) = \delta(\epsilon_s(a))b + \tau^l_\chi(\epsilon_s(a))\delta(b) = \delta(\epsilon_s(a))b + \epsilon_s(a)\delta(b).$$

Aplicando ϵ à igualdade acima, resulta

$$\begin{aligned} 0 &= (\epsilon \circ \delta)(\epsilon_s(a)b) \\ &= \epsilon\Big(\delta(\epsilon_s(a))b\Big) + \epsilon\Big(\epsilon_s(a)\delta(b)\Big) \\ &= \epsilon(\epsilon_s(a)\delta(b)) && (\delta(H_s) = 0) \\ &= \epsilon(a\delta(b)). && 1.4.5(v) \end{aligned}$$

Por fim, como todo elemento em $\mathcal{U}(\delta)$ é da forma $\sum_{i=1}^n a_n\delta(b_n)$, segue que $\epsilon(\mathcal{U}(\delta)) = 0$. □

O último resultado desta seção será especialmente útil no capítulo seguinte, permitindo a simplificação do cálculo para a classificação das extensões de Hopf-Ore primitivas fracas das álgebras de grupóide conexo.

Lema 2.3.12. *Sejam $\sigma \in End_k(H)$ e $g, h \in G_w(H)$. O conjunto $D_{\sigma,g,h}(H)$, dos morfismos $\delta\colon H \to H$ que são σ-derivações e (g, h)-coderivações, é um submódulo de $End_k(H)$.*

Demonstração. Lembramos que a ação de k em $End_k(H)$ é dada por $(r \triangleright f)(a) = f(a) \triangleleft r$, para todo $a \in H$. Assim, se H é uma álgebra sobre k, $(rf)(a) = f(a)u(r) = u(r)f(a)$. Por simplicidade, omitiremos o morfismo u da notação.

Sejam $\delta \in D_{\sigma,g,h}$, $r \in k$ e $a, b \in H$. Então

$$\begin{aligned} (r\delta)(ab) &= r[\delta(ab)] \\ &= r[\delta(a)b + \sigma(a)\delta(b)] && (\delta \in D_{\sigma,g,h}(H)) \\ &= r\delta(a)b + r\sigma(a)\delta(b) \\ &= r\delta(a)b + \sigma(a)r\delta(b) && (im(u) \subseteq Z(H)) \\ &= (r\delta)(a)b + \sigma(a)(r\delta)(b). \end{aligned}$$

Ou seja, $r\delta$ é uma σ-derivação.

$$\begin{aligned} \Delta((r\delta)(a)) &= \Delta(r\delta(a)) \\ &= r\Delta(\delta(a)) && (\Delta \text{ morf.}) \\ &= r[g \otimes \delta(a_1) + \delta(a_2) \otimes h] && (\delta \in D_{\sigma,g,h}(H)) \\ &= g \otimes r\delta(a_1) + r\delta(a_2) \otimes h \\ &= g \otimes (r\delta)(a_1) + (r\delta)(a_2) \otimes h, \end{aligned}$$

de onde $r\delta$ é uma (g, h)-coderivação. Agora, se $\delta, \delta' \in D_{\sigma,g,h}(H)$, então

$$(\delta + \delta')(ab) = \delta(ab) + \delta'(ab)$$

$$
\begin{aligned}
&= [\delta(a)b + \sigma(a)\delta(b)] + [\delta'(a)b + \sigma(a)\delta'(b)] \qquad\qquad (\delta, \delta' \in D_{\sigma,g,h}(H))\\
&= (\delta(a) + \delta'(a))b + \sigma(a)(\delta(b) + \delta'(b))\\
&= (\delta + \delta')(a)b + \sigma(a)(\delta + \delta')(b).
\end{aligned}
$$

Portanto $\delta + \delta'$ é uma σ-derivação. Por fim,

$$
\begin{aligned}
\Delta((\delta + \delta')(a)) &= \Delta(\delta(a)) + \Delta(\delta'(a))\\
&= [g \otimes \delta(a_1) + \delta(a_2) \otimes h] + [g \otimes \delta'(a_1) + \delta'(a_2) \otimes h]\\
&= g \otimes (\delta(a_1) + \delta'(a_1)) + (\delta(a_2) + \delta'(a_2)) \otimes h\\
&= g \otimes (\delta + \delta')(a_1) + (\delta + \delta')(a_2) \otimes h.
\end{aligned}
$$

Assim, $\delta + \delta'$ é uma (g, h)-coderivação. O morfismo nulo é sempre uma derivação e uma coderivação. Logo, $D_{\sigma,g,h}(H)$ é um submódulo de $End_k(H)$. □

2.4 Teorema de Panov para WHA's

Nesta seção vamos apresentar condições necessárias e suficientes para obter extensões de Hopf-Ore $(g, 1)$-primitivas fracas, além de reobter o Teorema de Panov para álgebras de Hopf e caracterizar tais extensões para as álgebras de Hopf fracas dos Exemplos 1.4.4(4) e 1.4.4(5). As referências para esta seção são [8] e [16].

Definição 2.4.1. Sejam H e R álgebras de Hopf fracas sobre um anel comutativo k. Dizemos que R é uma **extensão de Hopf-Ore fraca** de H se R contém H como subálgebra de Hopf fraca e $R = H[X; \sigma, \delta]$, para algum $\sigma, \delta \in End_k(H)$. Diremos ainda que R é uma **extensão de Hopf-Ore primitiva fraca** de H se for uma extensão de Hopf-Ore fraca com X um elemento (g, h)-primitivo fraco, onde $g, h \in G_w(H)$.

Para o restante desta seção, k denotará um anel comutativo, H uma álgebra de Hopf fraca sobre k e $R = H[X; \sigma, \delta]$ uma extensão de Ore de H, onde $\sigma \in Aut_k(H)$ e $\delta \in End_k(H)$ são morfismos de módulos.

Exemplo 2.4.2. Podemos obter extensões de Hopf-Ore primitivas fracas a partir das extensões de Hopf-Ore, caracterizadas pelo Teorema de Panov para álgebras de Hopf.

Seja A uma álgebra de Hopf sobre k. Suponha válido o Teorema de Panov e considere $B = A[X; \sigma, \delta]$ uma extensão de Hopf-Ore de A, onde X é um elemento $(g, 1_A)$-primitivo. Sejam $\overline{g} = g \otimes 1_H \in A \otimes H$ e $\overline{\sigma}, \overline{\delta}\colon A \otimes H \to A \otimes H$ as funções definidas, respectivamente, por

$$\overline{\sigma}(a \otimes b) = \sigma(a) \otimes b \quad \text{e} \quad \overline{\delta}(a \otimes b) = \delta(a) \otimes b.$$

Considere a estrutura de álgebra de Hopf fraca em $A \otimes H$ dada pelo Exemplo 1.4.4(3). Então $\overline{g}$ é um elemento group-like fraco, pois

$$\Delta_{A\otimes H}(1_{A\otimes H}) = \Delta_{A\otimes H}(1_A \otimes 1_H) = 1_A \otimes 1_1 \otimes 1_A \otimes 1_2,$$

de onde

$$
\begin{aligned}
\Delta_{A\otimes H}(\overline{g}) &= \Delta_{A\otimes H}(g \otimes 1_H) = g \otimes 1_1 \otimes g \otimes 1_2\\
&= (1_A \otimes 1_1 \otimes 1_A \otimes 1_2)(g \otimes 1_H \otimes g \otimes 1_H) = \Delta_{A\otimes H}(1_{A\otimes H})(\overline{g} \otimes \overline{g})
\end{aligned}
$$

$$= (g \otimes 1_H \otimes g \otimes 1_H)(1_A \otimes 1_1 \otimes 1_A \otimes 1_2) = (\overline{g} \otimes \overline{g})\Delta_{A\otimes H}(1_{A\otimes H}).$$

A função $\overline{\sigma}$ é um endomorfismo de anéis, pois $\overline{\sigma}(1_{A\otimes H}) = \sigma(1_A) \otimes 1_H = 1_A \otimes 1_H = 1_{A\otimes H}$, enquanto que, para $a \otimes r, b \otimes s \in A \otimes H$, temos

$$\begin{aligned}\overline{\sigma}([a \otimes r][b \otimes s]) &= \overline{\sigma}(ab \otimes rs)\\ &= \sigma(ab) \otimes rs\\ &= \sigma(a)\sigma(b) \otimes rs\\ &= (\sigma(a) \otimes r)(\sigma(b) \otimes s)\\ &= \overline{\sigma}(a \otimes r)\overline{\sigma}(b \otimes s).\end{aligned}$$

Mais ainda, $\overline{\sigma}$ é morfismo de módulos, pois σ e id_H são morfismos de módulos. Analogamente, $\overline{\delta}$ é um morfismo de módulos que é uma $\overline{\sigma}$-derivação, pois

$$\begin{aligned}\overline{\delta}([a \otimes r][b \otimes s]) &= \overline{\delta}(ab \otimes rs)\\ &= \delta(ab) \otimes rs\\ &= (\delta(a)b + \sigma(a)\delta(b)) \otimes rs\\ &= (\delta(a) \otimes r)(b \otimes s) + (\sigma(a) \otimes r)(\delta(b) \otimes s)\\ &= \overline{\delta}(a \otimes r)(b \otimes s) + \overline{\sigma}(a \otimes r)\overline{\delta}(b \otimes s).\end{aligned}$$

Com isso, $R = (A \otimes H)[Y; \overline{\sigma}, \overline{\delta}]$ é uma extensão de Ore de $A \otimes H$. Considere o morfismo $\overline{i} = (i \otimes id_H)\colon A \otimes H \to B \otimes H$, onde $i\colon A \to B$ é o monomorfismo da Proposição 1.3.2, e $y = X \otimes 1_H \in B \otimes H$. Então

$$\begin{aligned}y\overline{i}(a \otimes r) &= (X \otimes 1_H)(a \otimes r)\\ &= Xa \otimes r\\ &= (\sigma(a)X + \delta(a)) \otimes r\\ &= (\sigma(a) \otimes r)(X \otimes 1_H) + \delta(a) \otimes r\\ &= \overline{i}(\overline{\sigma}(a \otimes r))y + \overline{i}(\overline{\delta}(a \otimes r).\end{aligned}$$

Segue da Proposição 1.3.3 que existe um único morfismo de álgebras $f\colon R \to B \otimes H$ tal que $f(Y) = X \otimes 1_H$. O morfismo f é um isomorfismo, pois, se $\sum_{i=0}^{n} r_i Y^i \in ker(f)$, onde $r_0, \ldots, r_n \in A \otimes H$, então

$$0 = f\left(\sum_{i=0}^{n} r_i Y^i\right) = \sum_{i=1}^{n} r_i (X \otimes 1_H)^n = \sum_{i=0}^{n} r_i (X^i \otimes 1_H).$$

Notando que $B\otimes H$ é um $(A\otimes H)$-módulo à esquerda livre de base $\{X^n \otimes 1_H : n \in \mathbb{N}\}$, segue que $r_i = 0$, para todo $i = 0, \ldots, n$, ou seja, $ker(f) = 0$. Por fim, dado $p(X) \otimes r \in B \otimes H$, onde $p(X) = a_0 + a_1X + \cdots + a_nX^n$, então

$$f\left(\sum_{i=0}^{n}(a_i \otimes r)Y^i\right) = \sum_{i=0}^{n}(a_i \otimes r)(X \otimes 1_H)^i = \sum_{i=0}^{n} a_i X^n \otimes r = p(X) \otimes r.$$

Portanto, f é sobrejetora e $A[X; \sigma, \delta] \otimes H \simeq (A \otimes H)[Y; \overline{\sigma}, \overline{\delta}]$ como álgebras. Definindo a estrutura de álgebra de Hopf fraca em R através do isomorfismo, ou seja, tomando

$$\Delta_R = (f^{-1} \otimes f^{-1}) \circ \Delta_{B\otimes H} \circ f, \quad \epsilon_R = \epsilon_{B\otimes H} \circ f \quad \text{e} \quad S_R = f^{-1} \circ S_{B\otimes H} \circ f,$$

obtemos que $A \otimes H$ é uma subálgebra de Hopf fraca de R, onde

$$\begin{aligned}\Delta_R(Y) &= ((f^{-1} \otimes f^{-1}) \circ \Delta_{B\otimes H} \circ f)(Y) \\ &= (f^{-1} \otimes f^{-1})(\Delta_{B\otimes H}(X \otimes 1_H)) \\ &= (f^{-1} \otimes f^{-1})((X \otimes 1_H \otimes g \otimes 1_H + 1_A \otimes 1_H \otimes X \otimes 1_H)\Delta_{B\otimes H}(1_A \otimes 1_H)) \\ &= (Y \otimes f^{-1}(\overline{g}) + 1_R \otimes Y)\Delta_R(1_R),\end{aligned}$$

e, analogamente, $\Delta_R(Y) = \Delta_R(1_R)(Y \otimes f^{-1}(\overline{g}) + 1_R \otimes Y)$. Logo, $R = (A \otimes H)[Y; \sigma, \delta]$ é uma extensão de Hopf-Ore $(f^{-1}(\overline{g}), 1_R)$-primitiva fraca da álgebra de Hopf fraca $A \otimes H$.

Na Seção 2.1 mostramos que, dada uma extensão de Hopf-Ore $R = H[X; \sigma, \delta]$ de uma álgebra de Hopf H, se X é um elemento (g, h)-primitivo, $g, h \in G(H)$, então existem um endomofismo de anéis σ' e uma σ'-derivação δ' tais que $R = H[Y; \sigma', \delta']$, onde $Y = XS(h)$ é um elemento $(gS(h), 1)$-primitivo. Observamos ainda que tal caracterização foi possível pois, em [20], foram consideradas apenas elementos group-like, ou seja, elementos que satisfazem $\Delta(g) = g \otimes g$ e são inversíveis.

Lema 2.4.3. *Seja $R = H[X; \sigma, \delta]$ uma extensão de Hopf-Ore primitiva fraca de H, onde X é um elemento (g, h)-primitivo fraco e $\sigma \in Aut_k(H)$. Então $\epsilon_t(g) = \epsilon_s(h) = 1$.*

Demonstração. Como R é uma álgebra de Hopf fraca, vale o axioma da counidade, logo

$$\begin{aligned}X &= (u\epsilon \otimes id_R)\Delta(X) \\ &= (u\epsilon \otimes id_R)(1_1 g \otimes 1_2 X + 1_1 X \otimes 1_2 h) \\ &= \epsilon(1_1 g)1_2 X + \epsilon(1_1 X)1_2 h \\ &= \epsilon_t(g)X + \epsilon_t(X)h.\end{aligned}$$

Como $\epsilon_t(X) \in H$ e $R \simeq \bigoplus_{n\in\mathbb{N}} HX^n$ como H-módulos à esquerda, a igualdade acima implica em $\epsilon_t(g) = 1_H$ e $\epsilon_t(X)h = 0$. Analogamente,

$$\begin{aligned}X &= (id_R \otimes u\epsilon)\Delta(X) \\ &= (id_R \otimes u\epsilon)(g1_1 \otimes X1_2 + X1_1 \otimes h1_2) \\ &= g1_1\epsilon(X1_2) + X1_1\epsilon(h1_2) \\ &= g\epsilon_s(X) + X\epsilon_s(h).\end{aligned}$$

Como $\sigma \in Aut_k(H)$, segue da Proposição 1.3.9 que $R \simeq \bigoplus_{n\in\mathbb{N}} X^n H$ como H-módulos à direita, de onde obtemos $g\epsilon_s(X) = 0$ e $\epsilon_s(h) = 1_H$. □

Tendo em vista o Lema 2.2.5, o resultado acima mostra que, se σ é um automorfismo, então, para obtermos uma extensão de Hopf-Ore primitiva fraca de H, o elemento g deve ser inversível à direita, enquanto o elemento h deve ser inversível à esquerda.

Observamos que, no contexto de álgebras de Hopf, a hipótese sobre σ é desnecessária, pois, como $\epsilon_s(h) = u\epsilon(h) \in Z(R)$, os cálculos acima mostram que $X = gu\epsilon(X) + u\epsilon(h)X$, de onde concluímos que $\epsilon_s(h) = u\epsilon(h) = 1_H$. Consequentemente, no contexto de álgebras de Hopf sobre anéis comutativos, apesar de existirem elementos group-like fracos não nulos e não inversíveis, vide Exemplo 2.2.10, ao tratarmos de extensões de Hopf-Ore, podemos considerar apenas elementos group-like.

Proposição 2.4.4. *Seja $R = H[X; \sigma, \delta]$ uma extensão de Hopf-Ore fraca de H, onde $\sigma \in Aut_k(H)$ e X é um elemento (g, h)-primitivo fraco. Então:*

(i) $gS(g) = 1_H$ *e* $S(h)h = 1_H$*;*

(ii) δ *é uma* (g, h)*-coderivação;*

(iii) $\Delta(\sigma(a))(1_H \otimes h) = (1_H \otimes h)(\sigma(a_1) \otimes a_2)$*, para todo* $a \in H$*;*

(iv) $\Delta(\sigma(a))(g \otimes 1_H) = (g \otimes 1_H)(a_1 \otimes \sigma(a_2))$*, para todo* $a \in H$*.*

Demonstração. O item (i) segue do lema anterior juntamente do Lema 2.2.5. Agora, como Δ é multiplicativa, devem ser iguais

$$\begin{aligned}
\Delta(X)\Delta(a) &= (g \otimes X + X \otimes h)\Delta(1_H)\Delta(a) \\
&= (g \otimes X + X \otimes h)(a_1 \otimes a_2) \\
&= ga_1 \otimes Xa_2 + Xa_1 \otimes ha_2 \\
&= ga_1 \otimes [\sigma(a_2)X + \delta(a_2)] + [\sigma(a_1)X + \delta(a_1)] \otimes ha_2 \\
&= ga_1 \otimes \sigma(a_2)X + ga_1 \otimes \delta(a_2) + \sigma(a_1)X \otimes ha_2 + \delta(a_1) \otimes ha_2 \\
&= (ga_1 \otimes \sigma(a_2))(1_H \otimes X) + (\sigma(a_1) \otimes ha_2)(X \otimes 1_H) \\
&\quad + (ga_1 \otimes \delta(a_2) + \delta(a_1) \otimes ha_2)(1_H \otimes 1_H),
\end{aligned}$$

e

$$\begin{aligned}
\Delta(Xa) &= \Delta(\sigma(a)X + \delta(a)) \\
&= \Delta(\sigma(a))(g \otimes X + X \otimes h) + \Delta(\delta(a)) \\
&= [\Delta(\sigma(a))(g \otimes 1_H)](1_H \otimes X) + [\Delta(\sigma(a))(1_H \otimes h)](X \otimes 1_H) \\
&\quad + \Delta(\delta(a))(1_H \otimes 1_H).
\end{aligned}$$

Como $R \simeq \bigoplus_{n\in\mathbb{N}} HX^n$, segue da Proposição 1.2.6 que $R \otimes R$ é um $(H \otimes H)$-módulo livre com base $\{X^i \otimes X^j : i, j \in \mathbb{N}\}$. Assim, podemos igualar os coeficientes de $1_H \otimes X$, $X \otimes 1_H$ e $1_H \otimes 1_H$ nas escritas acima, obtendo respectivamente

$$\begin{aligned}
\Delta(\sigma(a))(g \otimes 1_H) &= ga_1 \otimes \sigma(a_2), \\
\Delta(\sigma(a))(1_H \otimes h) &= \sigma(a_1) \otimes ha_2, \\
\Delta(\delta(a)) &= ga_1 \otimes \delta(a_2) + \delta(a_1) \otimes ha_2.
\end{aligned}$$

Ou seja, valem (ii), (iii) e (iv). □

Os resultados acima mostram que, para obtermos uma extensão de Hopf-Ore primitiva fraca de H, o elemento $h \in G_w(H)$ deve ser inversível à esquerda. Caso h seja inversível, podemos reproduzir os cálculos feitos na Proposição 2.1.4, obtendo que $H[X; \sigma, \delta] = H[XS(h); \sigma', \delta']$, onde $XS(h)$ é um elemento $(gS(h), 1_H)$-primitivo fraco. Por outro lado, se $S(h)h = 1_H$ mas $hS(h) = \epsilon_t(h) \neq 1_H$, obteremos que $XS(h)$ é um elemento $(gS(h), \epsilon_t(h))$-primitivo fraco. Mais ainda, a função σ', definida por $\sigma'(a) = \sigma(S(h)ah)$, para todo $a \in H$, não é necessariamente um morfismo de anéis, pois

$$\sigma'(a)\sigma'(b) = \sigma(S(h)a\epsilon_t(h)bh) \quad \text{e} \quad \sigma'(ab) = \sigma(S(h)abh).$$

Assim, vamos nos restringir ao caso em que $h \in G_w(H)$ é inversível, ou equivalentemente, ao estudo das extensões de Hopf-Ore $(g, 1_H)$-primitivas fracas.

Proposição 2.4.5. *Seja* $R = H[X; \sigma, \delta]$ *uma extensão de Hopf-Ore fraca de* H*, onde* $\sigma \in Aut_k(H)$ *e* X *é um elemento* $(g, 1_H)$*-primitivo fraco. Então:*

(i) $gS(g) = 1_H$*;*

(ii) δ *é uma* $(g, 1_H)$*-coderivação;*

(iii) $\sigma = \tau^l_\chi$*, para algum* $\chi \in X^l_w(H)$*;*

(iv) $\Delta(\sigma(a))(g \otimes 1_H) = (g \otimes 1_H)(a_1 \otimes \sigma(a_2))$*, para todo* $a \in H$*;*

(v) $S(a)S(g) = S(g)(\sigma \circ S \circ \sigma)(a)$*, para todo* $a \in H$*;*

(vi) $(S \circ \delta)(a) = S(g)(\delta \circ S \circ \sigma)(a)$*, para todo* $a \in H$*.*

Nesse caso, valem $\epsilon(RX) = \epsilon(XR) = 0$ *e* $S(X) = -S(g)X$*.*

Demonstração. Os itens (i), (ii) e (iv) seguem diretamente da Proposição 2.4.4. O item (iii) segue da Proposição 2.4.4(iii), tomando $h = 1_H$ e aplicando o Lema 2.3.6.

Como X é um elemento $(g, 1_H)$-primitivo fraco e $\epsilon_t(g) = 1_H$, temos

$$\begin{aligned} X = (u\epsilon * id_R)(X) = u\epsilon(1_1 g)1_2 X + u\epsilon(1_1 X)1_2 = \epsilon_t(g)X + \epsilon_t(X) = X + \epsilon_t(X), \\ X = (u\epsilon * id_R)(X) = u\epsilon(g1_1)X1_2 + u\epsilon(X1_1)1_2 = X\epsilon'_t(g) + \epsilon'_t(X). \end{aligned}$$

Da primeira igualdade acima, segue que $\epsilon_t(X) = 0$. Como $\sigma \in Aut_k(H)$, temos da Proposição 1.3.9 que $\{X^i : i \in \mathbb{N}\}$ é uma H-base à direita para R. Assim, segue da segunda igualdade acima que $\epsilon'_t(X) = 0$. Com isso, segue do Lema 2.2.7 que $\epsilon(RX) = \epsilon(XR) = 0$. Mais ainda, o Lema 2.2.7 garante que $\epsilon'_t(X) = 0$ implica $\epsilon_s(X) = 0$ e, como $\epsilon_s(1_H) = 1_H = S(1_H)$, temos do Lema 2.2.8 que $S(X) = -S(g)X$.

Por fim, como S deve ser um anti-morfismo de álgebras, temos

$$\begin{aligned} -S(a)S(g)X &= S(a)S(X) \\ &= S(Xa) \\ &= S(\sigma(a)X + \delta(a)) \\ &= S(X)S(\sigma(a)) + S(\delta(a)) \\ &= -S(g)XS(\sigma(a)) + S(\delta(a)) \\ &= -S(g)[\sigma(S(\sigma(a)))X + \delta(S(\sigma(a)))] + S(\delta(a)) \\ &= -S(g)\sigma(S(\sigma(a)))X + S(\delta(a)) - S(g)\delta(S(\sigma(a))), \end{aligned}$$

de onde, igualando os coeficientes de 1_H e X, obtemos

$$S(a)S(g) = S(g)(\sigma \circ S \circ \sigma)(a) \quad \text{e} \quad S(\delta(a)) = S(g)(\delta \circ S \circ \sigma)(a).$$

Logo valem (v) e (vi). □

Conforme observado após o Lema 2.4.3, no contexto de álgebras de Hopf, a hipótese sobre σ ser um endomorfismo bijetor é supérflua. Assim, se $H[X; \sigma, \delta]$ é uma extensão de Hopf-Ore de uma álgebra de Hopf, onde X é um elemento $(g, 1)$-primitivo, obtemos da proposição acima que $\sigma = \tau^l_\chi$, para algum $\chi \in X^l_w(H)$. Mais ainda, obtemos do Lema 2.3.6 que todo caracter à esquerda (direita) fraco de uma álgebra de Hopf é um caracter, *ie*, um morfismo de álgebras. Nesse caso, sabemos que χ é inversível na álgebra de convolução $Hom_k(H, k)$, com inverso $\chi \circ S$, pois

$$(\chi * (\chi \circ S))(a) = \chi(a_1)\chi(S(a_2)) = \chi(a_1 S(a_2)) = \chi(\epsilon(a)) = \epsilon(a)\chi(1_H) = \epsilon(a).$$

Analogamente, mostra-se $(\chi \circ S) * \chi = \epsilon = 1_{Hom_k(H,k)}$. Segue do Lema 2.3.4 que $\sigma = \tau^l_\chi$ é inversível, com inversa $\tau^l_{\chi S}$. Assim, no contexto de álgebras de Hopf, $\sigma \in Aut_k(H)$ é uma condição necessária para a existência das extensões de Hopf-Ore, apesar de não ser explicitamente utilizada na demonstração do Teorema de Panov.

Para apresentar condições suficientes para a existência de extensões de Hopf-Ore $(g, 1_H)$-primitivas fracas, lembramos que: todo elemento $a \in R = H[X;\sigma,\delta]$ pode ser escrito, de maneira única, como $a = \sum_{i=0}^n a_i X^i$, onde $a_i \in H$, $i = 0, \ldots, n$; e $\mathcal{U}(\delta)$ é um ideal bilateral de H, gerado como submódulo à esquerda de ${}_HH$ por $im(\delta)$.

Lema 2.4.6. *Seja $\epsilon \in Hom_k(H[X;\sigma,\delta], k)$ tal que $\epsilon|_H = \epsilon_H$, $\epsilon(RX) = 0$ e $\epsilon(\mathcal{U}(\delta)) = 0$. Então $\epsilon(abc) = \epsilon_H(a_0b_0c_0)$, para quaisquer $a, b, c \in H[X;\sigma,\delta]$.*

Demonstração. Pelo Lema 1.3.6, dados $r \in H$ e $n \in \mathbb{N}$, temos $X^n r = \delta^n(r) + p_n(r)X$, onde $p_n(r) \in H[X;\sigma,\delta]$ é um elemento de grau $n-1$. Com isso, calculamos

$$\begin{aligned}
\epsilon(abc) &= \sum_{i,j,l=0}^n \epsilon(a_i X^i b_j X^j c_l X^l) \\
&= \sum_{i,j,l=0}^n \epsilon(a_i X^i b_j [\delta^j(c_l) + p_j(c_l)X] X^l) \\
&= \sum_{i,j,l=0}^n \epsilon(a_i X^i b_j \delta^j(c_l) X^l) + \epsilon([a_i X^i b_j p_j(c_l) X^l] X) \\
&= \sum_{i,j,l=0}^n \epsilon(a_i X^i b_j \delta^j(c_l) X^l) && (\epsilon(RX)) = 0) \\
&= \sum_{i,j,l=0}^n \epsilon(a_i [\delta^i(b_j \delta^j(c_l)) + p_i(b_j \delta^j(c_l))X] X^l) \\
&= \sum_{i,j,l=0}^n \epsilon(a_i \delta^i(b_j \delta^j(c_l)) X^l) + \epsilon([a_i p_i(b_j \delta^j(c_l)) X^l] X) \\
&= \sum_{i,j=0}^n \epsilon_H(a_i \delta^i(b_j \delta^j(c_0))) && (\epsilon(RX)) = 0) \\
&= \sum_{j=0}^n \epsilon_H(a_0 b_j \delta^j(c_0)) && (\epsilon(\mathcal{U}(\delta)) = 0) \\
&= \epsilon_H(a_0 b_0 c_0). && (\epsilon(\mathcal{U}(\delta)) = 0)
\end{aligned}$$

□

Lembramos que uma biálgebra fraca é uma quintupla $(H, \mu, u, \Delta, \epsilon)$ satisfazendo os axiomas (W1)-(W4) da Definição 1.4.3. Assim, uma álgebra de Hopf fraca é uma biálgebra fraca que admite uma antípoda S satisfazendo os axiomas em (W5). Ainda, consideramos $\sigma, \delta \in End_k(H)$, de forma que, pelo Lema 1.3.8, $R = H[X;\sigma,\delta]$ é uma k-álgebra.

Proposição 2.4.7. *Sejam $g \in H$ um elemento group-like fraco com $\epsilon_t(g) = 1_H$, $\sigma \in Aut_k(H)$ e $\delta \in End_k(H)$ uma σ-derivação satisfazendo $\epsilon(\mathcal{U}(\delta)) = 0$. Se valem*

(i) δ é uma $(g, 1_H)$-coderivação;

(ii) $\sigma = \tau^l_\chi$, *para algum* $\chi \in X^l_w(H)$;

(iii) $\Delta(\sigma(a))(g \otimes 1_H) = (g \otimes 1_H)(a_1 \otimes \sigma(a_2))$, *para todo* $a \in H$,

então $R = H[X; \sigma, \delta]$ *admite uma estrutura de biálgebra fraca, onde* X *é um elemento* $(g, 1_H)$*-primitivo fraco. Se valem adicionalmente* $\delta(H_s) = 0$ *e, para todo* $a \in H$,

(iv) $S(a)S(g) = S(g)(\sigma \circ S \circ \sigma)(a)$;

(v) $(S \circ \delta)(a) = S(g)(\delta \circ S \circ \sigma)(a)$,

então R *admite uma estrutura de álgebra de Hopf fraca, onde* $S(X) = -S(g)X$.

Demonstração. Começamos observando que, sob as hipóteses (i), (ii) e (iii), vale

$$\Delta(1_H)(g \otimes X + X \otimes 1_H) = (g \otimes X + X \otimes 1_H)\Delta(1_H).$$

Por (ii), juntamente do Lema 2.3.6(i), temos que $\Delta \circ \sigma = (\sigma \otimes id_H) \circ \Delta$. Como δ é uma derivação, $\delta(1_H) = 0$, logo, (i) implica $0 = \Delta(\delta(1_H)) = g1_1 \otimes \delta(1_2) + \delta(1_1) \otimes 1_2$. Com isso,

$$\begin{aligned}
(g \otimes X + X \otimes 1_H)\Delta(1_H) &= g1_1 \otimes X1_2 + X1_1 \otimes 1_2 \\
&= g1_1 \otimes (\sigma(1_2)X + \delta(1_2)) + (\sigma(1_1)X + \delta(1_1)) \otimes 1_2 \\
&= (g1_1 \otimes \sigma(1_2))(1_H \otimes X) + (\sigma(1_1) \otimes 1_2)(X \otimes 1_H) \\
&\quad + g1_1 \otimes \delta(1_2) + \delta(1_1) \otimes 1_2 \\
&= (g1_1 \otimes \sigma(1_2))(1_H \otimes X) + (\sigma(1_1) \otimes 1_2)(X \otimes 1_H) && (i) \\
&= (g1_1 \otimes \sigma(1_2))(1_H \otimes X) + \Delta(\sigma(1_H))(X \otimes 1_H) && (ii) \\
&= (g1_1 \otimes \sigma(1_2))(1_H \otimes X) + \Delta(1_H)(X \otimes 1_H) \\
&= \Delta(\sigma(1_H))(g \otimes 1_H)(1_H \otimes X) + \Delta(1_H)(X \otimes 1_H) && (iii) \\
&= \Delta(1_H)(g \otimes X) + \Delta(1_H)(X \otimes 1_H) \\
&= \Delta(1_H)(g \otimes X + X \otimes 1_H).
\end{aligned}$$

Assim, se for possível definir uma estrutura de biálgebra fraca em $R = H[X; \sigma, \delta]$ com $\Delta(X) = (g \otimes X + X \otimes 1_H)\Delta(1_H)$, então X será um elemento $(g, 1_H)$-primitivo fraco.

Para definir a estrutura de coálgebra em R, vamos utilizar a Propriedade Universal das Extensões de Ore. Como H é uma álgebra de Hopf fraca, $\Delta\colon H \to H \otimes H$ é um morfismo multiplicativo. Seja $x = (g \otimes X + X \otimes 1_H)\Delta(1_H) \in R \otimes R$, então

$$\begin{aligned}
x\Delta(a) &= (g \otimes X + X \otimes 1_H)\Delta(1_H)\Delta(a) \\
&= (g \otimes X + X \otimes 1_H)\Delta(a) && (W3) \\
&= ga_1 \otimes Xa_2 + Xa_1 \otimes a_2 \\
&= ga_1 \otimes (\sigma(a_2)X + \delta(a_2)) + (\sigma(a_1)X + \delta(a_1)) \otimes a_2 \\
&= (ga_1 \otimes \sigma(a_2))(1_H \otimes X) + (\sigma(a_1) \otimes a_2)(X \otimes 1_H) \\
&\quad + ga_1 \otimes \delta(a_2) + \delta(a_1) \otimes a_2 \\
&= (ga_1 \otimes \sigma(a_2))(1_H \otimes X) + (\sigma(a_1) \otimes a_2)(X \otimes 1_H) + \Delta(\delta(a)) && (i) \\
&= (ga_1 \otimes \sigma(a_2))(1_H \otimes X) + \Delta(\sigma(a))(X \otimes 1_H) + \Delta(\delta(a)) && (ii) \\
&= \Delta(\sigma(a))(g \otimes 1_H)(1_H \otimes X) + \Delta(\sigma(a))(X \otimes 1_H) + \Delta(\delta(a)) && (iii) \\
&= \Delta(\sigma(a))(g \otimes X + X \otimes 1_H) + \Delta(\delta(a)) \\
&= \Delta(\sigma(a))\Delta(1_H)(g \otimes X + X \otimes 1_H) + \Delta(\delta(a)) && (W3)
\end{aligned}$$

$$= \Delta(\sigma(a))x + \Delta(\delta(a)).$$

Segue da Propriedade Universal das Extensões de Ore que existe um único morfismo multiplicativo $\overline{\Delta}\colon R \to R \otimes R$, não necessariamente unitário, satisfazendo $\overline{\Delta}(a) = \Delta(a)$, para todo $a \in H$, e tal que

$$\overline{\Delta}(X) = \Delta(1_H)x = \Delta(1_H)(g \otimes X + X \otimes 1_H)\Delta(1_H) = (g \otimes X + X \otimes 1_H)\Delta(1_H).$$

Como $g, 1_H \in G_w(R)$, segue do Lema 2.2.1 que $\overline{\Delta}$ é coassociativo.

Se $\overline{\epsilon}\colon R \to k$ estende ϵ de forma que R admita uma estrutura de álgebra de Hopf fraca, então $\overline{\epsilon_t}(g) = \epsilon_t(g) = 1_H = \overline{\epsilon_t}(1_H)$. Assim, se X for um elemento $(g, 1_H)$-primitivo fraco, pelo Lema 2.2.9, deve ser $\overline{\epsilon_t}(X) = 0$, enquanto que, do Lema 2.2.7(i), obtemos $\overline{\epsilon}(RX) = 0$. Em particular, $\overline{\epsilon}(X^n) = 0$, para todo $n \geq 1$.

Como $\epsilon\colon H \to k$ não é um morfismo multiplicativo, não podemos utilizar a Propriedade Universal das Extensões de Ore. Por outro lado, como R é um H-módulo à esquerda livre de base $\{X^n\colon n \in \mathbb{N}\}$, podemos utilizar a Proposição 1.1.5 para obter um morfismo de H-módulos, $\epsilon'\colon R \to H$, tal que $\epsilon'(1_H) = 1_H$ e $\epsilon'(X^n) = 0$, para todo $n \geq 1$. Considere $\overline{\epsilon} = \epsilon \circ \epsilon'$, então $\overline{\epsilon}$ é um morfismo de k-módulos tal que

$$\begin{aligned}
\overline{\epsilon}(a) &= (\epsilon \circ \epsilon')(a1_H) = \epsilon(a\epsilon'(1_H)) = \epsilon(a), \quad \forall a \in H,\\
\overline{\epsilon}(aX^n) &= (\epsilon \circ \epsilon')(aX^n) = \epsilon(a\epsilon'(X^n)) = \epsilon(0) = 0, \quad \forall n \geq 1.
\end{aligned}$$

Ou seja, $\overline{\epsilon}$ estende ϵ e satisfaz $\overline{\epsilon}(RX) = 0$. Para mostrar que $(R, \overline{\Delta}, \overline{\epsilon})$ é uma coálgebra, resta provar o axioma da counidade. Como $\overline{\epsilon}|_H = \epsilon$, vale o axioma da counidade para elementos $a \in H$, assim, é suficiente considerar o axioma para elementos da forma aX^n, para $n \geq 1$. Começamos calculando

$$\begin{aligned}
\mu(u\overline{\epsilon} \otimes id_R)\overline{\Delta}(aX^n) &= \mu(u\overline{\epsilon} \otimes id_R)\Big(\Delta(a)\overline{\Delta}(X)^n\Big)\\
&= \mu(u\overline{\epsilon} \otimes id_R)\left(\sum_{i,j=0}^{n} a_1 C_{i,j}^{(n)} X^i \otimes a_2 X^j\right) && 1.3.7\\
&= \sum_{i,j=0}^{n} u\overline{\epsilon}\left(a_1 C_{i,j}^{(n)} X^i\right) a_2 X^j\\
&= \sum_{j=0}^{n} u\epsilon\left(a_1 C_{0,j}^{(n)}\right) a_2 X^j.
\end{aligned}$$

Pelo Lema 1.3.7, temos que $C_{0,j}^{(n)} \in \mathcal{U}(\delta)$, para $j = 0, \ldots, n-1$, e $C_{0,n}^{(n)} = g^n$. Como $\mathcal{U}(\delta)$ é um ideal bilateral, $\epsilon(\mathcal{U}(\delta)) = 0$ e $\epsilon_t(g) = 1$, obtemos

$$\begin{aligned}
\mu(u\overline{\epsilon} \otimes id_R)\overline{\Delta}(aX^n) &= \sum_{j=0}^{n} u\epsilon\left(a_1 C_{0,j}^{(n)}\right) a_2 X^j\\
&= u\epsilon\left(a_1 g^n\right) a_2 X^n\\
&= u\epsilon(a_1) a_2 X^n && 2.2.6(i)\\
&= aX^n. && (u\epsilon * id_H = id_H)
\end{aligned}$$

Por outro lado, temos que $C_{i,0}^{(n)} = 0$, para $i = 0, \ldots, n-1$, e $C_{n,0}^{(n)} = 1_H$, de onde

$$\mu(id_R \otimes u\overline{\epsilon})\overline{\Delta}(aX^n) = \sum_{i,j=0}^{n} a_1 C_{i,j}^{(n)} X^i u\overline{\epsilon}(a_2 X^j) \qquad 1.3.7$$

$$
\begin{aligned}
&= \sum_{i}^{n} a_1 C_{i,0}^{(n)} X^i u\epsilon(a_2) \\
&= a_1 X^n u\epsilon(a_2) \\
&= a_1 u\epsilon(a_2) X^n && (im(u) \subseteq Z(R)) \\
&= aX^n. && (id_H * u\epsilon = id_H)
\end{aligned}
$$

Portanto, $(R, \overline{\Delta}, \overline{\epsilon})$ é uma coálgebra. Mais ainda, $\overline{\Delta}$ é multiplicativa por construção e, como $1_R = 1_H$, $\overline{\Delta}(1_H) = \Delta(1_H)$ e H é uma álgebra de Hopf fraca, vale o axioma (W3) em R. Para que R seja uma biálgebra fraca, resta verificar o axioma (W4). Para isso, observamos que $\overline{\epsilon}(RXR) = 0$. De fato, dados $a, b \in H$ e $m, n \in \mathbb{N}$, calculamos

$$
\begin{aligned}
\overline{\epsilon}\left(aX^n X b X^m\right) &= \overline{\epsilon}\left(a[\delta^{n+1}(b) + p_{n+1}(b)X]X^m\right) && 1.3.6 \\
&= \overline{\epsilon}\left(a\delta^{n+1}(b)X^m\right) + \overline{\epsilon}\left(ap_{n+1}(b)X^{m+1}\right) \\
&= \overline{\epsilon}\left(a\delta^{n+1}(b)X^m\right). && (\overline{\epsilon}(RX) = 0)
\end{aligned}
$$

Assim, se $m \geq 1$, então $\overline{\epsilon}(a\delta^{n+1}(b)X^m) = 0$, pois $\overline{\epsilon}(RX) = 0$, enquanto que, se $m = 0$, então $\overline{\epsilon}(a\delta^{n+1}(b)X^m) = \epsilon(a\delta^{n+1}(b)) \in \epsilon(\mathcal{U}(\delta)) = 0$. Em todo caso, obtemos $\overline{\epsilon}(RXR) = 0$. Agora, dado $a \in R$, podemos escrever, de forma única, $a = a' + a''X$, onde $a' \in H$ e $a'' \in R$ é um polinômio de grau $\deg(a) - 1$. Assim,

$$
\begin{aligned}
\overline{\Delta}(a) &= \Delta(a') + \overline{\Delta}(a'')\overline{\Delta}(X) \\
&= a'_1 \otimes a'_2 + \overline{\Delta}(a'')\Delta(1_H)(g \otimes X + X \otimes 1_H) \\
&= a'_1 \otimes a'_2 + a''_1 g \otimes a''_2 X + a''_1 X \otimes a''_2.
\end{aligned}
$$

Por fim, dados $a, b, c \in R$, com a notação acima calculamos

$$
\begin{aligned}
\overline{\epsilon}(ab_1)\overline{\epsilon}(b_2c) &= \overline{\epsilon}(ab'_1)\overline{\epsilon}(b'_2c) + \overline{\epsilon}(ab''_1 g)\overline{\epsilon}(b''_2 Xc) + \overline{\epsilon}(ab''_1 X)\overline{\epsilon}(b''_2 c) \\
&= \overline{\epsilon}(ab'_1)\overline{\epsilon}(b'_2c) && (\overline{\epsilon}(RXR) = 0) \\
&= \epsilon(a'b'_1)\epsilon(b'_2c') && 2.4.6 \\
&= \epsilon(a'b'c') && (W4) \\
&= \overline{\epsilon}(abc). && 2.4.6
\end{aligned}
$$

e, analogamente, $\overline{\epsilon}(ab_2)\overline{\epsilon}(b_1c) = \overline{\epsilon}(abc)$. Logo, vale (W4), e segue que $(R, \mu, u, \overline{\Delta}, \overline{\epsilon})$ é uma biálgebra fraca. Para definir uma antípoda $\overline{S}\colon R \to R$ que estende S e satisfaz (W5), observamos que, pela Proposição 1.4.10(i), $S\colon H \to H^{op} \subseteq R^{op}$ é um morfismo de álgebras, logo, podemos utilizar a Propriedade Universal das Extensões de Ore.

Mostramos que $\overline{\epsilon}(XR) = 0$, logo, do Lema 2.2.7(ii), temos que $\epsilon_s(X) = 0$. Como X é um elemento $(g, 1_H)$-primitivo fraco com $\overline{\epsilon_t}(1_H) = 1_H$, segue do Lema 2.2.8 que, se R possuir uma estrutura de álgebra de Hopf fraca, deve ser $\overline{S}(X) = -S(g)X$. Seja $x = -S(g)X \in R^{op}$, então

$$
\begin{aligned}
S(\sigma(a)) \bullet_{op} x + S(\delta(a)) &= -S(g)XS(\sigma(a)) + S(\delta(a)) \\
&= -S(g)[\sigma(S(\sigma(a)))X + \delta(S(\sigma(a))] + S(\delta(a)) \\
&= -S(g)\sigma(S(\sigma(a)))X - S(g)\delta(S(\sigma(a)) + S(\delta(a)) \\
&= -S(a)S(g)X - S(g)\delta(S(\sigma(a))) + S(\delta(a)) && (iv) \\
&= -S(a)S(g)X - S(\delta(a) + S(\delta(a)) && (v)
\end{aligned}
$$

$$\begin{aligned}
&= -S(a)S(g)X \\
&= x \bullet_{op} S(a).
\end{aligned}$$

Segue da Propriedade Universal das Extensões de Ore que existe um único morfismo de álgebras $\overline{S}\colon R \to R^{op}$ que estende S e satisfaz $\overline{S}(X) = S(1_H)(-S(g)X) = -S(g)X$. Para verificar os axiomas em (W5), é suficiente considerar os elementos da forma aX^n para $n \geq 1$. Por um lado, de $\overline{\epsilon}(RXR) = 0$, temos que

$$\overline{\epsilon_t}(aX^n) = \overline{\epsilon}(1_1 aX^n)1_2 = 0 \quad \text{e} \quad \overline{\epsilon_s}(aX^n) = 1_1\overline{\epsilon}(aX^n 1_2) = 0.$$

Por outro, denotando $p = aX^{n-1}$, calculamos

$$\begin{aligned}
(id_R * \overline{S})(aX^n) &= \mu(id_R \otimes \overline{S})(p_1 g \otimes p_2 X + p_1 X \otimes p_2) \\
&= p_1 g\overline{S}(p_2 X) + p_1 X\overline{S}(p_2) \\
&= p_1 g\overline{S}(X)\overline{S}(p_2) + p_1 X\overline{S}(p_2) \\
&= -p_1 gS(g)X\overline{S}(p_2) + p_1 X\overline{S}(p_2) \\
&= -p_1 X\overline{S}(p_2) + p_1 X\overline{S}(p_2) && (gS(g) = 1_H) \\
&= 0.
\end{aligned}$$

Portanto, $id_R * \overline{S} = \overline{\epsilon_t}$, logo vale (W5)(c). Para (W5)(b), observamos que, se $s \in H_s$, então

$$\begin{aligned}
Xs &= \sigma(s)X + \delta(s) \\
&= \tau^l_\chi(s)X + \delta(s) && (ii) \\
&= sX + \delta(s) && 2.3.4(ii) \\
&= sX. && (\delta(H_s) = 0)
\end{aligned}$$

Vamos prosseguir por indução em $n \geq 1$. Se $n = 1$, então $p = aX^{n-1} = a \in H$, de onde

$$\begin{aligned}
(\overline{S} * id_R)(aX) &= (\overline{S} * id_R)(pX) \\
&= \overline{S}(p_1 g)p_2 X + \overline{S}(p_1 X)p_2 \\
&= S(g)\overline{S}(p_1)p_2 X + \overline{S}(X)\overline{S}(p_1)p_2 \\
&= S(g)\overline{S}(p_1)p_2 X - S(g)X\overline{S}(p_1)p_2 \\
&= S(g)\epsilon_s(p)X - S(g)X\epsilon_s(p) && (p \in H) \\
&= S(g)\epsilon_s(p)X - S(g)\epsilon_s(p)X && (Xs = sX) \\
&= 0 = \overline{\epsilon_s}(aX).
\end{aligned}$$

Agora, suponha que $(\overline{S} * id_R)(aX^n) = \overline{\epsilon_s}(aX^n) = 0$, para algum $n \geq 1$, então

$$\begin{aligned}
(\overline{S} * id_R)(aX^{n+1}) &= (\overline{S} * id_R)(pX) \\
&= S(g)\overline{S}(p_1)p_2 X - S(g)X\overline{S}(p_1)p_2 \\
&= S(g)\overline{\epsilon_s}(aX^n)X - S(g)X\overline{\epsilon_s}(aX^n) && (hip.) \\
&= 0.
\end{aligned}$$

Portanto, vale (W5)(b). Para (W5)(a), observamos que

$$(\overline{\Delta} \otimes id_R)\overline{\Delta}(pX) = (\overline{\Delta} \otimes id_R)(p_1 g \otimes p_2 X + p_1 X \otimes p_2)$$

$$
\begin{aligned}
&= \overline{\Delta}(p_1g) \otimes p_2X + \overline{\Delta}(p_1X) \otimes p_2 \\
&= \overline{\Delta}(p_1)\overline{\Delta}(g) \otimes p_2X + \overline{\Delta}(p_1)\overline{\Delta}(X) \otimes p_2 \\
&= p_11_1g \otimes p_21_2g \otimes p_3X + p_1g \otimes p_2X \otimes p_3 + p_1X \otimes p_2 \otimes p_3 \\
&= p_1g \otimes p_2g \otimes p_3X + p_1g \otimes p_2X \otimes p_3 + p_1X \otimes p_2 \otimes p_3,
\end{aligned}
$$

onde na terceira igualdade utilizamos que $\overline{\Delta}$ é um morfismo multiplicativo, e na última igualdade utilizamos que $p_1 \otimes p_2 \otimes p_3 = \overline{\Delta}(p_1) \otimes p_2 = \overline{\Delta}(p_1)\overline{\Delta}(1_H) \otimes p_2 = p_11_1 \otimes p_21_2 \otimes p_3$. Vamos argumentar por indução em $n \geq 1$, novamente. Se $n = 1$, então $aX^n = pX$, com $p = a \in H$, logo

$$
\begin{aligned}
&(\overline{S} * id_R * \overline{S})(aX) = (\overline{S} * id_R * \overline{S})(pX) \\
&= \overline{S}(p_1g)p_2g\overline{S}(p_3X) + \overline{S}(p_1g)p_2X\overline{S}(p_3) \\
&\quad + \overline{S}(p_1X)p_2\overline{S}(p_3) \\
&= \overline{S}(g)\overline{S}(p_1)p_2g\overline{S}(X)\overline{S}(p_3) + \overline{S}(g)\overline{S}(p_1)p_2X\overline{S}(p_3) && (\overline{S}\text{ anti-morf.}) \\
&\quad + \overline{S}(X)\overline{S}(p_1)p_2\overline{S}(p_3) \\
&= -S(g)\overline{S}(p_1)p_2gS(g)X\overline{S}(p_3) + S(g)\overline{S}(p_1)p_2X\overline{S}(p_3) && (\overline{S}(X) = -S(g)X) \\
&\quad + \overline{S}(X)\overline{S}(p_1)p_2\overline{S}(p_3) \\
&= -S(g)\overline{S}(p_1)p_2X\overline{S}(p_3) + S(g)\overline{S}(p_1)p_2X\overline{S}(p_3) && (gS(g) = 1_H) \\
&\quad + \overline{S}(X)\overline{S}(p_1)p_2\overline{S}(p_3) \\
&= \overline{S}(X)\overline{S}(p_1)p_2\overline{S}(p_3) \\
&= \overline{S}(X)S(p_1)p_2S(p_3) && (p \in H) \\
&= \overline{S}(X)S(p) && (W5)(a) \\
&= \overline{S}(X)\overline{S}(p) && (\overline{S}|_H = S) \\
&= \overline{S}(pX) = \overline{S}(aX).
\end{aligned}
$$

Note que, do cálculo acima, obtemos a identidade $(\overline{S} * id_R * \overline{S})(pX) = \overline{S}(X)\overline{S}(p_1)p_2\overline{S}(p_3)$, independentemente da escolha de $p \in R$. Agora, suponha que, para algum $n \geq 1$, vale $(\overline{S} * id_R * \overline{S})(aX^n) = \overline{S}(aX^n)$, então, denotando $p = aX^n$, temos

$$
\begin{aligned}
(\overline{S} * id_R * \overline{S})(aX^{n+1}) &= (\overline{S} * id_R * \overline{S})(pX) \\
&= \overline{S}(X)\overline{S}(p_1)p_2\overline{S}(p_3) \\
&= \overline{S}(X)(\overline{S} * id_R * \overline{S})(aX^n) \\
&= \overline{S}(X)\overline{S}(aX^n) && (hip.) \\
&= \overline{S}(aX^{+1}). && (\overline{S}\text{ anti-morf.})
\end{aligned}
$$

Logo, vale (W5)(a) e $(R, \mu, u, \overline{\Delta}, \overline{\epsilon}, \overline{S})$ é uma álgebra de Hopf fraca. □

Nas condições do resultado anterior, se $g \in G_w(H)$ for um elemento inversível, então $\epsilon_s(g) = 1_H$ e, pelo Lema 2.3.10, $\epsilon \circ \delta = 0$. Assim, supondo $\delta(H_s) = 0$, temos do Lema 2.3.11 que $\epsilon(\mathcal{U}(\delta)) = 0$. Ainda, tendo em vista o Lema 1.3.8, como $\sigma = \tau_\chi^l$ fixa os elementos de H_s, a hipótese $\delta(H_s) = 0$ equivale a $Xs = sX$, para todo $s \in H_s$. Assim, tais hipóteses são desnecessárias no contexto de álgebras de Hopf, pois neste caso $g \in G(H)$ é inversível e $H_s = k1_H \subseteq Z(R)$, de onde $\delta(H_s) = 0$. Dado um elemento inversível $g \in H$, denotando $Ad_g(a) = gag^{-1}$, das observações acima temos o seguinte.

Teorema 2.4.8. *Sejam H uma álgebra de Hopf fraca sobre um anel comutativo k, $g \in G(H) = G_w(H) \cap \mathcal{U}(H)$ um elemento group-like fraco inversível, $\sigma \in Aut_k(H)$ um morfismo de álgebras e $\delta \in End_k(H)$ uma σ-derivação tal que $\delta(H_s) = 0$. São equivalentes:*

(1) A estrutura de H pode ser estendida para uma estrutura de álgebra de Hopf fraca em $H[X;\sigma,\delta]$, de forma que X seja $(g, 1_H)$-primitivo fraco e $S(X) = -S(g)X$.

(2) g, σ e δ satisfazem:

(i) $\sigma = \tau^l_\chi = Ad_g \circ \tau^r_\chi$, para algum $\chi \in X^l_w(H)$;

(ii) δ é uma $(g, 1_H)$-coderivação;

(iii) $(Ad_g \circ S)(a) = (\sigma \circ S \circ \sigma)(a)$ e $(S \circ \delta)(a) = S(g)(\delta \circ S \circ \sigma)(a)$, para todo $a \in H$.

Demonstração. $[(1) \implies (2)]$ Segue da Proposição 2.4.5. Como o caracter $\chi \in X^l_w(H)$ de 2.4.5(iii) é dado por $\chi = \epsilon \circ \sigma$, multiplicando a identidade 2.4.5(iv) à direita por $g^{-1} \otimes 1_H$, obtemos que

$$\sigma(a) = (id_H * u\epsilon)(ga_1g^{-1} \otimes \sigma(a_2)) = ga_1g^{-1}u\chi(a_2) = ga_1u\chi(a_2)g^{-1} = (Ad_g \circ \tau^r_\chi)(a).$$

Juntamente com a Proposição 2.4.5(iii), obtemos o item (i). Os itens (ii) e (iii) são (ii), (v) e (vi) da Proposição 2.4.5.

$[(2) \implies (1)]$ Segue da Proposição 2.4.7. Como observado anteriormente, a hipótese $g \in G_w(H) \cap \mathcal{U}(H)$ implica $\epsilon_s(g) = 1_H$, portanto $\epsilon(\mathcal{U}(\delta)) = 0$. Assim, resta verificar que vale o item (iii) da Proposição 2.4.7. Como $g^{-1} = S(g)$ e $S(G_w(H)) \subseteq G_w(H)$, temos que $\Delta(g^{-1}) = \Delta(1_H)(g^{-1} \otimes g^{-1})$, logo

$$\begin{aligned}
\Delta(\sigma(a)) &= \Delta((Ad_g \circ \tau^r_\chi)(a)) && (i)\\
&= \Delta(ga_1u\chi(a_2)g^{-1})\\
&= \Delta(g)\Delta(a_1)\Delta(g^{-1}))u\chi(a_2)\\
&= (g \otimes g)\Delta(1_H)\Delta(a_1)\Delta(1_H)(g^{-1} \otimes g^{-1})u\chi(a_2)\\
&= (g \otimes g)\Delta(a_1)(g^{-1} \otimes g^{-1})u\chi(a_2) && (\Delta \text{ mult.})\\
&= (g \otimes g)(a_1 \otimes a_2)(g^{-1} \otimes g^{-1})u\chi(a_3)\\
&= ga_1g^{-1} \otimes ga_2g^{-1}u\chi(a_3)\\
&= ga_1g^{-1} \otimes ga_2u\chi(a_3)g^{-1} && (im(u) \subseteq Z(H))\\
&= ga_1g^{-1} \otimes g\tau^r_\chi(a_2)g^{-1}\\
&= ga_1g^{-1} \otimes Ad_g \circ (\tau^r_\chi)(a_2)\\
&= ga_1g^{-1} \otimes \sigma(a_2).
\end{aligned}$$

Por fim, multiplicando a identidade acima por $g \otimes 1_H$ à direita, segue que

$$\Delta(\sigma(a))(g \otimes 1_H) = (ga_1g^{-1} \otimes \sigma(a_2))(g \otimes 1_H) = ga_1 \otimes \sigma(a_2) = (g \otimes 1_H)(a_1 \otimes \sigma(a_2)).$$

Assim, podemos aplicar a Proposição 2.4.7 para obter (1). □

Conforme observado anteriormente, no contexto de álgebras de Hopf, a hipótese $\sigma \in Aut_k(H)$ é supérflua para a demonstração, porém é uma condição necessária para a obtenção de extensões de Hopf-Ore. Os elementos $g \in G_w(H) \cap \mathcal{U}(H)$ são exatamente os elementos group-like de uma álgebra de Hopf e a hipótese $\delta(H_s) = 0$ é sempre satisfeita. Assim, o Teorema de Panov para álgebras de Hopf é um corolário do Teorema 2.4.8.

Exemplo 2.4.9. Sejam H uma álgebra de Hopf e $H' = ke \oplus H$ a álgebra de Hopf fraca de Kaplansky, com operações

$$\begin{aligned} u(r) &= re, & (re+a)(se+b) &= rse + (rb + sa + ab), \\ \epsilon(re+a) &= 2r + \epsilon_H(a), & \Delta(re+a) &= r(1_H \otimes 1_H + f \otimes f) + \Delta_H(a), \end{aligned}$$

onde $f = e - 1_H$, e antípoda definida por $S(re+a) = re + S_H(a)$. Vamos caracterizar as extensões de Hopf-Ore primitivas fracas de H'.

Pelo Exemplo 2.2.3, os elementos group-like fracos de H são da forma $g = sf + b$, onde $b \in H$ é um elemento group-like fraco. Mais ainda, no Exemplo 2.3.8, mostramos que vale $\epsilon_t(g) = e$ se, e somente se, $s = 1_k$ e $u_H\epsilon(b) = 1_H$. Mas então b é inversível em H com $b^{-1} = S(b)$, de onde obtemos

$$\begin{aligned} S(f+b)(f+b) &= (f + S(b))(f+b) & (S(f) = f) \\ &= f^2 + fb + S(b)f + S(b)b \\ &= f + 1_H & (f^2 = f, fH = Hf = 0) \\ &= e - 1_H + 1_H \\ &= e. \end{aligned}$$

Portanto $g = f + b$ é inversível à esquerda e, como $\epsilon_t(g) = e$, segue do Lema 2.2.5 que g é inversível com $g^{-1} = S(f+b) = f + S(b)$. Assim, a caracterização das extensões de Hopf-Ore primitivas fracas de H' pode ser feita pelo Teorema 2.4.8.

Por outro lado, dado $re + a \in H'$, temos

$$\begin{aligned} \epsilon_s(re+a) &= 1_H\epsilon((re+a)1_H) + f\epsilon((re+a)f) \\ &= 1_H\epsilon(r1_H + a) + f(\epsilon(rf)) \\ &= r1_H + \epsilon(a)1_H + rf \\ &= re + \epsilon(a)1_H, \end{aligned}$$

portanto $H'_s = ke \oplus k1_H$. Pelo Exemplo 2.3.8, se $\delta \in End_k(H')$ é uma τ^l_χ-derivação, então $\delta|_H \in End_k(H)$ é uma $\tau^l_\chi|_H$-derivação. Em particular, $\delta(e) = \delta(1_H) = 0$, logo, $\delta(H'_s) = 0$.

Suponha que $R' = H'[X; \sigma, \delta]$ seja uma extensão de Hopf-Ore (g, e)-primitiva fraca de H'. Então, pelo Teorema 2.4.8, $\sigma = \tau^l_\chi = Ad_g \circ \tau^r_\chi$, para algum $\chi \in X^l_w(H')$, $\delta \in End_k(H')$ é uma (g, e)-coderivação e valem

$$(Ad_g \circ S)(a) = (\sigma \circ S \circ \sigma)(a) \quad \text{e} \quad (S \circ \delta)(a) = S(g)(\sigma \circ S \circ \delta)(a), \quad \forall a \in H'.$$

Pelos Exemplos 2.3.2 e 2.3.8, $\sigma|_H = \tau^l_\chi|_H = \tau^l_{\chi|_H} \in Aut_k(H)$ é um morfismo de álgebras e $\delta|_H \in End_k(H)$ é uma $\sigma|_H$-derivação, assim, podemos considerar a extensão de Ore $R = H[Y; \sigma|_H, \delta|_H]$. Como a inclusão $i\colon H \to R'$, definida por $i(a) = (0e + a)X^0$, para todo $a \in H$, é um morfismo multiplicativo e

$$Xi(a) = Xa = \sigma(a)X + \delta(a) = \sigma|_H(a)X + \delta|_H(a) = i(\sigma|_H(a))X + i(\delta|_H(a)),$$

obtemos da Propriedade Universal das Extensões de Ore que existe um único morfismo multiplicativo $\bar{i}\colon R \to R'$ tal que $\bar{i}(a) = a \in R'$, para todo $a \in H$, e $\bar{i}(Y) = i(1_H)X = 1_HX$. O morfismo $\bar{i}$ é injetor, pois, se

$$0 = \bar{i}\left(\sum_{j=0}^{n} a_j Y^j\right) = \sum_{j=0}^{n} a_j (1_H X)^j = \sum_{j=0}^{n} (0e + a_j) X^j \in R',$$

então $a_j = 0$, para todo $j = 0, \dots, n$, pois $\{X^n : n \in \mathbb{N}\}$ é linearmente independente à esquerda sobre $ke \oplus H$. Ainda, $im(\bar{i}) = \bigoplus_{n\in\mathbb{N}} HX^n = 1_H R'$ é um ideal unitário de $H'[X;\sigma,\delta]$. Assim, vamos considerar $R = im(\bar{i}) \subseteq H'[X;\sigma,\delta] = R'$. Vamos mostrar que R possui uma estrutura de álgebra de Hopf fraca, induzida por R'. Calculamos

$$\begin{aligned}
\Delta(1_H X) &= \Delta(1_H)\Delta(e)(g \otimes X + X \otimes e) \\
&= \Delta(1_H)(g \otimes X + X \otimes e) && (\Delta \text{ mult.}) \\
&= (1_H \otimes 1_H)((f+b) \otimes X + X \otimes e) \\
&= 1_H(f+b) \otimes 1_H X + 1_H X + 1_H e \\
&= b \otimes 1_H X + 1_H X \otimes 1_H. && (Hf = 0)
\end{aligned}$$

De onde $\Delta(1_H X) \in R \otimes R$ e $1_H X$ é um elemento $(b, 1_H)$-primitivo fraco. Mais ainda, como R é um ideal de R', segue que $R \otimes R$ é um ideal de $R' \otimes R'$. Com isso

$$\Delta(a(1_H X)^n) = \Delta(a(1_H X)^{n-1})\Delta(1_H X) \in R \otimes R, \quad \forall a \in H, n \geq 1,$$

enquanto que $\Delta(H) \subseteq H \otimes H \subseteq R \otimes R$, portanto $\Delta(R) \subseteq R \otimes R$. Por outro lado,

$$\begin{aligned}
S(1_H X) &= S(X)1_H && 1.4.10(i) \\
&= -S(g)X1_H && 2.4.8 \\
&= -S(f+b)X1_H \\
&= -(f + S(b))X1_H \\
&= -(f + S(b))1_H X && (1_H \in Z(R')) \\
&= -S(b)1_H X, && (fH = 0)
\end{aligned}$$

de onde $S(1_H X) \in R$. Portanto, $S(aX^n) = S(1_H X)S(aX^{n-1}) \in R$, para todo $a \in H$ e $n \geq 1$, enquanto que $S(H) \subseteq R$. Assim, $S(R) \subseteq R$. Como R é fechado para a multiplicação, comultiplicação, convolução e antípoda, os axiomas da Definição 1.4.3, bem como a identidade $(1_H X)a = \sigma|_H(a)(1_H X) + \delta|_H(a)$, para todo $a \in H$, são herdados de R'. Assim, $R = H[1_H X; \sigma|_H, \delta|_H]$ é uma extensão de Hopf-Ore $(b, 1_H)$-primitiva de H.

Reciprocamente, suponha que $H[Y;\sigma,\delta']$ seja uma extensão de Hopf-Ore $(b, 1_H)$-primitiva de H. Pelo Teorema de Panov para álgebras de Hopf, $g \in G(H)$ é um elemento inversível, $\sigma = \tau^l_\xi = Ad_b \circ \tau^r_\xi$, para algum caracter ξ de H, $\delta' \in End_k(H)$ é uma $(b, 1_H)$-coderivação e valem as identidades

$$(Ad_b \circ S)(a) = (\sigma \circ S \circ \sigma)(a) \quad \text{e} \quad (S \circ \delta')(a) = S(b)\delta'(S(\sigma(a))), \quad \forall a \in H.$$

Pelos Exemplos 2.3.2 e 2.3.8, temos que: $\chi\colon H' \to k$, definido por $\chi(re + a) = 2r + \xi(a)$, é um caracter à esquerda fraco de H' tal que $\chi|_H = \xi$; $g = f + b \in G_w(H)$ satisfaz $\epsilon_t(g) = e$, logo $gS(g) = e$; e $\delta\colon H' \to H'$, definido por $\delta(re + a) = \delta'(a)$, é uma τ^l_χ-derivação que é uma (g, e)-coderivação. Agora, para todo $a \in H$, temos

$$\begin{aligned}
(Ad_g \circ \tau^r_\chi)(a) &= g\tau^r_\chi(a)S(g) \\
&= g\tau^r_\xi(a)S(g) && (\chi|_H = \xi) \\
&= (f+b)\tau^r_\xi(a)(f + b^{-1}) \\
&= b\tau^r_\xi(a)b^{-1} && (fH = Hf = 0) \\
&= (Ad_b \circ \tau^r_\xi)(a)
\end{aligned}$$

$$= \tau^l_\xi(a) = \tau^l_\chi(a), \qquad 2.1.5(i)$$

enquanto que, de $\chi(1_H) = 1_k$, $\chi(f) = \chi(e - 1_H) = 2 - 1_k = 1_k$ e $u(1_k) = e$, temos

$$\begin{aligned}
(Ad_g \circ \tau^r_\chi)(e) &= g1_H u\chi(1_H)S(g) + gfu\chi(f)S(g) \\
&= g1_H S(g) + gfS(g) \\
&= 1_H gS(g) + fgS(g) && (1_H, f \in Z(H')) \\
&= 1_H + f && (gS(g) = e) \\
&= e = \tau^l_\chi(e).
\end{aligned}$$

Assim, como Ad_g, τ^r_χ, τ^l_χ e σ são morfismos de k-módulos, obtemos

$$(Ad_g \circ \tau^r_\chi)(re + a) = r(Ad_g \circ \tau^r_\chi)(e) + (Ad_g \circ \tau^r_\chi)(a) = r\tau^l_\chi(e) + \tau^l_\chi(a) = \tau^l_\chi(re + a).$$

Ou seja, vale 2.4.8(i). Por fim, verificamos

$$\begin{aligned}
(Ad_g \circ S)(a) &= (f + b)S(a)(f + S(b)) \\
&= bS(a)S(b) && (fH = Hf = 0) \\
&= (Ad_b \circ S)(a) \\
&= (\tau^l_\xi \circ S \circ \tau^l_\xi)(a) && 2.1.5(iii) \\
&= (\tau^l_\chi \circ S \circ \tau^l_\chi)(a), && (\chi|_H = \xi)
\end{aligned}$$

e

$$\begin{aligned}
(Ad_g \circ S)(e) &= gS(e)S(g) \\
&= geS(g) \\
&= gS(g) \\
&= e = (\tau^l_\chi \circ S \circ \tau^l_\chi)(e),
\end{aligned}$$

de onde $(Ad_g \circ S)(re + a) = (\tau^l_\chi \circ S \circ \tau^l_\chi)(re + a)$, para todo $re + a \in H'$. Ainda,

$$\begin{aligned}
(S \circ \delta)(a) &= (S \circ \delta')(a) \\
&= S(b)(\delta' \circ S \circ \tau^l_\xi)(a) \\
&= S(b)(\delta \circ S \circ \tau^l_\chi)(a) && (\chi|_H = \xi) \\
&= (f + S(b))(\delta \circ S \circ \tau^l_\chi)(a) && (fH = 0) \\
&= S(g)(\delta \circ S \circ \tau^l_\chi)(a),
\end{aligned}$$

e, como $\delta(e) = 0$ e $S(e) = e = \tau^l_\chi(e)$,

$$(S \circ \delta)(e) = 0 = S(g)(\delta \circ S \circ \tau^l_\chi)(e),$$

portanto, $(S \circ \delta)(re + a) = S(g)(\delta \circ S \circ \sigma)(re + a)$, para todo $re + a \in H'$. Assim, obtemos do Teorema 2.4.8 que $g = f + b$, χ e δ definem uma estrutura de extensão de Hopf-Ore (g, e)-primitiva fraca de H'.

Em suma, as extensões de Hopf-Ore primitivas fracas de H' correspondem às extensões de Hopf-Ore de H, onde cada extensão $(f + b, e)$-primitiva fraca de H' define uma extensão $(b, 1_H)$-primitiva de H, restringindo a estrutura de $H'[X; \sigma, \delta]$ para $H[1_H X; \sigma|_H, \delta|_H]$, e cada extensão $(b, 1_H)$-primitiva de H define uma extensão $(f + b, e)$-primitiva de H', onde $\xi \in X(H)$ é estendido para H' tomando $\chi(e) = 2$ e $\chi|_H = \xi$, enquanto que $\delta' \in End_k(H)$ é estendido para H' tomando $\delta(e) = 0$ e $\delta|_H = \delta'$.

Exemplo 2.4.10. Vamos utilizar o exemplo anterior e a classificação das extensões de Hopf-Ore das álgebras de grupo, feita por Panov em [20, Proposition 2.2] e reobtida no Corolário 3.3.15, para obter uma extensão de Hopf-Ore primitiva fraca de $ke \oplus kG$.

Sejam $k = \mathbb{C}$, $G = \{1_G, g, \ldots, g^{r-1}\}$ e $H = kG$ com a estrutura de álgebra de Hopf de grupo. Considere $H' = ke \oplus H$ a álgebra de Hopf fraca de Kaplansky. Então as extensões de Hopf-Ore primitivas fracas de H' são determinadas por

- Um elemento group-like fraco da forma $r = (e - 1_H) + g^s$, $s = 0, \ldots, r-1$;
- Um morfismo de grupos $\rho\colon G \to \mathbb{C} \setminus \{0\}$, o qual fica bem determinado se, e somente se, $\rho(g)^r = 1$, ou seja, se $\rho(g) = e^{2ni\pi/r} =: q_r^n$, para algum $n = 0, \ldots, r-1$;
- Um 1-cociclo $\gamma\colon G \to \mathbb{C}$ associado a ρ (ver Definição 3.3.12). Considere a função definida por, $\gamma(g^t) = 1 - \rho(g^t)$, então γ é um 1-cociclo, pois, se $h, h' \in G$, então
$$\begin{aligned}\gamma(h) + \rho(h)\gamma(h') &= (1 - \rho(h)) + \rho(h)(1 - \rho(h'))\\ &= 1 - \rho(h) + \rho(h) - \rho(h)\rho(h') = 1 - \rho(hh') = \gamma(hh').\end{aligned}$$
Mais ainda, mostra-se que o conjunto dos 1-cociclos associados a um morfismo de grupos $\rho\colon G \to \mathcal{U}(k)$ é um módulo sobre k, com ação $(a \triangleright \gamma)(h) = a\gamma(h)$, para todo $h \in G$ e $a \in k$, e soma pontual.

Assim, temos um caracter à esquerda fraco $\chi\colon H' \to k$, definido por $\chi(e) = 2$, $\chi(g^t) = \rho(g^t) = (q_r^n)^t$, e uma derivação $\delta\colon H' \to H'$, definida por por $\delta(e) = 0$, e
$$\delta(g^t) = \gamma(g^t)(e - r)g^t = (1_{\mathbb{C}} - (q_r^n)^t)(g^s - 1_G)g^t.$$
Como $H'_s = ke \oplus k1$ e $\delta(e) = \delta(1) = 0$, segue que $R = H'[X; \tau_\chi, \delta]$ possui uma estrutura de álgebra de Hopf fraca, onde X é um elemento $(e - 1_H + g^s, e)$-primitivo fraco, e cuja multiplicação é dada por
$$X\left(ae + \sum_{t=0}^{r-1} a_t g^t\right) = aeX + \sum_{t=0}^{r-1}(q_r^n)^t g^t X + \sum_{t=1}^{r-1}(1_{\mathbb{C}} - (q_r^n)^t)(g^s - 1_G)g^t.$$

Exemplo 2.4.11. Sejam $n \geq 1$ e $H = \bigoplus_{i,j=1}^n ke_{ij}$ a álgebra de Hopf fraca de Hayashi, com morfismos definidos por
$$\mu(e_{ij} \otimes e_{rs}) = [i = r, j = s]e_{ij}, \quad u(1_k) = \sum_{i,j=1}^n e_{ij},$$
$$\epsilon(e_{ij}) = [i = j], \quad \Delta(e_{ij}) = \sum_{p=1}^n e_{ip} \otimes e_{pj} \quad \text{e} \quad S(e_{ij}) = e_{ji}.$$
Vamos mostrar que $R = H[X; \sigma, \delta]$ é uma extensão de Hopf-Ore primitiva fraca de H se, e somente se, $R = H[X]$ é o anel de polinômios usual, onde X é um elemento $(g, 1_H)$-primitivo fraco e $g = \sum_{i,j=1}^n \lambda_i \lambda_j^{-1} e_{ij}$, onde $\lambda_1, \ldots, \lambda_n \in \mathcal{U}(k)$.

Como H é comutativa, um elemento $g \in G_w(H)$ satisfaz $\epsilon_t(g) = 1_H$ se, e somente se, $gS(g) = 1_H$ se, e somente se, $S(g) = g^{-1}$. Assim as extensões de Hopf-Ore primitivas fracas de H ficam determinadas pelo Teorema 2.4.8. Pelo Exemplo 2.3.9, se $g \in G_w(H)$

satisfaz $\epsilon_t(g) = 1_H$ e $\chi \in X^l_w(H)$, então a única τ^l_χ-derivação que é uma $(g, 1_H)$-coderivação é o morfismo nulo. Assim, basta determinar os pares $(\chi, g) \in X^l_w(H) \times (G_w(H) \cap \mathcal{U}(H))$ tais que τ^l_χ é um automorfismo, $\tau^l_\chi = Ad_g \circ \tau^r_\chi$ e $Ad_g \circ S = \tau^l_\chi \circ S \circ \tau^l_\chi$. Novamente, como H é comutativa, $Ad_g(x) = gxg^{-1} = id_H(x)$, portanto, devem valer $\tau^l_\chi = \tau^r_\chi$ e $S = \tau^l_\chi \circ S \circ \tau^l_\chi$.

Pelo Exemplo 2.3.3, $\chi \in X^l_w(H)$ se, e somente se, para cada $j = 1, \dots, n$, o conjunto $\{\chi(e_{1j}), \dots, \chi(e_{nj})\}$ é formado por idempotentes ortogonais tais que $\sum_{i=1}^n \chi(e_{ij}) = 1_k$. Assim, vale $\tau^l_\chi = \tau^r_\chi$ se, e somente se, para cada $i, j = 1, \dots, n$, temos

$$\sum_{p=1}^{n} \chi(e_{ip})e_{pj} = \tau^l_\chi(e_{ij}) = \tau^r_\chi(e_{ij}) = \sum_{p=1}^{n} \chi(e_{pj})e_{ip}.$$

O único termo que aparece tanto à esquerda quanto à direita na igualdade acima é e_{ij}. Assim, deve ser $\chi(e_{pj}) = 0$, para todo $p \neq i$, e $\chi(e_{ip}) = 0$, para todo $p \neq j$, ou seja, $\chi(e_{ij}) = 0$, sempre que $i \neq j$. Mas então, fixado $j = 1, \dots, n$, deve valer $\chi(e_{jj}) = \sum_{i=1}^n \chi(e_{ij}) = 1_k$. Portanto

$$\tau^l_\chi(e_{ij}) = \sum_{p=1}^{n} \chi(e_{ip})e_{pj} = \chi(e_{ii})e_{ij} = e_{ij} = id_H(e_{ij}).$$

Assim, uma tripla (g, σ, δ) satisfaz o Teorema 2.4.8 se, e somente se, $g \in G_w(H) \cap \mathcal{U}(H)$, $\sigma = id_H$ e $\delta = 0$. Por fim, pelos Exemplos 2.2.4 e 2.3.9, temos que $g \in G_w(H) \cap \mathcal{U}(H)$ se, e somente se, $g = \sum_{i,j=1}^n \lambda_i \lambda_j^{-1} e_{ij}$, onde $\lambda_1, \dots, \lambda_j \in \mathcal{U}(k)$ podem ser escolhidos livremente.

No Exemplo 2.4.2 mostramos que, se A é uma álgebra de Hopf e H é uma álgebra de Hopf fraca, então, para cada extensão de Hopf-Ore de A, obtemos uma extensão de Hopf-Ore primitiva fraca da álgebra de Hopf fraca $A \otimes H$. No próximo capítulo vamos classificar as extensões de Hopf-Ore primitivas fracas das álgebras $H = kG \otimes M_n(k)$, onde mostraremos que existem extensões de Hopf-Ore primitivas fracas que não são obtidas através do Teorema de Panov para álgebras de Hopf, juntamente do Exemplo 2.4.2.

O próximo resultado mostra que as hipóteses $\delta(H_s) = 0$ e $\chi \circ S = \chi^{-1}$, na álgebra de convolução $End_k(H)$, são supérfluas para [16, Proposition 5.1].

Lema 2.4.12. *Sejam H uma álgebra de Hopf fraca cocomutativa e $R = H[X; \sigma, \delta]$ uma extensão de Hopf-Ore primitiva fraca de H, onde X é um elemento $(g, 1_H)$-primitivo fraco. Então g é um elemento central de H. Em particular $Ad_g = id_H$.*

Demonstração. Por definição, $\sigma \in Aut_k(H)$. Pela Proposição 2.4.5(3), temos $\sigma = \tau^l_\chi$, para algum $\chi \in X_w(H)$. Segue do Lema 2.3.4(iv) que $\chi' = \epsilon \circ \sigma^{-1}$ é um inverso convolutivo à direita de χ. Mais ainda, multiplicando a identidade (iv) da Proposição 2.4.5 à direita por $S(g)$, segue da Proposição 2.4.5(i) que

$$u\chi(a_1)a_2 \otimes a_3 = \Delta(\tau^l_\chi(a)) = ga_1S(g) \otimes \tau^l_\chi(a_2) = ga_1S(g) \otimes u\chi(a_2)a_3. \qquad (*)$$

Com isso, para todo $a \in H$, temos

$$\begin{aligned} a &= u\epsilon(a_1)a_2 && (u\epsilon * id_H = id_H) \\ &= u(\chi * \chi')(a_1)a_2 && (\chi * \chi' = \epsilon) \\ &= u\chi(a_1)u\chi'(a_2)a_3 \end{aligned}$$

$$\begin{aligned}
&= u\chi(a_1)a_3u\chi'(a_2) && (im(u) \subseteq Z(H))\\
&= u\chi(a_1)a_2u\chi'(a_3) && (cocomut.)\\
&= ga_1S(g)u\chi(a_2)u\chi'(a_3) && (*)\\
&= ga_1S(g)u(\chi * \chi')(a_2) &&\\
&= ga_1S(g)u\epsilon(a_2) && (\chi * \chi' = \epsilon)\\
&= ga_1u\epsilon(a_2)S(g) && (im(u) \subseteq Z(H))\\
&= gaS(g) && (id_H * u\epsilon = id_H).
\end{aligned}$$

Substituindo a por ag no cálculo acima, segue da Proposição 2.4.5(i) que $g \in G_w(H)$ satisfaz $ag = gagS(g) = ga$, ou seja, $g \in Z(H)$. Consequentemente,

$$Ad_g(a) = gaS(g) = agS(g) = a, \quad \forall a \in H.$$

□

Como consequência do lema acima, para classificarmos as extensões de Hopf-Ore primitivas fracas de álgebras de Hopf fracas cocomutativas, o elemento $g \in G_w(H)$ deve ser inversível. Neste caso, podemos utilizar o Teorema 2.4.8 para obter uma caracterização simplificada das extensões de Hopf-Ore primitivas fracas de H.

Teorema 2.4.13. *Sejam H uma álgebra de Hopf fraca cocomutativa, $g \in H$ um elemento group-like fraco, central e inversível, $\chi \in X_w^l(H)$ tal que $\sigma := \tau_\chi^l \in Aut_k(H)$ e $\delta \in End_k(H)$ uma σ-derivação tal que $\delta(H_s) = 0$. Então os seguintes são equivalentes:*

(1) $R = H[X;\sigma,\delta]$ admite uma estrutura de extensão de Hopf-Ore de H, onde X é um elemento $(g, 1_H)$-primitivo fraco.

(2) Valem os seguintes itens:

- *(i) δ é uma $(g, 1_H)$-coderivação.*
- *(ii) $(S \circ \delta)(h) = S(g)(\delta \circ S \circ \sigma)(h)$, para todo $h \in H$.*
- *(iii) $\chi * (\chi \circ S) = \epsilon$.*

Demonstração. Como $g \in G_w(H)$ é inversível, $\sigma \in Aut_k(H)$ e $\delta(H_s) = 0$, segue do Teorema 2.4.8 que vale (1) se, e somente se, valem os seguintes itens:

(i') $\sigma = \tau_\chi^l = Ad_g \circ \tau_\chi^r$;

(ii') δ é uma $(g, 1_H)$-coderivação;

(iii') $(Ad_g \circ S)(h) = (\sigma \circ S \circ \sigma)(h)$ e $(S \circ \delta)(h) = S(g)(\delta \circ S \circ \sigma)(h)$, $\forall h \in H$.

[(2) $\Longrightarrow$ (1)] Temos $\sigma = \tau_\chi^l$ por definição e, como g é central, $Ad_g = id_h$. Mais ainda, como H é cocomutativa, $a_1\chi(a_2) = \chi(a_2)a_1 = \chi(a_1)a_2$, para todo $a \in H$. Portanto $\sigma = \tau_\chi^l = Ad_g \circ \tau_\chi^r$, de ibde vale (i'). O item (ii') segue de (i), enquanto que a segunda igualdade em (iii') segue de (ii). Para a primeira igualdade em (iii'), dado $a \in H$, temos

$$\begin{aligned}
(\tau_\chi^l \circ S \circ \tau_\chi^l)(a) &= (\tau_\chi^l \circ S)(u\chi(a_1)a_2)\\
&= u\chi(a_1)(\tau_\chi^l \circ S)(a_2) && (\tau_\chi^l, S \text{ morf.})\\
&= u\chi(a_1)u\chi(S(a_2)_1)S(a_2)_2
\end{aligned}$$

$$
\begin{aligned}
&= u\chi(a_1)u(\chi\circ S)(a_3)S(a_2) && 1.4.10(iii)\\
&= u\chi(a_1)u(\chi\circ S)(a_2)S(a_3) && (cocomut.)\\
&= u(\chi * \chi S)(a_1)S(a_2) && \\
&= u\epsilon(a_1)S(a_2) && (iii)\\
&= S(u\epsilon(a_1)a_2) && (S \text{ morf.})\\
&= S(a). && (u\epsilon * id_H = id_H)
\end{aligned}
$$

Ou seja, $\sigma \circ S \circ \sigma = S$. Segue de $Ad_g = id_H$ que vale (iii') e, portanto, (1).

[(1) $\implies$ (2)] O item (i) segue de (ii'), enquanto que (ii) segue de (iii'). Como $\sigma = \tau^l_\chi$, onde $\chi \in X^l_w(H) \subseteq Hom_k(H, k)$, segue do Lema 2.3.6(i) que $\sigma = \tau^l_{\epsilon\sigma}$. Como a extensão depende apenas de σ, podemos considerar $\chi = \epsilon \circ \sigma$. Como $\sigma \in Aut_k(H)$, temos do Lema 2.3.4(iv) que $\chi * (\epsilon \circ \sigma^{-1}) = \epsilon$. Por fim, dado $a \in H$, calculamos

$$
\begin{aligned}
(\chi\circ S)(\sigma(a)) &= \epsilon((\sigma\circ S\circ\sigma)(a)) && \\
&= \epsilon((Ad_g\circ S)(a)) && (iii')\\
&= \epsilon(S(a)) && (Ad_g = id_H)\\
&= \epsilon(a). && 1.4.10(iv)
\end{aligned}
$$

Como $\sigma \in Aut_k(H)$, podemos substituir a por $\sigma^{-1}(a)$ no cálculo acima, obtendo a igualdade $(\chi \circ S)(a) = (\epsilon \circ \sigma^{-1})(a)$, para todo $a \in H$. Ou seja, $\epsilon = \chi * (\epsilon \circ \sigma^{-1}) = \chi * (\chi \circ S)$. Assim, vale (iii) e, portanto, (2). $\square$

Mesmo que H não seja cocomutativa, se g for um elemento group-like fraco e inversível, $\sigma = \tau^l_\chi \in Aut_k(H)$, para algum $\chi \in X^l_w(H)$, e vale $Ad_g \circ S = \sigma \circ S \circ \sigma$, então deve valer $\chi * (\chi \circ S) = \epsilon$. Neste caso, como g é um elemento group-like e inversível, segue do Lema 2.2.5 que $\epsilon_s(g) = \epsilon_t(g) = 1_H$, enquanto que, pelo Lema 2.2.6(ii), um elemento $x \in H$ satisfaz $\epsilon_s(x) = 1_H$ se, e somente se, $\epsilon(x^n h) = \epsilon(h)$, para todo $n \in \mathbb{N}$ e $h \in H$. Assim, para todo $a \in H$, temos que

$$
\begin{aligned}
\epsilon((Ad_g\circ S)(a)) &= \epsilon(gS(a)S(g)) && \\
&= \epsilon(S(a)S(g)) && 2.2.5, 2.2.6\\
&= \epsilon(S(ga)) && 1.4.10(i)\\
&= \epsilon(ga) && 1.4.10(iv)\\
&= \epsilon(a). && 2.2.5, 2.2.6
\end{aligned}
$$

Assim como na demonstração anterior, podemos considerar $\chi = \epsilon \circ \sigma$, de onde segue que $\epsilon((\sigma \circ S \circ \sigma)(a)) = (\chi \circ S)(\sigma(a))$ e, como $\sigma \in Aut_k(H)$, obtemos

$$(\epsilon\circ\sigma^{-1})(a) = \epsilon((Ad_g\circ S)(\sigma^{-1}(a))) = \epsilon((\sigma\circ S\circ\sigma)(\sigma^{-1})(a)) = (\chi\circ S)(a).$$

Portanto $\epsilon = \chi * (\epsilon \circ \sigma^{-1}) = \chi * (\chi \circ S)$. Isto mostra que, nas condições do Teorema 2.4.8, toda extensão de Hopf-Ore primitiva fraca vêm de um caractere à esquerda fraco satisfazendo $\chi * (\chi \circ S) = \epsilon$. Porém, sem a hipótese sobre a cocomutatividade de H, não é conhecido se todo caracter à esquerda fraco tal que $\chi * (\chi \circ S) = \epsilon$ e $\tau^l_\chi \in Aut_k(H)$ satisfaz também $Ad_g \circ S = \tau^l_\chi \circ S \circ \tau^l_\chi$.

Terminamos esta seção apresentando um método de obter exemplos de extensões de Hopf-Ore primitivas fracas de álgebras de Hopf fracas cocomutativas.

Proposição 2.4.14. *Sejam H uma álgebra de Hopf fraca cocomutativa, $\chi \in X_w^l(H)$ tal que $\chi \circ S = \chi^{-1}$ na álgebra de convolução $End_k(H)$ e $g \in G_w(H)$ um elemento group-like fraco, central e inversível. Suponha que $\alpha \colon H \to k$ seja um morfismo satisfazendo as identidades $\alpha \circ \epsilon_s = 0$ e*

$$\alpha(ab) = \alpha(a)\epsilon(b) + \chi(a)\alpha(b), \quad \forall a, b \in H. \tag{$*$}$$

Então $\delta \colon H \to H$, definida por $\delta(h) = (1_H - g)\tau_\alpha^l(h)$, é um morfismo de k-módulos, uma τ_χ^l-derivação e uma $(g, 1_H)$-coderivação. Mais ainda, $H[X; \tau_\chi^l, \delta]$ é uma extensão de Hopf-Ore primitiva fraca de H.

Demonstração. A função δ definida no enunciado é um morfismo, pois τ_α^l é um morfismo. Para verificar que δ é uma τ_χ^l-derivação e uma $(g, 1_H)$-coderivação, calculamos

$$\begin{aligned}
\delta(ab) &= (1_H - g)\tau_\alpha^l(ab) \\
&= (1_H - g)\alpha(a_1b_1)a_2b_2 \\
&= (1_H - g)[\alpha(a_1)\epsilon(b_1) + \chi(a_1)\alpha(b_1)]a_2b_2 && (*) \\
&= (1_H - g)\alpha(a_1)\epsilon(b_1)a_2b_2 + (1_H - g)\chi(a_1)\alpha(b_1)a_2b_2 \\
&= (1_H - g)\alpha(a_1)a_2\epsilon(b_1)b_2 + (1_H - g)\chi(a_1)a_2\alpha(b_1)b_2 && (im(\alpha) \subseteq k) \\
&= (1_H - g)\tau_\alpha^l(a)b + (1_H - g)\tau_\chi^l(a)\tau_\alpha^l(b) \\
&= (1_H - g)\tau_\alpha^l(a)b + \tau_\chi^l(a)(1_H - g)\tau_\alpha^l(b) && (1_H - g \in Z(H)) \\
&= \delta(a)b + \tau_\chi^l(a)\delta(b),
\end{aligned}$$

de onde δ é uma τ_χ^l-derivação, e

$$\begin{aligned}
\Delta(\delta(a)) &= \Delta((1_H - g)\tau_\alpha^l(a)) \\
&= \Delta((1_H - g)\alpha(a_1)a_2) \\
&= \alpha(a_1)\Delta(1 - g)\Delta(a_2) && (W3) \\
&= \alpha(a_1)(1_H \otimes 1_H - g \otimes g)\Delta(1_H)\Delta(a_2) && (1_H, g \in G_w(H)) \\
&= \alpha(a_1)((1_H - g) \otimes 1_H + g \otimes (1_H - g))\Delta(a_2) \\
&= (1_H - g)\alpha(a_1)a_2 \otimes a_3 + ga_2 \otimes (1_H - g)\alpha(a_1)a_3 && (im(\alpha) \subseteq k) \\
&= (1_H - g)\alpha(a_1)a_2 \otimes a_3 + ga_1 \otimes (1_H - g)\alpha(a_2)a_3 && (H\ cocomut.) \\
&= (1_H - g)\tau_\alpha^l(a_1) \otimes a_2 + ga_1 \otimes (1_H - g)\tau_\alpha^l(a_2) \\
&= \delta(a_1) \otimes a_2 + ga_1 \otimes \delta(a_2),
\end{aligned}$$

de onde δ é uma $(g, 1_H)$-coderivação. Como $\chi \in X_w^l(H)$ é inversível na álgebra de convolução, com inverso $\chi \circ S$, segue do Lema 2.3.4(iii) que $\sigma = \tau_\chi^l \in Aut_k(H)$. Por hipótese, temos $\alpha(H_s) = 0$, ou seja, $\alpha \circ \epsilon_s = 0$. Assim, se $h \in H_s$, então

$$\begin{aligned}
\delta(h) &= (1_H - g)\alpha(h_1)h_2 \\
&= (1_H - g)\alpha(1_1)h1_2 && 1.4.6(iv) \\
&= (1_H - g)\alpha(\epsilon_s(1_1))h1_2 && 1.4.6(ii) \\
&= 0.
\end{aligned}$$

Tendo em vista o teorema anterior, para mostrar que $H[X; \sigma, \delta]$ é uma extensão de Hopf-Ore primitiva fraca, resta verificar que $(S \circ \delta)(a) = S(g)(\delta \circ S \circ \tau_\chi^l)(a)$, para todo $a \in H$.

Para isso, seja $t \in H_t$, então, pelo Lema 1.4.6(iii), temos que $\Delta(t) = t1_1 \otimes 1_2$. Como H é cocomutativa, isto implica que

$$\Delta(t) = (\tau \circ \Delta)(t) = 1_2 \otimes t1_1 = 1_1 \otimes t1_2.$$

Pelo Lema 1.4.6(iv), segue que $t \in H_s$. Logo, $\alpha \circ \epsilon_s = 0$ implica $\alpha \circ \epsilon_t = 0$. Com isso,

$$\begin{aligned}
0 &= (\alpha \circ \epsilon_t)(a) \\
&= \alpha(a_1 S(a_2)) && (W5)(c) \\
&= \alpha(a_1)\epsilon(S(a_2)) + \chi(a_1)\alpha(S(a_2)) && (*) \\
&= \alpha(a_1)\epsilon(S(a_2)) + \alpha(S(\tau^l_\chi(a))) && (im(\chi) \subseteq k) \\
&= \alpha(a_1)\epsilon(a_2) + \alpha(S(\tau^l_\chi(a))) && 1.4.10(iv) \\
&= \alpha(a_1\epsilon(a_2)) + \alpha(S(\tau^l_\chi(a))) && (im(\epsilon) \subseteq k) \\
&= \alpha(a) + \alpha(S(\tau^l_\chi(a))). && (id_H * u\epsilon = id_H)
\end{aligned}$$

Em suma, para todo $a \in H$, vale a identidade

$$\alpha(a) = -(\alpha \circ S \circ \tau^l_\chi)(a). \qquad (**)$$

Por fim, calculamos

$$\begin{aligned}
S(g)(\delta \circ S \circ \tau^l_\chi)(a) &= S(g)(1_H - g)\tau^l_\alpha(S(\tau^l_\chi(a))) \\
&= -S(1_H - g)\tau^l_\alpha(S(\tau^l_\chi(a))) && (S(g)g = 1_H) \\
&= -S(1_H - g)\alpha(S(\tau^l_\chi(a))_1)S(\tau^l_\chi(a))_2 \\
&= -S(1_H - g)\alpha(S(\tau^l_\chi(a)_2))S(\tau^l_\chi(a)_1) && 1.4.10(iii) \\
&= -S(1_H - g)\alpha(S(\tau^l_\chi(a)_1))S(\tau^l_\chi(a)_2) && (H\ cocomut.) \\
&= -S(1_H - g)\alpha(S(\tau^l_\chi(a_1)))S(a_2) && 2.3.6(i) \\
&= S(1_H - g)\alpha(a_1)S(a_2) && (**) \\
&= S(1_H - g)S(\alpha(a_1)a_2) && (im(\alpha) \subseteq k) \\
&= S(1_H - g)S(\tau^l_\alpha(a)) \\
&= S(\tau^l_\alpha(a)(1_H - g)) && 1.4.10(i) \\
&= S((1_H - g)\tau^l_\alpha(a)) && (1_H - g \in Z(H)) \\
&= S(\delta(a)).
\end{aligned}$$

Portanto $H[X; \sigma, \delta]$ é uma extensão de Hopf-Ore primitiva fraca de H. $\square$

Capítulo 3

Exemplos

Neste capítulo, discutiremos a existência de elementos group-like fracos tais que $\epsilon_s(g) = 1$ mas $\epsilon_t(g) \neq 1$ e as iteradas de extensões de Hopf-Ore primitivas fracas, apresentaremos as álgebras de Hopf fracas de unidade sobrejetora - que, no caso de k ser um corpo, reduz-se ao Exemplo 1.4.2(1) - e a construção das álgebras de grupóide conexo $H \simeq M_n(kG)$, bem como a classificação das extensões de Hopf-Ore primitivas fracas destas.

3.1 Extensões de Ore Noetherianas

Nesta seção, vamos apresentar a classe dos anéis Dedekind-finitos. Mostraremos que todo anel noetheriano, à direita ou à esquerda, é Dedekind-finito, e que extensões de Ore de anéis noetherianos, quando σ é um automorfismo, são anéis noetherianos. As referências desta seção são [14], para os resultados sobre anéis Dedekind-finitos, e [11], para os resultados sobre anéis noetherianos e extensões de Ore.

Na Seção 2.1, mostramos que toda extensão de Hopf-Ore (g, h)-primitiva de uma álgebra de Hopf H é equivalente a uma extensão de Hopf-Ore $(r, 1_H)$-primitiva, cuja demonstração se baseia em considerar a mudança de variáveis $Y = Xh^{-1}$. No contexto de álgebras de Hopf fracas, o Lema 2.4.3 garante que, para termos uma extensão de Hopf-Ore (g, h)-primitiva fraca, deve ocorrer $S(h)h = 1_H$. Porém, se $hS(h) \neq 1_H$, não há garantia que a mudança de variáveis do Lema 2.1.4 defina uma extensão de Ore.

Definição 3.1.1. Um anel A é chamado **Dedekind-finito** quando os elementos de A são inversível à direita se, e somente se, são inversível à esquerda. Ou seja, quando, dados $a, b \in A$, $ab = 1$ implica $ba = 1$.

Se uma álgebra de Hopf fraca H (ou a subálgebra de H gerada por h e $S(h)$) é um anel Dedekind-finito, então podemos repetir a demonstração do Lema 2.1.4, garantindo que toda extensão de Hopf-Ore (g, h)-primitiva fraca corresponde a uma extensão de Hopf-Ore $(gh^{-1}, 1_H)$-primitiva fraca. Mais ainda, quando H é Dedekind-finito, a caracterização das extensões de Hopf-Ore (g, h)-primitivas fracas de H, a menos de uma mudança de variáveis, fica completamente determinada pelo Teorema 2.4.8.

Definição 3.1.2. Seja $(P, \prec)$ um conjunto parcialmente ordenado.

- Dizemos que P satisfaz a **condição de cadeia ascendente** (ACC) se, para toda família enumerável e completamente ordenada $p_1 \prec p_2 \prec \cdots \prec p_n \prec \ldots$, existe $n \in \mathbb{N}$ tal que $p_{n+j} = p_n$, pra todo $j \in \mathbb{N}$.

- Dizemos que um elemento $m \in P$ é **maximal** se todo elemento comparável com m é menor ou igual que m, ou seja, se $m \prec p$ implica $m = p$.

Sejam A um anel e M um A-módulo, à esquerda ou à direita, então o conjunto P, dos A-submódulos de M, é um conjunto parcialmente ordenado pela inclusão. Ou seja, dados $N, N' \subseteq M$ submódulos, temos $N \prec N'$ se $N \subseteq N'$. Assim, dizemos que um A-módulo M satisfaz **ACC em submódulos** se, para toda cadeia $N_1 \subseteq N_2 \subseteq \ldots$ de submódulos de M, existe $n \in \mathbb{N}$ tal que $N_{n+j} = N_n$, para todo $j \in \mathbb{N}$. Quando $M = {}_AA$, os A-submódulos de M são exatamente os ideais à esquerda de A, enquanto que, para $M = A_A$, os A-submódulos de M são os ideais à direita de A.

Lema 3.1.3. *Sejam A um anel e $M \in \mathfrak{M}_A$. São equivalentes:*

(i) M satisfaz ACC em submódulos;

(ii) Toda família não vazia de submódulos de M admite um elemento maximal;

(iii) Todo submódulo de M é finitamente gerado.

Demonstração. [(i) $\implies$ (ii)] Seja $\mathcal{P}$ uma família não vazia de submódulos de M. Suponha que $\mathcal{P}$ não admite um elemento maximal. Então, fixado $N_1 \in \mathcal{P}$, deve existir $N_2 \in \mathcal{P}$ tal que $N_1 \subsetneq N_2$. Recursivamente, devem existir $N_i \in \mathcal{P}$ tais que $N_i \subsetneq N_{i+1}$. Mas então $N_1 \subseteq N_2 \subseteq \ldots$ é uma cadeia completamente ordenada de submódulos de M para a qual não existe $n \in \mathbb{N}$ tal que $N_{n+1} = N_n$, o que contradiz M satisfazer ACC em submódulos. Portanto $\mathcal{P}$ admite um elemento maximal.

[(ii) $\implies$ (iii)] Sejam $N \subseteq M$ um submódulo de M e $\mathcal{P}$ a família dos submódulos finitamente gerados de N. Então $0 \in \mathcal{P}$, e todo submódulo de N é um submódulo de M, assim, por hipótese, $\mathcal{P}$ admite um elemento maximal P. Se $P \subsetneq N$, então existe $x_0 \in N \setminus P$, de onde $P' = P + x_0A$ é um submódulo finitamente gerado de N. Mas $P \subsetneq P'$, o que contradiz P ser maximal em $\mathcal{P}$. Portanto, deve ser $P = N$, de onde N é finitamente gerado.

[(iii) $\implies$ (i)] Sejam $N_1 \subseteq N_2 \subseteq \ldots$ uma cadeia completamente ordenada de submódulos de M e $N = \bigcup_{i \in \mathbb{N}} N_i$. Então N é um submódulo de M, de onde existem $n_1, \ldots, n_r \subseteq N$ tais que $N = \sum_{j=1}^r n_jA$. Como $n_j \in N = \bigcup_{i \in \mathbb{N}} N_i$, existem $i_j \in \mathbb{N}$ tais que $n_j \in N_{i_j}$. Seja $n = max\{i_1, \ldots, i_r\}$, então $n_j \in N_{i_j} \subseteq N_n$, para todo $j = 1, \ldots, r$. Portanto $N = \sum_{j=1}^r n_jA \subseteq \sum_{j=1} N_{i_j} \subseteq N_n$. Assim, se $j \in \mathbb{N}$, então $N_{n+j} \subseteq N \subseteq N_n \subseteq N_{n+j}$, de onde $N_{n+j} = N_n$. Logo, M satisfaz ACC em submódulos. □

Um enunciado análogo ao lema acima pode ser enunciado e provado para A-módulos à esquerda, tomando $P' = P + Ax_0$ em (ii) $\implies$ (iii), e $N = \sum_{j=1}^r An_j$ em (iii) $\implies$ (i).

Definição 3.1.4. Um módulo é dito **noetheriano** se satisfaz um dos itens do lema acima. Dizemos que um anel A é: **noetheriano à esquerda**, se ${}_AA$ é um módulo noetheriano; **noetheriano à direita**, se A_A é um módulo noetheriano; e **noetheriano**, se for noetheriano à direita e à esquerda.

Poderíamos considerar uma *condição de cadeia descendente* (DCC) para cadeias completamente ordenadas $p_{i+1} \prec p_i$, $i \in \mathbb{N}$. O Teorema de Hopkins-Levitzki mostra que a DCC em ideais à direita (esquerda) implica a ACC em ideais à direita (esquerda). Mais ainda, em [14], são discutidas ambas as condições de cadeia sobre famílias menores de ideais unilaterais - como ideais principais e anuladores - obtendo, em [14, Proposition 6.60], vinte condições de cadeia que implicam num dado anel ser Dedekind-finito. O argumento geral é semelhante ao que será apresentado abaixo, mas, nesta seção, vamos considerar exclusivamente a condição de cadeia ascendente em ideais à direta ou à esquerda.

Proposição 3.1.5. *Se A é noetheriano à direita ou à esquerda, então A é Dedekind-finito.*

Demonstração. Vamos mostrar que, se A não é Dedekind-finito, então não é noetheriano à direita nem à esquerda. Neste caso, devem existir $a, b \in A$ tais que $ab = 1$, mas $ba \neq 1$. O elemento $ba \in A$ é um idempotente não trivial, pois $(ba)^2 = b(ab)a = ba$, $ba \neq 1$ por hipótese e, se $ba = 0$, então $a = 1a = (ab)a = a(ba) = 0$, contradizendo $ab = 1$. Ainda,

$$(1 - ba)b = b - b(ab) = b - b = 0 \quad \text{e} \quad a(1 - ba) = a - (ab)a = a - a = 0.$$

Considere os elementos $e_{ij} = b^i(1 - ba)a^j \in A$, então $e_{ij}e_{rs} = [j = r]e_{is}$. De fato, se $j > r$, então $j - r - 1 \geq 0$, de onde

$$\begin{aligned} e_{ij}e_{rs} &= b^i(1 - ba)a^j \cdot b^r(1 - ba)a^s \\ &= b^i(1 - ba)a^{j-r}(1 - ba)a^s \\ &= b^i(1 - ba)a^{j-r-1}[a(1 - ba)]a^s = 0. \end{aligned}$$

Se $j < r$, então $a^j \cdot b^r = b^{r-j} = b \cdot b^{r-j-1}$, de onde $e_{ij}e_{rs} = b^i[(1-ba)b]b^{r-j-1}(1-ba)a^s = 0$. Por outro lado, como $ba \in A$ é um idempotente, $1 - ba$ é um idempotente. Assim, se $j = r$, então $a^j \cdot b^j = 1$, de onde obtemos $e_{ij}e_{js} = b^i(1 - ba)^2a^s = b^i(1 - ba)a^s = e_{is}$. Os elementos e_{ij} são não nulos, pois

$$b^i(1 - ba)a^j = 0 \implies a^i[b^i(1 - ba)a^j]b^j = 0 \implies 1 - ba = 0 \implies ba = 1,$$

o que contradiz A não ser Dedekind-finito. Denote $e_i := e_{ii}$ e considere os ideais à direita definidos por $I_n = \sum_{i=1}^n e_iA$, então $I_1 \subseteq I_2 \subseteq \dots$ é uma cadeia de ideais completamente ordenada em A. Mais ainda, $e_{n+1} \in I_{n+1} \setminus I_n$, para todo $n \in \mathbb{N}$, pois $e_{n+1}^2 = e_{n+1}$, mas $e_{n+1}e_i = 0$, para todo $i \neq n + 1$, de onde

$$e_{n+1}I_n = \sum_{i=1}^{n} e_{n+1}e_iA = \sum_{i=1}^{n} 0A = 0.$$

Assim, não pode ocorrer $e_{n+1} \in I_n$, pois neste caso teríamos $e_{n+1} \in e_{n+1}I_n = 0$, o que contradiz os elementos e_{ij} serem todos não nulos. Isso mostra que A não é noetheriano à direita, pois $I_1 \subsetneq I_2 \subsetneq \dots$ é uma cadeia estrita de ideais à direita. De forma análoga, considerando os ideais à esquerda $J_n = \sum_{j=1}^n Ae_j$, temos que $J_1 \subsetneq J_2 \subsetneq \dots$, pois ocorre $e_{n+1} \in J_{n+1} \setminus J_n$, uma vez que $J_ne_{n+1} = 0$. Logo, A não é noetheriano à esquerda nem à direita. □

Utilizando o Lema 3.1.3(iii), obtemos que todo domínio de ideais principais D é um anel noetheriano, portanto Dedekind-finito. Neste caso, os submódulos de ${}_DD$ e de D_D são, respectivamente, os ideais à esquerda e à direita de D. Assim, os submódulos de ${}_DD$ e D_D são gerados por um único elemento, portanto ambos são módulos noetherianos. Mais geralmente, todo domínio (independente de ser PID à direita ou à esquerda) é Dedekind-finito, pois, como visto na demonstração acima, anéis que não são Dedekind-finitos possuem idempotentes não triviais, portanto divisores de zero não nulos. O próximo lema nos permite obter mais exemplos de módulos noetherianos.

Lema 3.1.6. *Seja A um anel. Então:*

(i) Se $M_1, \dots, M_n \in \mathfrak{M}_A$ são módulos noetherianos, então $M = M_1 \oplus \cdots \oplus M_n$ é um módulo noetheriano;

(ii) Se M é um módulo noetheriano e $f \in Hom_A(M, N)$ é um epimorfismo, então N é um módulo noetheriano;

(iii) Se A é um anel noetheriano à direita (esquerda) e N é um A-módulo à direita (esquerda) finitamente gerado, então N é noetheriano.

Demonstração. (i) Seja N um submódulo de $M = M_1 \oplus \cdots \oplus M_n$. Utilizando as projeções $\pi_i \colon M \to M_i \subseteq M$, definidas por $\pi_i(m_1 + \cdots + m_n) = m_i$, obtemos $N = N(1) \oplus \cdots \oplus N(n)$, onde $N(i) := \pi_i(N)$ é um submódulo de M_i.

Seja $N_1 \subseteq N_2 \subseteq \dots$ uma cadeia completamente ordenada de submódulos de M. Então, para cada $i \in \mathbb{N}$, temos $N_i = N_i(1) \oplus \cdots \oplus N_i(n)$, onde $N_i(j) \subseteq M_j$. Fixado $j \in \{1, \dots, n\}$, como $N_i \subseteq N_{i+1}$, temos $N_i(j) = \pi_j(N_i) \subseteq \pi_j(N_{i+1}) = N_{i+1}(j)$, de onde $N_1(j) \subseteq N_2(j) \subseteq \dots$ é uma cadeia completamente ordenada de submódulos de M_j. Como M_j é um módulo noetheriano, existe $m_j \in \mathbb{N}$ tal que $N_{m_j+k}(j) = N_{m_j}(j)$, para todo $k \in \mathbb{N}$. Seja $m = \max\{m_1, \dots, m_n\}$, então, para todo $j = 1, \dots, n$, temos

$$N_{m+k}(j) = N_{m_j+(m-m_j+k)}(j) = N_m(j) = N_{m_j+(m-m_j)}(j) = N_m(j), \quad k \in \mathbb{N},$$

de onde $N_{m+k} = N_{m+k}(1) \oplus \cdots \oplus N_{m+k}(n) = N_m(1) \oplus \cdots \oplus N_m(n) = N_m$, para todo $k \in \mathbb{N}$. Logo, M satisfaz ACC em submódulos, portanto é um módulo noetheriano.

(ii) Seja $f \colon M \to N$ um epimorfismo. Se P é um submódulo de N, então $f^{-1}(P) = \{m \in M \colon f(m) \in P\}$ é um submódulo de M. Se $P \subseteq P'$, então $f^{-1}(P) \subseteq f^{-1}(P')$. Mais ainda, se $n \in P' \setminus P$, então existe $m \in M$ tal que $f(m) = n$. Assim, $m \in f^{-1}(P') \setminus f^{-1}(P)$.

Suponha que N não é noetheriano. Então existe uma cadeia completamente ordenada $N_1 \subsetneq N_2 \subsetneq \dots$ de submódulos de N, de onde $f^{-1}(N_1) \subsetneq f^{-1}(N_2) \subsetneq \dots$ é uma cadeia completamente ordenada de submódulos de M. Mas isso contradiz M ser noetheriano. Portanto N deve ser noetheriano.

(iii) Suponha que A é noetheriano à direita e seja $N = \sum_{i=1}^n n_i A$ um módulo à direita finitamente gerado. Sejam $M = \bigoplus_{i=1}^n e_i A \simeq A_A \oplus \cdots \oplus A_A$ e $f \colon M \to N$, definido por $f(e_i) = n_i$. Então M é um módulo noetheriano, pois é soma direta finita dos módulos noetherianos A_A, e f é um epimorfismo de módulos. Portanto N é noetheriano. Analogamente, se A é noetheriano à esquerda e $N = \sum_{i=1}^n A n_i$ é um módulo à esquerda finitamente gerado, então existe um epimorfismo ${}_AA \oplus \cdots \oplus {}_AA \to N$. Logo N é noetheriano. □

Com isso podemos mostrar que, se A é um anel noetheriano e comutativo - neste caso A é noetheriano à direita se, e somente se, é noetheriano à esquerda - e (R, u) uma álgebra sobre A que é finitamente gerada como A-módulo, então R é um anel noetheriano. De fato, pelo Lema 3.1.6(iii), temos que R é um módulo noetheriano sobre A. Seja $I \subseteq R$ um ideal à direita de R, então I é um A-submódulo de R, pois $I \triangleleft A = Iu(A) \subseteq IR = I$. Segue do Lema 3.1.3(iii) que I é finitamente gerado como A-módulo. Sejam $r_1, \dots, r_n \in I$ geradores de I como A-módulo, então

$$I = \sum_{i=1}^n r_i \triangleleft A = \sum_{i=1}^n r_i u(A) \subseteq \sum_{i=1}^n r_i R \subseteq I \quad \therefore \quad I = \sum_{i=1}^n r_i R.$$

Portanto I é finitamente gerado como R-submódulo de R_R. Logo, R é noetheriano à direita. Analogamente, se J é um ideal à esquerda de R e $s_1, \dots, s_t \in J$ é um conjunto gerador de J como A-módulo, então $J = \sum_{i=1}^{t} Rs_i$. Portanto R é noetheriano à esquerda. Em particular, se k é um corpo e R é uma álgebra de dimensão finita sobre k, então k é noetheriano e R é finitamente gerado, logo R é um anel Dedekind-finito.

No contexto da Seção 2.4, consideramos apenas extensões de Ore onde σ é um automorfismo. Para mostrar que a propriedade de ser noetheriano à direita (esquerda) é preservada por extensões de Ore, tal hipótese também é necessária - se k é um corpo, $k[t]$ é um domínio, portanto noetheriano à esquerda e à direita, mas a extensão de Ore $R = k[t][X;\sigma]$, onde $\sigma(t) = 0$, $\sigma|_k = id_k$, não é noetheriana à direita ou à esquerda.

De fato, considerando os ideais à direita $I_n = \sum_{i=0}^{n} t^i XR$. Então $I_n \subseteq I_{n+1}$, para todo $n \in \mathbb{N}$, e um elemento genérico $x \in I_n$ é da forma

$$x = \sum_{i=0}^{n} \sum_{r,s} t^i X \cdot a_{rs} t^r X^s = \sum_{i=0}^{n} \sum_{r,s} a_{rs} t^i \sigma(t^r) X^{s+1} = \sum_{i=0}^{n} \sum_{s} a_{0s} t^i X^{s+1}.$$

Assim, segue que $t^{n+1}X \in I_{n+1}$ mas $t^{n+1}X \notin I_n$. Portanto $I_n \subsetneq I_{n+1}$ é uma cadeia estritamente ascendente de ideais à direita de R, de onde segue que R não é noetheriano à direita. Por outro lado, considerando os ideais à esquerda $J_n = \sum_{i=0}^{n} RtX^i$, temos que $J_n \subseteq J_{n+1}$, para todo $n \in \mathbb{N}$, e um elemento genérico $y \in J_n$ é da forma

$$y = \sum_{i=0}^{n} \sum_{r,s} a_{rs} t^r X^s \cdot tX^i = \sum_{i=0}^{n} \sum_{r,s} a_{rs} t^r \sigma^s(t) X^{s+i} = \sum_{i=0}^{n} \sum_{r} a_{rs} t^{t+1} X^i,$$

onde, na última igualdade, utilizamos que $\sigma^0(t) = id_R(t) = t$. Em particular, temos que $tX^{n+1} \in J_{n+1}$, mas $tX^{n+1} \notin J_n$. Portanto R não é noetheriano à esquerda.

Lembrando que, dado um anel A, denotamos por A^{op} seu anel oposto, o qual consiste no conjunto A munido de uma nova multiplicação, definida por $a \bullet b = ba$. Desta forma, se I é um ideal à esquerda de A, $x \in I$ e $a \in A$, então $x \bullet a = ax \in I$. Ou seja, I é um ideal à direita de A^{op}. Reciprocamente, se I é um ideal à direita de A, então $A \bullet I = IA \subseteq I$, de onde I é um ideal à esquerda de A^{op}. Portanto, um anel A é noetheriano à esquerda se, e somente se, A^{op} é noetheriano à direita. Assim, para mostrarmos que extensões de Ore $R = A[X;\sigma,\delta]$ de anéis noetherianos são também noetherianos, à direita ou à esquerda, será útil conhecermos o anel oposto R^{op}. Quando σ é um automorfismo, o próximo lema mostra que R^{op} é novamente uma extensão de Ore.

Lema 3.1.7. *Sejam A um anel e $R = A[X;\sigma,\delta]$ uma extensão de Ore de A. Se σ é inversível, então $R^{op} = A^{op}[X;\sigma^{-1}, -\delta \circ \sigma^{-1}]$ é uma extensão de Ore ed A^{op}.*

Demonstração. Como $\sigma \in Aut(A)$, segue que $\sigma^{-1}\colon A \to A$ é um morfismo de anéis, de onde $\sigma^{-1}\colon A^{op} \to A^{op}$ é um morfismo de anéis, ou seja, $\sigma^{-1} \in Aut(A^{op})$. Agora, como δ é uma σ-derivação, dados $a, b \in A^{op}$, temos

$$\begin{aligned}
-(\delta \circ \sigma^{-1})(a \bullet b) &= -\delta(\sigma^{-1}(ba)) \\
&= -\delta(\sigma^{-1}(b)\sigma^{-1}(a)) \\
&= -\delta(\sigma^{-1}(b))\sigma^{-1}(a) - \sigma(\sigma^{-1}(b))\delta(\sigma^{-1}(a)) \\
&= (-\delta \circ \sigma^{-1})(a) \bullet b + \sigma^{-1}(a) \bullet (-\delta \circ \sigma^{-1})(b).
\end{aligned}$$

Portanto, $-\delta \circ \sigma^{-1} \colon A^{op} \to A^{op}$ é uma σ^{-1}-derivação. Assim, existe a extensão de Ore $S = A^{op}[Y; \sigma^{-1}, -\delta \circ \sigma^{-1}]$. Considere a inclusão $j \colon A^{op} \to R^{op}$, definida por $j(a) = a$. Então j é um morfismo de anéis, pois $j(a \bullet b) = j(ba) = ba = a \bullet b = j(a) \bullet j(b)$. Ainda,

$$\begin{aligned} \sigma^{-1}(a) \bullet X - (\delta \circ \sigma^{-1})(a) &= X\sigma^{-1}(a) - (\delta \circ \sigma^{-1})(a) \\ &= [\sigma(\sigma^{-1}(a))X + \delta(\sigma^{-1}(a))] - (\delta \circ \sigma^{-1})(a) \\ &= aX \\ &= X \bullet a. \end{aligned}$$

Assim, segue da Propriedade Universal das Extensões de Ore que existe um único morfismo de anéis $j' \colon S \to R^{op}$ tal que $j'(a) = a$ e $j'(Y) = j(1_{A^{op}})X = X$.

Desta forma j' é uma bijeção. De fato, j leva a base $\{Y^n \colon n \in \mathbb{N}\}$ de S como A^{op}-módulo à esquerda na base $B = \{X^n \colon n \in \mathbb{N}\}$ de R como A-módulo à esquerda. Como σ é um automorfismo, segue da Proposição 1.3.9 que B é uma base para R como A-módulo à direita, ou ainda, como A^{op}-módulo à esquerda. Como j' é, em particular, um morfismo de A^{op}-módulos, segue que j' é uma bijeção. Identificando $X = Y$, temos que $S = R^{op}$ como conjuntos, de onde podemos considerar $R^{op} = S = A^{op}[X; \sigma^{-1}, -\delta \circ \sigma^{-1}]$. □

Na literatura, o *Teorema da Base de Hilbert* afirma que, se A é um anel noetheriano, à direita ou à esquerda, então o anel de polinômios usual $A[X]$ é noetheriano, à direita ou à esquerda, respectivamente. Em [11, Theorem 2.6] este resultado é generalizado para extensões de Ore $A[X; \sigma, \delta]$, onde σ é um automorfismo, e chamado de *Teorema da Skew-Base de Hilbert Generalizada.*

Teorema 3.1.8 (Base de Hilbert). *Sejam A um anel noetheriano à direita (esquerda) e $R = A[X; \sigma, \delta]$. Se $\sigma \in Aut(A)$, então R é um anel noetheriano à direita (esquerda).*

Demonstração. Esta demonstração será dividida em quatro (pequenas) partes: Na primeira parte, supomos que A_A é noetheriano e I é um ideal à direita de R, criaremos J, um ideal à direita de A. Em seguida, tomando geradores de J como A-módulo, definiremos I_0, um ideal à direita finitamente gerado de R. Na terceira parte, mostraremos que $I = I_0$, de onde seguirá que todo ideal à direita de R é finitamente gerado, e portanto R_R é noetheriano. Por fim, utilizaremos o anel oposto para concluir o enunciado para anéis noetherianos à esquerda.

Parte 1. Suponha que A é um anel noetheriano à direita e sejam $I \neq 0$ um ideal à direita de R e $p \in I \setminus \{0\}$. Então, podemos escrever p, de maneira única, como $p = \sum_{i=0}^{n} a_i X^i$, onde $a_n \neq 0$. Neste caso, denotamos por $\deg(p) = n$ o grau de p, por $cl(p) = a_n$ o coeficiente livre de p, e

$$p = a_n X^n + \mathcal{O}(X^{n-1}).$$

Seja $J = \{cl(p) \colon p \in I \setminus \{0\}\} \cup \{0\}$. Vamos mostrar que J é um ideal à direita de A. Se $a, b \in J$, então existem $p, q \in I$ tais que $a = cl(p)$ e $b = cl(q)$. Sejam $n = \deg(p)$ e $m = deg(q)$. Suponha sem perda de generalidade que $n \leq m$. Então,

$$pX^{m-n} + q = \left(aX^n + \mathcal{O}(X^{n-1})\right) X^{m-n} + (bX^m + \mathcal{O}(X^{m-1})) = (a+b)X^m + \mathcal{O}(X^{m-1}).$$

Como $p, q \in I$ e I é um ideal à direita de R, $pX^{m-n} + q \in I$. Logo $a + b = cl(pX^{m-n} + q) \in J$. Seja $r \in A$. Se $ar = 0$, então $ar \in J$. Caso contrário, temos

$$p\sigma^{-n}(r) = aX^n\sigma^{-n}(r) + \mathcal{O}(X^{n-1})$$

$$
\begin{aligned}
&= a\left(\sigma^n(\sigma^{-n}(r))X^n + \mathcal{O}(X^{n-1})\right) + \mathcal{O}(X^{n-1}) && 1.3.6\\
&= arX^n + \mathcal{O}(X^{n-1}).
\end{aligned}
$$

Como $ar \neq 0$, segue que $cl(p\sigma^{-n}(r)) = ar \in J$. Assim, J é um ideal à direita de A.

Parte 2. Como A é um anel noetheriano à direita, segue que J é finitamente gerado como A-módulo à direita. Sejam $a_1, \dots, a_k \in J$ tais que $J = \sum_{i=1}^{k} a_i A$. Então existem $p_1, \dots, p_k \in I$ tais que $cl(p_i) = a_i$, para cada $i = 1, \dots, k$. Vamos mostrar que podemos escolher $p_i \in I$ todos com mesmo grau. De fato, sejam $n_i = \deg(p_i)$ e $n = \max\{n_1, \dots, n_k\}$. Então

$$
p_i X^{n-n_i} = \left(a_i X^{n_i} + \mathcal{O}(X^{n_i-1})\right) X^{n-n_i} = a_i X^n + \mathcal{O}(X^{n-1}).
$$

Ou seja, $p_i X^{n-n_i} \in I$, $\deg(p_i X^{n-n_i}) = n$ e $cl(p_i X^{n-n_i}) = cl(p_i) = a_i$. Assim, podemos assumir $\deg(p_i) = n$. Seja $N = \sum_{i=0}^{n-1} X^i A \subseteq R$, então N é um A-módulo à direita finitamente gerado. Pelo Lema 3.1.6 temos que N é noetheriano, de onde $I \cap N \subseteq N$ é um A-submódulo finitamente gerado de N. Dados $q_1, \dots, q_t \in I \cap N$ um conjunto gerador de $I \cap N$ como A-módulo à direita, defina $I_0 = \sum_{i=1}^{k} p_i R + \sum_{i=1}^{t} q_i R$. Então I_0 é um R-módulo à direita finitamente gerado, e valem

$$
I \cap N = \sum_{i=1}^{t} q_i A \subseteq \sum_{i=1}^{t} q_i R \subseteq I_0 = \sum_{i=1}^{k} p_i R + \sum_{i=1}^{t} q_i R \subseteq I,
$$

onde a última contenção segue de $p_i, q_i \in I$ e I ser um ideal à direita de R.

Parte 3. Vamos mostrar que $I_0 = I$. Para isso, utilizaremos indução em $\deg(p)$, $p \in I$. Se $\deg(p) < n$, então, pela definição de N, temos $p \in I \cap N \subseteq I_0$. Seja $p \in I$ tal que $\deg(p) = m \geq n$ e suponha que, para todo $q \in I$ com $\deg(q) < m$, vale $q \in I_0$. Escreva $p = rX^m + \mathcal{O}(X^{m-1}) \in I$, então $r = cl(p) \in J$, de onde $r = \sum_{i=1}^{k} a_i r_i$, $r_i \in A$. Seja

$$
\begin{aligned}
q &= \sum_{i=1}^{k} p_i \sigma^{-n}(r_i) X^{m-n}\\
&= \sum_{i=1}^{k} \left(a_i X^n + \mathcal{O}(X^{n-1})\right) \sigma^{-n}(r_i) X^{m-n}\\
&= \sum_{i=1}^{k} a_i X^n \sigma^{-n}(r_i) X^{m-n} + \mathcal{O}(X^{m-1})\\
&= \sum_{i=1}^{k} a_i \left(r_i X^n + \mathcal{O}(X^{n-1})\right) X^{m-n} + \mathcal{O}(X^{m-1})\\
&= \left(\sum_{i=1}^{k} a_i r_i\right) X^m + \mathcal{O}(X^{m-1})\\
&= rX^m + \mathcal{O}(X^{m-1}).
\end{aligned}
$$

Então $\deg(q) = m$, $cl(q) = r$ e $q \in I_0$, pois $p_1, \dots, p_k \in I_0$ e I_0 é um R-módulo à direita. Com isso, obtemos $\deg(p - q) < m$, logo, pela hipótese de indução, $p - q \in I_0$. Portanto $p = (p - q) + q \in I_0$. Logo $I = I_0$ e I é finitamente gerado como R-módulo à direita. Isso conclui que R é noetheriano à direita.

Parte 4. Suponha que A é um anel noetheriano à esquerda, então A^{op} é um anel noetheriano à direita. Utilizando do Lema 3.1.7, segue que $R^{op} = A^{op}[X; \sigma^{-1}, -\delta \circ \sigma^{-1}]$ é um anel noetheriano à direita. Portanto $R = (R^{op})^{op}$ é um anel noetheriano à esquerda. $\square$

Tendo em vista a Proposição 3.1.5, o teorema acima mostra que, se H é uma álgebra de Hopf fraca que é um anel noetheriano, à direita ou à esquerda, então as extensões de Hopf-Ore (g, h)-primitivas fracas de H - e também das extensões de Ore de H - correspondem a extensões de Hopf-Ore $(r, 1_H)$-primitivas fracas, e são relevantes para sua caracterização apenas os elementos group-like fracos inversíveis. Em particular, podemos construir iteradas $R_{n+1} = R_n[X_n; \sigma_n, \delta_n] = H[X_0; \sigma_0, \delta_0][X_1; \sigma_1, \delta_1] \dots [X_n; \sigma_n, \delta_n]$ de extensões de Hopf-Ore primitivas fracas utilizando o Teorema 2.4.8.

Por outro lado, ressaltamos que, até o presente momento, é desconhecido para o autor qualquer exemplo de álgebra de Hopf fraca que não seja Dedekind-finita. A condição $\Delta(1)(g \otimes g) = (g \otimes g)\Delta(1)$ não aparenta implicar $gt = tg$, para todo $t \in H_t$, mas, se isto ocorre e $g \in G_w(H)$ é inversível à esquerda, então

$$g\epsilon_s(g) = g = \epsilon_t(g)g = g\epsilon_t(g) \implies \epsilon_s(g) = 1_H = \epsilon_t(g),$$

de onde g é inversível. O exemplo clássico de uma álgebra que não é Dedekind-finita é a k-subálgebra de $End_k(V)$, onde V é um k-módulo livre com base $\{e_i \colon i \in \mathbb{N}\}$, gerada pelos morfismos $h, g \in End_k(V)$, definidos por $h(e_i) = e_{i+1}$, para todo $i \in \mathbb{N}$, $g(e_1) = 0$ e $g(e_i) = e_{i-1}$, se $i \geq 2$. Nesse caso, $gh = id_V$, mas $hg = id_V - p_1 \neq id_V$, onde $p_1(e_i) = [i = 1]e_1$ é a projeção linear em ke_1.

Vamos terminar esta seção observando que endomorfismos vindos de caracteres à esquerda fracos de uma extensão de Hopf-Ore primitiva fraca, mesmo em casos razoavelmente simples, podem ser bastante complexos.

Sejam $k = \mathbb{C}$, $G = \{e, g, \dots, g^{r-1}\}$ e $n > 1$. Considere $H = kG \otimes M_n(k) \simeq M_n(kG)$, via $g \otimes e_{ij} \mapsto ge_{ij}$, com a estrutura do Exemplo 1.4.4(3) e $q_r = e^{2i\pi/r} \in \mathbb{C}$. Então $\rho(g) = q_r$ define um morfismo de grupos $G \to \mathbb{C} \setminus \{0\}$. Utilizando o Exemplo 2.4.2 e a classificação das extensões de Hopf-Ore de kG - [20, Proposition 2.2] ou Corolário 3.3.15 - obtemos que $R = H[X; \sigma]$ é uma extensão de Hopf-Ore $(g, 1_H)$-primitiva fraca de H, onde

$$Xg^te_{ij} = \sigma(g^te_{ij})X = q_r^tg^te_{ij}X, \quad \forall i, j = 1, \dots, n, \ t = 0, \dots, r-1.$$

Utilizando-se *coeficientes q-binomiais* [21, Section 7.2] e técnica semelhante àquelas que serão utilizadas no Lema 3.3.10, podemos mostrar que, se $\chi \in X_w^l(R)$, então

$$\tau_\chi^l(g^te_{ij}X^m) = \sum_{s=0}^{m} \left[\binom{m}{s}_{q_r} \chi(g^{ms-s^2-t}e_{ij})C^s \right] g^te_{ij}X^{m-s},$$

onde $\chi|_H \in X_w^l(H)$ e $C = \chi(e_{11}X) \in \mathbb{C}$.

3.2 WHA's de unidade sobrejetora

Nesta seção vamos apresentar a caracterização das álgebras de Hopf fracas de unidade sobrejetora, obtida durante a tentativa de encontrar exemplos de álgebras de Hopf fracas satisfazendo (1)-(4) da Proposição 1.4.11, mas com $\epsilon(1_H) \neq 1_k$. Como corolário, mostramos que todo idempotente não trivial define uma estrutura de álgebra de Hopf fraca e classificaremos as álgebras de Hopf fracas da forma $\mathbb{Z}_n$, vistas como álgebras sobre $\mathbb{Z}_m$. As referências para os resultados da teoria de anéis utilizados nesta seção são [1] e [15].

Proposição 3.2.1. *Sejam k um anel comutativo e (H, μ, u) uma álgebra sobre k, onde u é sobrejetora. Então H admite uma estrutura de álgebra de Hopf fraca sobre k se, e somente se, $\Delta(1_H) = 1_H \otimes 1_H$, $S = id_H$ e $\epsilon(1_H) = x$, onde $x \in k$ é um idempotente satisfazendo $u(x) = 1_H$ e $ker(u)x = 0$. Em particular, temos que $ker(u) = k(1_k - x)$ e $H \simeq kx$, como anéis.*

Demonstração. De forma geral, como $H = im(u) \subseteq Z(H)$, segue que H é um anel comutativo. Como u é sobrejetora, dado $a \in H$, existe $a' \in k$ tal que $a = u(a')$. Desta forma, dado $M \in \mathfrak{M}_k$, temos que $f\colon H \to M$ é um morfismo de k-módulos se, e somente se, $f(a) = f(u(a')1_H) = a'f(1_H)$. Assim, todo morfismo fica completamente determinado por $f(1_H)$, e está bem determinado se, e somente se, $ker(u)$ anula $f(1_H)$.

Suponha que H admite uma estrutura de álgebra de Hopf fraca sobre k. Sejam $a_i, b_i \in H$ tais que $\Delta(1_H) = \sum_i a_i \otimes b_i$ e $b'_i \in k$ tais que $b_i = u(b'_i)$. Como o produto tensorial é k-bilinear, temos que

$$\Delta(1_H) = \sum_i a_i \otimes b_i = \sum_i a_i \otimes u(b'_i)1_H = \sum_i a_i u(b'_i) \otimes 1_H = \left(\sum_i a_i b_i\right) \otimes 1_H.$$

Denote $e = \sum_i a_i b_i \in H$. Como Δ é multiplicativa, temos

$$e \otimes 1_H = \Delta(1_H) = \Delta(1_H)^2 = e^2 \otimes 1_H.$$

Aplicando μ à igualdade acima, obtemos que $e = e^2$ é um idempotente, portanto vale $(1_H - e)e = 0$. Com isso, $\Delta(1_H - e) = (1_H - e)e \otimes 1_H = 0$. Segue do axioma da counidade que $1_H - e = 0$, ou seja, $e = 1_H$ e $\Delta(1_H) = 1_H \otimes 1_H$. Assim, vale a equivalência da Proposição 1.4.11. Em particular, temos que ϵ deve ser um morfismo multiplicativo, de onde $x := \epsilon(1_H) \in k$ deve ser um idempotente. Pelo axioma da counidade, temos que

$$1_H = (u\epsilon * id_H)(1_H) = u\epsilon(1_H)1_H = u(x),$$

e, como $\epsilon\colon H \to k$ é um morfismo de módulos, $ker(u)x = ker(u)\epsilon(1_H) = \epsilon(u(ker(u))) = 0$. Logo, $x \in k$ é um idempotente satisfazendo $u(x) = 1_H$ e $ker(u)x = 0$. Por fim, pela Proposição 1.4.11, temos que $S * id_H = u\epsilon$, portanto

$$1_H = u(x) = u\epsilon(1_H) = (S * id_H)(1_H) = S(1_H)1_H = S(1_H).$$

Assim, $S(a) = S(u(a')) = u(a')S(1_H) = u(a')1_H = a$, para todo $a \in H$. Isso mostra a primeira implicação do enunciado.

Por outro lado, suponha que $x \in k$ é um idempotente satisfazendo $u(x) = 1_H$ e $ker(u)x = 0$. Considere o morfismo $\Delta\colon H \to H \otimes H$, dado por $\Delta(a) = a \otimes 1_H$. Então Δ é um morfismo bem definido, é coassociativo, pois

$$(\Delta \otimes id_H)(\Delta(a)) = a \otimes 1_H \otimes 1_H = (id_H \otimes \Delta)(\Delta(a)),$$

é multiplicativo, pois, dados $a, b \in H$, temos que

$$\Delta(a)\Delta(b) = (a \otimes 1_H)(b \otimes 1_H) = ab \otimes 1_H = \Delta(ab),$$

e satisfaz a identidade em 1.4.3(W3), pois, neste caso, todos os termos são $1_H \otimes 1_H \otimes 1_H$.

Agora, dado $a \in H$, seja $a' \in k$ tal que $u(a') = a$. Considere a função $\epsilon\colon H \to k$, dada por $\epsilon(a) = a'x$. Então ϵ está bem definida, pois, se $a = u(a') = u(a'')$, então $a'' - a' \in ker(u)$, de onde $(a'' - a')x \in ker(u)x = 0$, ou ainda, $a''x = a'x$. Desta forma, a função ϵ é um morfismo de k-módulos, pois, dados $a \in H$ e $b \in k$, temos $u(ba') = u(b)a$, de onde podemos considerar $(u(b)a)' = ba'$. Com isso, calculamos $\epsilon(u(b)a) = (ba')x = b(a'x) = b\epsilon(a)$. O morfismo $\epsilon\colon H \to k$ satisfaz (W4), pois, como $u(1_k) = 1_H$, temos

$$\epsilon(abc) = a'b'c'x = (a'b'x)(1_k c'x) = \epsilon(ab)\epsilon(1_H c) = \epsilon(ab_1)\epsilon(b_2 c),$$

e, analogamente, $\epsilon(abc) = (a'1_k x)(b'c'x) = \epsilon(ab_2)\epsilon(b_1 c)$. A tripla (H, Δ, ϵ) satisfaz o axioma da counidade, pois $(u\epsilon * id_H)(a) = u\epsilon(a)1_H = u(a'x) = au(x) = a$, onde, na última igualdade, utilizamos que $u(x) = 1_H$. Analogamente, mostra-se a identidade $(id_H * u\epsilon)(a) = 1_H u\epsilon(a) = a$. Com isso, (H, Δ, ϵ) é uma coálgebra. Logo vale (W2). Por fim, considerando $S\colon H \to H$ o morfismo identidade, temos que

$$(S * id_H * S)(a) = S(a)1_H S(1_H) = a = S(a),$$
$$u\epsilon(1_1 a)1_2 = u\epsilon(1_H a)1_H = u\epsilon(a) = a = S(a)1_H = (S * id_H)(a),$$

e

$$1_1 u\epsilon(a1_2) = 1_H u\epsilon(a1_H) = u\epsilon(a) = aS(1_H)a = (id_H * S)(a),$$

de onde vale (W5). Assim, H é uma álgebra de Hopf fraca com morfismos definidos por $\Delta(1_H) = 1_H \otimes 1_H$, $S = id_H$ e $\epsilon(1_H) = x$.

Por fim, note que, como $u(x) = 1_H = u(1_k)$, temos que $1_k - x \in ker(u)$. Como u é um morfismo de k-módulos, $k(1_k - x) \subseteq ker(u)$. Por outro lado, para que $\epsilon\colon H \to k$ seja um morfismo bem definido, deve valer $ker(u)\epsilon(a) = \epsilon(u(\ker(u))a) = 0$, para todo $a \in H$. Em particular, temos que $0 = ker(u)\epsilon(1_H) = ker(u)x$. Seja $r \in ker(u)$, então $rx = 0$, de onde

$$r = r(x + (1_k - x)) = rx + r(1_k - x) = r(1_k - x).$$

Portanto $r \in k(1_k - x)$. Ou seja, $k(1_k - x) \subseteq ker(u) \subseteq k(1_k - x)$. Isso mostra que $ker(u) = k(1_k - x)$. Consequentemente, a restrição $u|_{kx}\colon kx \subseteq k \to H$ é injetora. Como u é sobrejetora, dado $a \in H$ e $a' \in k$ tal que $u(a') = a$, temos que $a'x \in kx$ e

$$u(a'x) = u(a'x) + u(a'(1_k - x)) = u(a') = a.$$

Portanto a restrição $u|_{kx}$ é também sobrejetora e $H \simeq kx$, como anéis. □

Nas condições da proposição anterior, temos que H é uma álgebra de Hopf (conforme Definição 1.4.1) se, e somente se, $x = \epsilon(1_H) = 1_k$ se, e somente se, $ker(u) = k(1_k - 1_k) = 0$ se, e somente se, $H \simeq k$ como anéis, e portanto como álgebras de Hopf. Em particular, se k é um corpo (ou não possui idempotentes não triviais), então a única estrutura de álgebra de Hopf fraca em H ocorre quando $H \simeq k$, e nesse caso H é uma álgebra de Hopf. Assim, somente conseguimos utilizar a proposição acima para obter exemplos de álgebras de Hopf fracas que não são algebras de Hopf no contexto de álgebras sobre anéis comutativos.

Corolário 3.2.2. *Sejam k um anel comutativo, $e \in k$ um idempotente e $I = k(1 - e)$ o ideal gerado por $1 - e$. Então $H = k/I$ possui uma estrutura de álgebra de Hopf fraca sobre k, com $\epsilon(1_H) = e$.*

Demonstração. O morfismo quociente $u = \pi\colon k \to k/I$ é um morfismo de anéis com núcleo $ker(u) = I = k(1-e)$. Por hipótese, $e \in k$ é um idempotente, de onde

$$ker(u)e = k(1-e)e = 0 \quad \text{e} \quad u(e) = u(e) + u(1-e) = u(1) = 1_{k/I}.$$

Segue da Proposição 3.2.1 que $H = k/I$ possui uma estrutura de álgebra de Hopf fraca, definida por $\Delta(a) = a \otimes 1_H$, $\epsilon(a) = ae$ e $S \equiv id_H$, para todo $a \in H$. □

Definição 3.2.3. Sejam R um anel e $I, J \subsetneq R$ ideais bilaterais de R.

(i) Se R é comutativo, dizemos que I é um **ideal primário** se, para $a, b \in R$,

$$ab \in I, a \notin I \implies \exists n \in \mathbb{N}\colon b^n \in I.$$

(ii) Dizemos que I e J são **ideais comaximais** se $I + J = R$.

Sejam P é um ideal primário de R e $a, b \in R$ tais que $ab + P = (a+P)(b+P) = P$, mas $a + P \neq P$. Então $ab \in P$ e $a \notin P$, de onde existe $n \in \mathbb{N}$ tal que $b^n \in P$, logo $(b+P)^n = b^n + P = P$. Ou seja, se P é ideal primário, os divisores de zero não nulos de R/P são nilpotentes. Em particular, R/P não possui elementos idempotentes não triviais, pois todo elemento idempotente não trivial é divisor de zero - $x \neq 0, 1$ e $x^2 = x$ implicam $x(1-x) = 0$ com $x, 1-x \neq 0$ - e, nesse caso, $x + P = x^n + P = (x+P)^n = P$.

Lema 3.2.4 (Teorema do Homomorfismo para Anéis)**.** *Sejam $f\colon R \to S$ um morfismo de anéis e I um ideal de R. Se $I \subseteq ker(f)$, então existe um único morfismo de anéis $\overline{f}\colon R/I \to S$ tal que $f = \overline{f} \circ \pi$, onde $\pi\colon R \to R/I$ denota o morfismo quociente.*

Demonstração. Um morfismo de anéis $f\colon R \to S$ é, em particular, um morfismo de grupos abelianos $(R, +) \to (S, +)$, e um ideal I de R é, em particular, um subgrupo (normal) de $(R, +)$. Como $I \subseteq ker(f)$, podemos aplicar o Teorema do Homomorfismo para Grupos, obtendo que existe um único morfismo de grupos $\overline{f}\colon (R/I, +) \to (S, +)$ tal que $f = \overline{f} \circ \pi$. Resta verificar que $\overline{f}$ é um morfismo de anéis. Para $x \in R$, denote $\pi(x) = x + I \in A/I$. Então, dados $a, b \in R$, temos

$$\overline{f}((a+I)(b+I)) = \overline{f}(ab+I) = f(ab) = f(a)f(b) = \overline{f}(a+I)\overline{f}(b+I),$$

de onde $\overline{f}$ é multiplicativo, e $\overline{f}(1_{A/I}) = \overline{f}(1_A + I) = f(1_A) = 1_B$, de onde $\overline{f}$ é unitário. □

No contexto do lema acima, se $I = ker(f)$, então $\overline{f}$ é injetora, pois $a + ker(f) \in ker(\overline{f})$ se, e somente se, $0 = \overline{f}(a + ker(f)) = f(a)$ se, e somente se, $a \in ker(f)$ se, e somente se, $a + ker(f) = ker(f)$. Logo, se $f\colon A \to B$ é um morfismo de anéis sobrejetor, $\overline{f}\colon A/ker(f) \to B$ é um isomorfismo de anéis.

Proposição 3.2.5 (Teorema do Resto Chinês)**.** *Sejam R um anel, I e J ideais bilaterais de R. Se I e J são comaximais, então $R/(I \cap J) \simeq R/I \times R/J$ como anéis.*

Demonstração. Dados $x, a \in R$, vamos denotar

$$x \equiv a \pmod{I} \iff x - a \in I \iff x + I = a + I \in R/I.$$

Considere a função $f\colon R \to R/I \times R/J$, definida por $f(r) = (r + I, r + J)$. Então f é um morfismo de anéis. A aplicação f é sobrejetora se, e somente se, para quaisquer $a, b \in R$, existe $x \in R$ satisfazendo

$$x \equiv a \ (mod\ I) \quad \text{e} \quad x \equiv b \ (mod\ J).$$

Como $I + J = R$, existem $e \in I$ e $f \in R$ tais que $e + f = 1$. Defina $x = af + be$, então

$$x \equiv af + be \equiv af \equiv af + ae \equiv a(f + e) \equiv a \quad (mod\ I)$$

e, analogamente, $x \equiv b\ (mod\ J)$. Portanto f é sobrejetora e, pelo Teorema do Homomorfismo para Anéis, obtemos que $g\colon R/ker(f) \to R/I \times R/J$, dada por $g(r+ker(f)) = f(r)$, é um isomorfismo. Por fim, note que $r \in ker(f)$ se, e somente se, $(r + I, r + J) = (0 + I, 0 + J)$ se, e somente se, $r \in I$ e $r \in J$. Ou seja, $ker(f) = I \cap J$, de onde segue o resultado. □

Utilizando a proposição acima, se I e J são ideais comaximais, um elemento $x \in R/(I \cap J)$ é idempotente se, e somente se, $(x + I, x + J) \in R/I \times R/J$ é um idempotente se, e somente se, $x+I \in R/I$ e $x+J \in R/J$ são idempotentes. Em particular, se os ideais I e J são primários, então os idempotentes de $R/I \times R/J$ são $0 = (0, 0)$, $1 = (1, 1)$, $e = (1, 0)$ e $1 - e = (0, 1)$. Argumentando por indução, se $J = J_1 \cap \cdots \cap J_n$, onde cada J_i é um ideal primário e $J_i + J_j = R$, para quaisquer $i, j = 1, \dots, n$, então R/J possui 2^n idempotentes, os quais correspondem aos elementos da forma $(\delta_1, \dots, \delta_n) \in R/J_1 \times \cdots \times R/J_n$, onde $\delta_i \in \{0, 1\}$.

Corolário 3.2.6. *Sejam A um anel comutativo e $J_1, \dots, J_n$ ideais primários de A. Considere $k = A/J_1 \times \cdots \times A/J_n$ e $H = A/J_1 \times \cdots \times A/J_r$, para algum $r \in \{1, \dots, n\}$. Então H possui uma única estrutura de álgebra de Hopf fraca sobre k compatível com a projeção linear $u\colon k \to H$, dada por $(a_1 \dots, a_n) \mapsto (a_1, \dots, a_r)$.*

Demonstração. Pela observação anterior, os idempotentes de k são da forma $x = (\delta_1, \dots, \delta_n)$, onde $\delta_i \in \{0, 1\}$. Como $u\colon k \to H$ é a projeção linear nas r primeiras coordenadas de k, temos que $u(x) = 1_H$ se, e somente se,

$$(\delta_1, \dots, \delta_r) = u(x) = u(1) = (1, \dots, 1).$$

Ou seja, deve ser $x = (1, \dots, 1, \delta_{r+1}, \dots, \delta_n)$. Por outro lado, temos que

$$\begin{aligned} ker(u) &= \{(a_1, \dots, a_n)\colon (a_1, \dots, a_r) = 0\} \\ &= \{(0, \dots, 0, a_{r+1}, \dots, a_n)\colon a_{r+1}, \dots, a_n \in A\}, \end{aligned}$$

de onde, tomando $a_{r+1}, \dots, a_n = 1$, segue que

$$\begin{aligned} ker(u)x = 0 &\implies (0, \dots, 0, 1, \dots, 1)(1, \dots, 1, \delta_{r+1}, \dots, \delta_n) = 0 \\ &\implies (0, \dots, 0, \delta_{r+1}, \dots, \delta_n) = (0, \dots, 0) \\ &\implies \delta_{r+1} = \cdots = \delta_n = 0. \end{aligned}$$

Portanto, deve ser $x = (1, \dots, 1, 0, \dots, 0)$, com 1 nas r primeiras coordenadas. Logo, existe e é único o elemento $x \in k$ satisfazendo a Proposição 3.2.1. □

Por fim, vamos apresentar a classificação das estruturas de álgebra de Hopf fraca em $\mathbb{Z}_n$, vista como álgebra sobre $\mathbb{Z}_m$. Para fins de completude, vamos listar algumas definições e resultados clássicos sobre a estrutura de domínio de ideais principais de $\mathbb{Z}$, os quais podem ser encontrados em mais detalhes em [10].

Sejam $a, b, p \in \mathbb{Z}$, onde $p \neq \pm 1$. Dizemos que a **divide** b, e denotamos $a \mid b$, se existe $q \in \mathbb{N}$ tal que $b = aq$. O elemento p é dito **primo** se $p \mid ab$ implica $p \mid a$ ou $p \mid b$. Chamamos de **maior divisor comum** de a e b um elemento $d \in \mathbb{Z}_+$ tal que

$$(i)\ d \mid a \text{ e } d \mid b, \quad \text{e} \quad (ii)\ c \mid a \text{ e } c \mid b \implies c \mid d.$$

Mostra-se que dois elementos d e d' satisfazendo as duas condições acima são associados, ou seja, existe um elemento inversível $u \in \mathbb{Z}$ tal que $d' = ud$. Como $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$, a condição $d \geq 0$ garante a unicidade de d. Assim, podemos denotar $d = mdc(a, b)$. Por fim, os elementos a e b são ditos **coprimos** se $mdc(a, b) = 1$.

Vamos utilizar, sem demonstração: que $\mathbb{Z}$ é um domínio de ideais principais, ou seja, se I é um ideal de $\mathbb{Z}$, então existe $n \in \mathbb{Z}$ tal que $I = n\mathbb{Z}$; que todo elemento $n \in \mathbb{Z}$ admite uma fatoração única em elementos primos, $n = p_1^{e_1} \dots p_r^{e_r}$; e que os únicos divisores de um número primo p são ± 1 e $\pm p$. O primeiro resultado é consequência da existência do algoritmo de divisão euclidiana em $\mathbb{Z}$, o segundo é o Teorema Fundamental da Aritmética, e o último é uma aplicação direta da definição de elemento primo. Em termos de ideais, $b \in a\mathbb{Z}$ se, e somente se, $a \mid b$. Utilizaremos ainda o seguinte lema, o qual pode ser provado utilizando a definição de mdc, e o fato de $\mathbb{Z}$ ser um domínio de ideais principais.

Lema 3.2.7 (Identidade de Bézout)**.** *Sejam $a, b \in \mathbb{Z}$. Então $mdc(a, b) = 1$ se, e somente se, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.*

Como uma consequência do resultado acima, os ideais $I = a\mathbb{Z}$ e $J = b\mathbb{Z}$ de $\mathbb{Z}$ são comaximais se, e somente se, a e b são coprimos. A Identidade de Bézout mostra que, se $mdc(a, b) = 1$, então $1 \in a\mathbb{Z} + b\mathbb{Z}$, de onde $\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z} \subseteq \mathbb{Z}$. A outra implicação é análoga à demonstração do teorema: se $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$, então 1 é uma combinação linear de a e b, de onde $mdc(a, b) = 1$.

Seja $I = a\mathbb{Z}$ um ideal de $\mathbb{Z}$ e suponha que a é composto, com pelo menos dois fatores primos distintos. Então existe um número primo p tal que $a = p^n b$, onde $mdc(p, b) = 1$, mas $b \neq 1$. Então $p^n b = a \in I$, mas $p^n \notin I$ - pois não é divisível por b - e, para todo $m \in \mathbb{N}$, $b^m \notin I$ - pois não é divisível por p - ou seja, se a é composto com pelo menos dois fatores primos distintos, então $a\mathbb{Z}$ não é um ideal primário. Por contrapositiva, se um ideal I de $\mathbb{Z}$ é primário, então $I = p^n\mathbb{Z}$ para algum primo $p \in \mathbb{Z}$.

Reciprocamente, se $p \in \mathbb{Z}$ é um número primo e $n \in \mathbb{N}$, então $I = p^n\mathbb{Z}$ é um ideal primário. De fato, sejam $a, b \in \mathbb{Z}$ tais que $ab \in I$ mas $a \notin I$, então podemos escrever $a = p^e a'$ e $b = p^f b'$, onde $mdc(p, a') = mdc(p, b') = 1$. Como $ab = p^{e+f} a'b' \in I$ temos que $e + f \geq n$, mas $a \notin I$ implica em $e < n$. Logo, deve ser $f \geq 1$, portanto

$$b^n = p^{nf} b'^n = p^n \cdot p^{n(f-1)} b'^n \in I.$$

Ou seja, um ideal $a\mathbb{Z}$ de $\mathbb{Z}$ é primário se, e somente se, $a = p^n$, para algum primo $p \in \mathbb{Z}$ e $n \in \mathbb{N}$. Por fim, vamos chamar de **menor múltiplo comum** de dois inteiros a e b, um número $m \in \mathbb{Z}_+$, satisfazendo

$$(i)\ a \mid m \text{ e } b \mid m, \quad \text{e} \quad (ii)\ a \mid m' \text{ e } b \mid m' \implies m \mid m'.$$

A existência de um menor múltiplo comum se dá pela existência e unicidade da fatoração em primos de qualquer número inteiro, e a unicidade é análoga à unicidade do maior divisor comum. Mais precisamente, denotaremos $mmc(a, b) = m = ab/mdc(a, b)$, onde, por /, entende-se tomar o complemento q de $mdc(a, b)$ na escrita $ab = mdc(a, b)q$. Em particular, se $mdc(a, b) = 1$, então $mmc(a, b) = ab/mdc(a, b) = ab$.

Sejam $a, b \in \mathbb{Z}$ e $m = mmc(a, b)$, então $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. De fato, se $n \in a\mathbb{Z} \cap b\mathbb{Z}$, então n é divisível por a e b. Por definição, n é divisível por m, logo $a\mathbb{Z} \cap b\mathbb{Z} \subseteq m\mathbb{Z}$. Por outro lado, se $n \in m\mathbb{Z}$, então $n = mn'$ para algum $n' \in \mathbb{Z}$. Mas m, por definição, é divisível por a e por b, ou seja, existem $m', m'' \in \mathbb{Z}$ tais que $n = am'n' = bm''n'$, de onde $n \in a\mathbb{Z} \cap b\mathbb{Z}$.

Corolário 3.2.8. *Sejam $n, m \in \mathbb{N}$. Então $\mathbb{Z}_n$ admite uma estrutura de álgebra de Hopf fraca sobre $\mathbb{Z}_m$ se, e somente se, $m = nr$, onde $mdc(n, r) = 1$. Nesse caso, a estrutura de álgebra de álgebra de Hopf fraca em $\mathbb{Z}_n$ é única.*

Demonstração. Se $m = nr$ com $mdc(n, r) = 1$, podemos escrever $n = p_1^{e_1} \dots p_s^{e_s}$ e $r = p_{s+1}^{e_{s+1}} \dots p_{s+j}^{e_{s+j}}$, notando que as escritas não possuem primos em comum, pois n e r não admitem divisores em comum. Como $mdc(p_i^{e_i}, p_j^{e_j}) = 1$, para todo $i \neq j$, e $m\mathbb{Z} = p_1^{e_1}\mathbb{Z} \cap \dots \cap p_{s+j}^{e_{s+j}}\mathbb{Z}$, podemos aplicar o Teorema do Resto Chinês $s + j - 1$ vezes, obtendo

$$\mathbb{Z}_m \simeq \mathbb{Z}_n \times \mathbb{Z}_r \simeq \left(\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{p_s^{e_s}\mathbb{Z}} \right) \times \left(\frac{\mathbb{Z}}{p_{s+1}^{e_{s+1}}\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{p_{s+j}^{e_{s+j}}\mathbb{Z}} \right).$$

Com isso, o morfismo unidade $\mathbb{Z}_m \to \mathbb{Z}_n \simeq \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{p_s^{e_s}\mathbb{Z}}$ é dado pela projeção linear nas s primeiras coordenadas de $\mathbb{Z}_m$. Segue do Corolário 3.2.2 que $\mathbb{Z}_n$ admite uma única estrutura de álgebra de Hopf fraca sobre $\mathbb{Z}_m$.

Reciprocamente, suponha que $\mathbb{Z}_n$ admite uma estrutura de álgebra de Hopf fraca sobre $\mathbb{Z}_m$. Então existe um morfismo de anéis unitários $u \colon \mathbb{Z}_m \to \mathbb{Z}_n$. Como $(\mathbb{Z}_m, +)$ e $(\mathbb{Z}_n, +)$ são grupos cíclicos gerados por 1 e $u \colon (\mathbb{Z}_m, +) \to (\mathbb{Z}_n, +)$ é um morfismo de grupos, segue que tal morfismo existe se, e somente se, $n = |\mathbb{Z}_n|$ divide $|\mathbb{Z}_m| = m$, ou seja, se $m = nr$, para algum $r \in \mathbb{N}$, e nesse caso temos $ker(u) = n\mathbb{Z}_{nr}$. Agora, pela Proposição 3.2.1, temos que $\mathbb{Z}_n$ admite uma estrutura de álgebra de Hopf fraca sobre $\mathbb{Z}_{nr}$ se, e somente se, existir $x \in \mathbb{Z}_{nr}$ tal que $x^2 = x$, $u(x) = 1_{\mathbb{Z}_n}$ e $ker(u)x = 0$. Nesse caso, temos que $1_{\mathbb{Z}_m} - x \in ker(u)$, de onde

$$1 - x \equiv ns \quad (mod\ nr) \iff 1 - x = ns + nrs' = n(s + rs'), \ s, s' \in \mathbb{Z},$$

ou seja, $x = 1 + ny$, para algum $y \in \mathbb{Z}$. Por outro lado, de $0 = ker(u)x = (n\mathbb{Z}_{nr})x$, temos

$$nx \equiv 0 \quad (mod\ nr) \iff nx = nrs, \ s \in \mathbb{Z} \overset{n \neq 0}{\iff} x = rs.$$

Igualando as duas escritas de x, segue que $1 + ny = x = rs$, ou ainda, $1 = rs - ny$. Pela Identidade de Bézout, obtemos que $mdc(n, r) = 1$. □

Apesar da demonstração acima ser existencial, mostramos que existe um elemento $x \in \mathbb{Z}_m$ satisfazendo as condições da Proposição 3.2.1 se, e somente se, $m = nr$ com $mdc(n, r) = 1$, e nesse caso $x = rs = 1 + ny$, onde $s, y \in \mathbb{Z}$ são tais que $1 = rs - ny$.

Por um lado, temos que a Identidade de Bézout não admite solução única, pois, se $1 = rs - ny$ e $q \in \mathbb{Z}$, então

$$1 = rs - ny = rs + rnq - rnq - ny = r(s + nq) - n(y + rq).$$

Por outro lado, se $1 = rs - ny = rs' - ny'$, então $r(s - s') = n(y - y')$. Como $mdc(r, n) = 1$ e n divide $r(s - s')$, segue que n deve dividir $s - s'$, de onde $s = s' + ns''$. Consequentemente,

$$rs \equiv r(s' + ns'') \equiv rs' + rns'' \equiv rs' \quad (mod\ nr).$$

Ou seja, $x \in \mathbb{Z}_{nr}$ fica completamente determinado pela classe de rs em $\mathbb{Z}_{nr}$, onde $s \in \mathbb{Z}$ é qualquer inteiro satisfazendo a identidade $1 = rs - ny$.

Exemplo 3.2.9. Tomando $n = 2$ e $r = 3$, como $mdc(2,3) = 1$, temos que $\mathbb{Z}_2$ admite uma única estrutura de álgebra de Hopf fraca sobre $\mathbb{Z}_6$. Mais ainda, de

$$1r - 1n = 3 - 2 = 1,$$

temos que $\epsilon(1_{\mathbb{Z}_2}) = 3 + 6\mathbb{Z}$, reobtendo o exemplo mencionado após a Proposição 1.4.11.

Exemplo 3.2.10. Sejam $n = 289 = 17^2$ e $r = 458 = 2 \cdot 229$, então $mdc(289, 458) = 1$. Vamos utilizar o algoritmo de Euclides para obter o elemento x que define a estrutura de álgebra de Hopf fraca de $\mathbb{Z}_{289}$ sobre $\mathbb{Z}_{289 \cdot 458} = \mathbb{Z}_{132362}$. Começamos calculando as divisões $r_i = r_{i+1}q_i + r_{i+2}$ e escrevendo na forma $r_{i+2} = r_i - r_{i+1}q_i$,

$$\begin{aligned}
458 &= 289 \cdot 1 + 169, & 169 &= 458 - 289 \cdot 1,\\
289 &= 169 \cdot 1 + 120, & 120 &= 289 - 169 \cdot 1,\\
169 &= 120 \cdot 1 + 49, & 49 &= 169 - 120 \cdot 1,\\
120 &= 49 \cdot 2 + 22, & 22 &= 120 - 49 \cdot 2,\\
49 &= 22 \cdot 2 + 5, & 5 &= 49 - 22 \cdot 2,\\
22 &= 5 \cdot 4 + 2, & 2 &= 22 - 5 \cdot 4,\\
5 &= 2 \cdot 2 + 1, & 1 &= 5 - 2 \cdot 2.
\end{aligned}$$

Substituindo recursivamente os restos obtidos na coluna à direita, obtemos

$$\begin{aligned}
1 &= 5 - 2 \cdot 2\\
&= 5 - (22 - 5 \cdot 4) \cdot 2 = 5 \cdot 9 - 22 \cdot 2\\
&= (49 - 22 \cdot 2) \cdot 9 - 22 \cdot 2 = 49 \cdot 9 - 22 \cdot 20\\
&= 49 \cdot 9 - (120 - 49 \cdot 2) \cdot 20 = 49 \cdot 49 - 120 \cdot 20\\
&= (169 - 120) \cdot 49 - 120 \cdot 20 = 169 \cdot 49 - 120 \cdot 69\\
&= 169 \cdot 49 - (289 - 169) \cdot 69 = 169 \cdot 118 - 289 \cdot 69\\
&= (458 - 289) \cdot 118 - 289 \cdot 69\\
&= 458 \cdot 118 - 289 \cdot 187,
\end{aligned}$$

de onde $x \equiv 458 \cdot 118 \equiv 54044 \in \mathbb{Z}_{132362}$. Pode-se verificar que, de fato, valem

$$\begin{gathered}
54044^2 - 54044 = 132362 \cdot 22066 \equiv 0 \cdot 22066 \ (mod\ 132362) \implies x^2 \equiv x,\\
54044 = 1 + 54043 = 1 + 187 \cdot 289 \equiv 1 \ (mod\ 289) \implies u(x) = 1_{\mathbb{Z}_{289}},\\
289n \cdot 54044 = 118n \cdot (289 \cdot 458) \equiv 118n \cdot 0 \ (mod\ 132362) \implies ker(u)x = 0.
\end{gathered}$$

Portanto, a única estrutura de álgebra de Hopf fraca de $\mathbb{Z}_{289}$ sobre $\mathbb{Z}_{132362}$ fica completamente determinada por $\Delta(a) = a \otimes 1$, $\epsilon(a) = 54044a$ e $S \equiv id_{\mathbb{Z}_{289}}$.

Por fim, observamos que, se H é uma álgebra de Hopf fraca sobre k, nas condições da Proposição 3.2.1, então $H[X]$, onde $\Delta(X) = X \otimes 1H_+ 1_H \otimes X$, é a única extensão de Hopf-Ore primitiva fraca de H. De fato, se $\sigma \in Aut_k(H)$ é um morfismo de anéis, então $\sigma(1_H) = 1_H$. Como H é gerado, como k-módulo, por 1_H, segue que $\sigma(a) = u\epsilon(a)\sigma(1) = u\epsilon(a) = a$, para todo $a \in H$, de onde $\sigma = id_H$. Analogamente, se $\delta \in End_k(H)$ é uma derivação, então $\delta(1_H) = 0$, de onde $\delta(a) = 0$, para todo $a \in H$. Por fim, os elementos group-like fracos de H são precisamente os idempotentes de H, mas o único idempotente inversível é 1_H. Portanto, a única escolha compatível com o Teorema 2.4.8 é $(\sigma, \delta, g) = (id_H, 0, 1_H)$, de onde $H[X; \sigma, \delta] = H[X]$ com X um elemento $(1_H, 1_H)$-primitivo fraco.

3.3 WHA's de grupóide conexo

Nesta seção, vamos apresentar um teorema de estrutura para grupóides conexos, a construção das álgebras de Hopf fracas de grupóide e a classificação das extensões de Hopf-Ore primitivas fracas de grupóides conexos. As referências para esta seção são [12] e [2], para os resultados sobre grupóides, [16], para a caracterização da álgebra de grupóide conexo e seus caracteres, e [20], para a classificação das extensões de Hopf-Ore das álgebras de grupo.

Definição 3.3.1. Seja $\mathcal{G}$ um conjunto não vazio e munido de uma operação parcialmente definida, denotada pela concatenação de símbolos, de forma que

(G1) Existe $(gh)l$ se, e somente se, existe $g(hl)$, e nesse caso $(gh)l = g(hl)$;

(G2) Existe $g(hl)$ se, e somente se, existem gh e hl.

Dizemos que um elemento $x \in \mathcal{G}$ é uma **identidade** se $\exists xg$ implica $xg = g$ e $\exists gx$ implica $gx = g$. Considere $\mathcal{G}^2$ o conjunto dos pares (g, h) tais que existe gh. Se, para todo $g \in \mathcal{G}$,

(G3) existem identidades $t(g)$ e $s(g)$, tais que $(t(g), g), (g, s(g)) \in \mathcal{G}^2$;

(G4) e existe $g^{-1} \in \mathcal{G}$, tal que existem e valem $gg^{-1} = t(g)$ e $g^{-1}g = s(g)$,

dizemos que $\mathcal{G}$ é um **grupóide**. Denotamos por $\mathcal{G}_0 = \{e \in \mathcal{G} \colon \exists g \in \mathcal{G}, e = s(g) = t(g^{-1})\}$ o conjunto das identidades de $\mathcal{G}$ associadas a algum elemento $g \in \mathcal{G}$.

Observamos que, na notação da definição acima, os elementos $t(g)$, $s(g)$ e g^{-1} são únicos. De fato, dado $g \in \mathcal{G}$, se x e y são identidades tais que $(x, g), (y, g) \in \mathcal{G}^2$, então $(y, xg) = (y, g) \in \mathcal{G}^2$, ou seja, existe $y(xg)$. Por (G2), existe yx. Como x e y são identidades, segue que $x = yx = y$. Logo $t(g)$ é unicamente determinado. Analogamente, se x e y são identidades tais que $(g, x), (g, y) \in \mathcal{G}^2$, então existe xy e portanto $x = xy = y$. Logo $s(g)$ é unicamente determinado. Por fim, se $h, h' \in \mathcal{G}$ satisfazem (G4), então existem hg e gh'. Por (G1), existem $ht(g) = h(gh') = (hg)h' = s(g)h'$ e, como $s(g)$ e $t(g)$ são identidades, obtemos que

$$h = ht(g) = s(g)h' = h'.$$

Logo g^{-1} é unicamente determinado.

Para o restante desta seção, $\mathcal{G}$ denotará um grupóide.

Exemplo 3.3.2. São exemplos de grupóides:

(1) Todo grupo G é um grupóide. Nesse caso, todos os produtos existem, a operação é associativa e, para todo $g \in G$, $s(g) = t(g) = e_G$ é o elemento neutro de G, de forma que $gg^{-1} = e_G = g^{-1}g$, onde g^{-1} denota o inverso usual de $g \in G$.

(2) Seja $\{G_i \colon i \in I\}$ uma família de grupóides. Então $\coprod_{i \in I} G_i = \{(g, i) \colon i \in I, g \in G_i\}$ admite uma estrutura de grupóide, onde existe $(g, i)(h, j)$ se, e somente se, $i = j$ e existe $gh \in G_i$, e nesse caso $(g, i)(h, i) = (gh, i)$. Assim, para cada $(g, i) \in \coprod_{i \in I} G_i$ temos $s((g, i)) = (s_i(g), i)$ e $t((g, i)) = (t_i(g), i)$, e $(g, i)^{-1} = (g^{-1}, i)$. Em particular, se G_1 e G_2 são grupos, então $\coprod_{i=1,2} G_i$ é um grupóide que não é um grupo.

(3) Sejam X um conjunto e $\mathcal{G}$ o conjunto das bijeções $f\colon A \to B$, onde $A, B \subseteq X$. Então $\mathcal{G}$ possui uma estrutura de grupóide, onde existe fg se, e somente se, $dom(g) = im(f)$, e nesse caso $fg = f \circ g$. Para cada $f\colon A \to B$, $s(f) = id_A$ e $t(f) = id_B$. Ainda, como $f\colon A \to B$ é bijeção, existe a função inversa $f^{-1}\colon B \to A$. Neste exemplo, $\mathcal{G}$ é um grupo se, e somente se, $X = \emptyset$. Nesse caso $\mathcal{G} = \{id\colon \emptyset \to \emptyset\}$.

(4) Sejam A um anel, $M \in {}_A\mathfrak{M}$ um módulo à esquerda de A e $\mathcal{G}$ o conjunto dos isomorfismos de módulos $f\colon N \to N'$, onde N e N' são submódulos de M. Então $\mathcal{G}$ possui uma estrutura de grupóide, com a operação definida de forma análoga ao exemplo (3). Nesse caso, todo isomorfismo $f\colon N \to N'$ é, em particular, uma bijeção, de onde existe a função inversa $f^{-1}\colon N' \to N$, a qual é um isomorfismo de módulos.

(5) Seja I um conjunto. Então $\mathcal{G}(I) = I \times I$ possui uma estrutura de grupóide, onde existe $(i,j)(r,s)$ se, e somente se, $j = r$, e nesse caso $(i,j)(r,s) = (i,s)$. Assim, $s((i,j)) = (j,j)$, $t((i,j)) = (i,i)$ e $(i,j)^{-1} = (j,i)$.

(6) Sejam $\mathcal{G}$ e $\mathcal{H}$ grupóides. Então $\mathcal{G} \times \mathcal{H}$ possui uma estrutura de grupóide, onde existe $(g,h)(g',h')$ se, e somente se, existem $gg' \in \mathcal{G}$ e $hh' \in \mathcal{H}$, e nesse caso $(g,h)(g',h') = (gg', hh')$. Assim, $s((g,h)) = (s(g), s(h))$, $t((g,h)) = (t(g), t(h))$ e $(g,h)^{-1} = (g^{-1}, h^{-1})$.

Vamos demonstrar algumas propriedades necessárias para o cálculo em grupóides.

Proposição 3.3.3. *Sejam $g, h \in \mathcal{G}$. Então:*

(i) $(g,h) \in \mathcal{G}^2$ *se, e somente se,* $s(g) = t(h)$*;*

(ii) Valem $s(gh) = s(h)$, $t(gh) = t(g)$, $s(g) = t(g^{-1})$, $t(g) = s(g^{-1})$ *e* $(g^{-1})^{-1} = g$*;*

(iii) Existe gh *se, e somente se, existe* $h^{-1}g^{-1}$*. Nesse caso* $(gh)^{-1} = h^{-1}g^{-1}$*;*

(iv) $e \in \mathcal{G}_0$ *se, e somente se,* $e = s(e) = t(e)$*;*

(v) Seja $e \in \mathcal{G}_0$*. O conjunto* $G_e = \{g \in \mathcal{G} : e = s(g) = t(g)\}$ *é um grupo.*

Demonstração. (i) Suponha $s(g) = t(h)$, então existem $gs(g)$ e $t(h)h = s(h)h$. Por (G2), existe $g(s(g)h) = g(t(h)h) = gh$. Reciprocamente, suponha que existe gh. Como existe $g^{-1}g$, segue de (G2) que existe (g^{-1}, gh). Com isso, temos

$$g^{-1}(gh) \overset{(G1)}{=} (g^{-1}g)h \overset{(G4)}{=} s(g)h.$$

Como $s(g)$ é um identidade e $(s(g), h) \in \mathcal{G}^2$, segue da unicidade da identidade à esquerda de h que $s(g) = t(h)$.

(ii) Por (G4), existe gg^{-1} e $g^{-1}g$. Pelo item (i) segue que $s(g) = t(g^{-1})$ e $t(g) = s(g^{-1})$. Assim, se existe gh, por (G2) existe $(gh)h^{-1}$. Segue de (i) que $s(gh) = t(h^{-1}) = s(h)$. Ainda, existe $g^{-1}(gh)$, logo $t(gh) = s(g^{-1}) = t(g)$. Consequentemente temos que $gg^{-1} = t(g) = s(g^{-1})$ e $g^{-1}g = s(g) = t(g^{-1})$. Assim, segue da unicidade do elemento satisfazendo (G4) que $(g^{-1})^{-1} = g$.

(iii) Suponha que existe gh. Utilizando (i) e (ii) obtemos $t(g^{-1}) = s(g) = t(h) = s(h^{-1})$, portanto existe $h^{-1}g^{-1}$. A recíproca é análoga. Nesse caso, como existem gh,

hh^{-1}, $g^{-1}g$ e $h^{-1}g^{-1}$, obtemos de (G2) que existem $((gh)h^{-1})g^{-1}$ e $h^{-1}(g^{-1}(gh))$. Mais ainda, valem

$$\begin{aligned}
(gh)(h^{-1}g^{-1}) &= ((gh)h^{-1})g^{-1} && (G1)\\
&= (g(hh^{-1}))g^{-1} && (G1)\\
&= (gt(h))g^{-1} && (G4)\\
&= (gs(g))g^{-1} && (i)\\
&= gg^{-1} && (G3)\\
&= t(g) && (G4)\\
&= t(gh). && (ii)
\end{aligned}$$

Analogamente, mostra-se $(h^{-1}g^{-1})(gh) = s(gh)$. Pela unicidade do elemento satisfazendo (G4) segue que $(gh)^{-1} = h^{-1}g^{-1}$.

(iv) Se $e \in \mathcal{G}_0$, então existe $g \in \mathcal{G}$ tal que $e = s(g) = t(g^{-1})$. Assim, $(g, e) = (g, s(g)) \in \mathcal{G}^2$. Por (i), segue que $t(e) = s(g) = e$. Analogamente, $(e, g^{-1}) = (t(g^{-1}), g^{-1}) \in \mathcal{G}^2$, de onde $s(e) = t(g^{-1}) = e$. Por outro lado, se $e = s(e) = t(e)$, então $(e, e) \in \mathcal{G}^2$. Como e é uma identidade, temos $s(e) = e = ee = e = t(e)$. Pela unicidade do elemento satisfazendo (G4), segue que $e = e^{-1}$. Ou seja, $e = s(e) = t(e^{-1})$ e $e \in \mathcal{G}_0$.

(v) Sejam $e \in \mathcal{G}_0$ e $G_e = \{g \in \mathcal{G} \colon e = s(g) = t(g)\}$. Por (iv), temos que $e = s(e) = t(e)$, portanto $e \in G_e$. Se $g, h \in G_e$, então $s(g) = e = t(h)$. Por (i) segue que existe gh, enquanto que por (iii) temos $s(gh) = s(h) = e = t(g) = t(gh)$. Portanto $gh \in G_e$. Se $g \in G_e$, segue de (ii) que $s(g^{-1}) = t(g) = e = s(g) = t(g^{-1})$, de onde $g^{-1} \in G_e$. Por fim, para todo $g \in G_e$ temos $eg = t(g)g = g = gs(g) = ge$, de onde $e \in G_e$ é o elemento neutro. Com isso, G_e é um grupo e vale (v). □

Sejam $f, g \in \mathcal{G}$. Dizemos que f e g são conectados se existe $h \in \mathcal{G}$ tal que existe fhg. Assim, a relação $f \sim g$ se f e g são conectados é de equivalência. De fato, existe $gg^{-1}g$, de onde $g \sim g$. Se $f \sim g$, então existe h tal que existe fhg, portanto existe $g[g^{-1}h^{-1}f^{-1}]f$, de onde $g \simeq f$. Por fim, se $f \sim g$ e $g \sim h$, então existem p e q tais que existem gpf e hqg. Portanto existe $h[qgg^{-1}gp]f$, ou seja, $f \sim h$. Ainda, todo elemento $g \in \mathcal{G}$ é conectado às suas identidades $s(g)$ e $t(g)$, pois $s(g)s(g) = s(g)$ e $t(g)t(g) = t(g)$, de onde existem $t(g)t(g)g$ e $gs(g)s(g)$, ou seja, $g \sim t(g)$ e $s(g) \sim g$.

Com isso, toda classe de equivalência $[g] = \{h \in \mathcal{G} \colon h \sim g\}$ no conjunto quociente $\mathcal{G}/\sim$ pode ser representada por uma identidade $e = s(g) \in \mathcal{G}_0$. Mais ainda, cada classe $[e]$, $e \in \mathcal{G}_0$, é um subgrupóide de $\mathcal{G}$. De fato, como observado acima, $g \in [e]$ implica $s(g), t(g) \in [e]$. Se $g \in [e]$ e $(g, h) \in \mathcal{G}^2$, então existem $gh = gs(g)h$ e $(gh)h^{-1}h$, de onde $g \simeq h$ e $h \simeq gh$, ou seja $h, gh \in [e]$. Por fim, temos $g(g^{-1}g)g^{-1}$, de onde $g \sim g^{-1}$. Assim, cada classe de equivalência $[e]$ contém as identidades, produtos - quando definidos - e inversos de seus elementos. Portanto $[e]$ é um grupóide. Cada $[e] \in \mathcal{G}/\sim$ é chamado de **componente conexa** de $\mathcal{G}$.

Como $\sim$ é uma relação de equivalência, temos $\mathcal{G} = \bigcup_{[e] \in \mathcal{G}/\sim} [e]$. Por outro lado, do Exemplo 3.3.2(2), temos que $\coprod_{[e] \in \mathcal{G}/\sim} [e]$ é um grupóide, onde existe $(g, [e])(h, [f])$ se, e somente se, $[e] = [f]$ e existe $gh \in [e]$, e nesse caso $(g, [e])(h, [e]) = (gh, [e])$. Como os conjuntos $[e] \in \mathcal{G}/\sim$ são dois a dois disjuntos, obtemos uma bijeção entre $\mathcal{G} = \bigcup_{[e] \in \mathcal{G}/\sim} [e]$ e o grupóide $\coprod_{[e] \in \mathcal{G}/\sim} [e]$. Mais ainda, esta bijeção preserva a operação parcial de $\mathcal{G}$, de forma que todo grupóide pode ser visto como a união das suas componentes conexas.

Definição 3.3.4. Dizemos que um grupóide $\mathcal{G}$ é **conexo** se quaisquer dois elementos de $\mathcal{G}$ são conectados. Ou seja, quando ocorre $\mathcal{G}/\sim = \{\mathcal{G}\}$.

Do ponto de vista da teoria de grupóides, às vezes é suficiente considerar propriedades sobre grupóides conexos, de forma que o caso geral pode ser recuperado através da união das suas componentes conexas. Para o próximo lema, utilizaremos a notação do Exemplo 3.3.2(5).

Lema 3.3.5. *Seja $\mathcal{G}$ um grupóide conexo. Então para quaisquer $e, f \in \mathcal{G}_0$, temos $G_e \simeq G_f$, como grupos. Mais ainda, $\mathcal{G} \simeq G_e \times \mathcal{G}(\mathcal{G}_0)$ como grupóides.*

Demonstração. Sejam $e, f \in \mathcal{G}_0$. Como $\mathcal{G}$ é conexo, existem $g \in \mathcal{G}$ tal que existe egf, ou seja, tal que $s(g) = f$ e $t(g) = e$. Defina $\varphi_g \colon G_e \to G_f$ por $\varphi_g(h) = g^{-1}hg$. A função φ_g está bem definida, pois $s(h) = e = t(g)$ e $t(h) = e = t(g) = s(g^{-1})$, de onde existem $g^{-1}h$ e hg, portanto $g^{-1}hg$, ainda, $s(ghg^{-1}) = s(g^{-1}) = t(g) = e$ e $t(ghg^{-1}) = t(g) = e$, portanto $Im(\varphi_g) \subseteq G_f$. A função φ_g é bijetiva, pois existe $fg^{-1}e$, de onde podemos definir $\varphi_{g^{-1}}$ e ocorre $\varphi_g^{-1} = \varphi_{g^{-1}}$. Sejam $h, h' \in G_e$, então

$$
\begin{aligned}
\varphi_g(h)\varphi_g(h) &= (g^{-1}hg)(g^{-1}h'g) && \\
&= g^{-1}h(gg^{-1})h'g && (G1)\\
&= g^{-1}ht(g)h'g && \\
&= g^{-1}heh'g && \\
&= g^{-1}hh'g && h \in G_e\\
&= \varphi_g(hh').
\end{aligned}
$$

Lembrando que $e \in G_e$ e $f \in G_f$ são elementos neutros, temos

$$\varphi_g(e) = g^{-1}eg = g^{-1}t(g)g = g^{-1}g = s(g) = f.$$

Logo φ_g é bijetiva, preserva neutro e produtos, portanto é um isomorfismo de grupos. Lembrando que $G_e \times \mathcal{G}(\mathcal{G}_0)$ é um grupóide, cujos elementos são da forma (g, e_1, e_2), onde $g \in G_e$ e $e_1, e_2 \in \mathcal{G}_0$, com operação definida por

$$(g, e_1, e_2)(h, e_3, e_4) = (gh, e_1, e_4), \quad \text{se } e_2 = e_3.$$

Para cada $e_i \in \mathcal{G}_0$, fixe um elemento $g_i \in \mathcal{G}$ tal que existe eg_ie_i. Defina $\Phi \colon G_e \times \mathcal{G}(\mathcal{G}_0) \to \mathcal{G}$ por $\Phi(g, e_1, e_2) = (e_1g_1^{-1}e)g(eg_2e_2) = g_1^{-1}gg_2$. Então Φ é um morfismo de grupóides, pois

$$
\begin{aligned}
\Phi(g, e_1, e_2)\Phi(h, e_2, e_3) &= (g_1^{-1}gg_2)(g_2^{-1}hg_3) && \\
&= g_1^{-1}g(g_2g_2^{-1})hg_3 && (G1)\\
&= g_1^{-1}gt(g_2)hg_3 && (G4)\\
&= g_1^{-1}gehg_3 && \\
&= g_1^{-1}ghg_3 && e = s(g)\\
&= \Phi(gh, e_1, e_3),
\end{aligned}
$$

ou seja, Φ preserva a operação, sempre que ela existe, e

$$
\begin{aligned}
\Phi(g, e_1, e_2)^{-1} &= (g_1^{-1}gg_2)^{-1} && \\
&= g_2^{-1}g^{-1}g_1 && 3.3.3(ii), (iii)\\
&= \Phi(g^{-1}, e_2, e_1) && \\
&= \Phi((g, e_1, e_2)^{-1}),
\end{aligned}
$$

de onde Φ preserva inversos. Portanto Φ é um morfismo de grupóides. Por outro lado, $\Psi\colon \mathcal{G} \to G_e \times \mathcal{G}(\mathcal{G}_0)$ definida por $\Psi(g) = (g_{t(h)} h g_{s(h)}^{-1}, t(h), s(h))$ é tal que

$$\begin{aligned}(\Psi \circ \Phi)(g, e_1, e_2) &= \Psi(g_1^{-1} g g_2) \\ &= (g_1[g_1^{-1} g g_2^{-1}] g_2, e_1, e_2) \\ &= (ege, e_1, e_2) \\ &= (g, e_1, e_2),\end{aligned} \qquad \begin{aligned}(\Phi \circ \Psi)(g) &= \Phi(g_{s(h)} h g_{t(h)}^{-1}, t(h), s(h)) \\ &= g_{t(h)}^{-1}[g_{t(h)} h g_{s(h)}^{-1}] g_{s(h)} \\ &= t(h) h s(h) \\ &= h.\end{aligned}$$

Assim, Φ é uma bijeção, portanto um isomorfismo de grupóides. $\square$

Uma observação que poderia ser feita a partir da definição de grupóide, mas que fica clara com o resultado acima: um grupóide é um grupo se, e somente se, possui uma única identidade. Nesse caso temos $\mathcal{G} \simeq G_e \times \{e\} \simeq G_e$. Para definir a álgebra de grupóide, lembramos que, pela Proposição 1.1.5, se M é um módulo livre, então todo morfismo fica completamente determinado pela imagem dos elementos da base de M.

Lema 3.3.6. *Sejam k um anel comutativo e $k\mathcal{G}$ o módulo livre de base $\mathcal{G}$. Então $k\mathcal{G}$ admite uma estrutura de álgebra sobre k com operação definida por*

$$a_g \mathbf{g} \cdot a_h \mathbf{h} = \begin{cases} a_g a_h \mathbf{gh}, & \exists gh \\ 0, & c.c. \end{cases}, \quad \forall g, h \in \mathcal{G}, a_g, a_h \in k$$

se, e somente se, $\mathcal{G}$ possui finitas identidades. Nesse caso, $k\mathcal{G}$ possui uma estrutura de álgebra de Hopf fraca, com morfismos

$$u(1_k) = \sum_{e \in \mathcal{G}_0} \mathbf{e}, \qquad \Delta(\mathbf{g}) = \mathbf{g} \otimes \mathbf{g}, \qquad \epsilon(\mathbf{g}) = 1_k \qquad e \qquad S(\mathbf{g}) = \mathbf{g^{-1}}.$$

Demonstração. A multiplicação definida acima sempre é associativa, pois

$$\begin{aligned}(a_g \mathbf{g} \cdot a_h \mathbf{h}) \cdot a_l \mathbf{l} &= \begin{cases} a_g a_h \mathbf{gh} \cdot a_l \mathbf{l}, & \exists gh \\ 0, & c.c. \end{cases} \\ &= \begin{cases} a_g a_h a_l (\mathbf{gh}) \mathbf{l}, & \exists (gh)l \\ 0, & c.c. \end{cases} \\ &= \begin{cases} a_g a_h a_l \mathbf{g}(\mathbf{hl}), & \exists g(hl) \\ 0, & c.c. \end{cases} \qquad (G1) \\ &= \begin{cases} a_g \mathbf{g} \cdot a_h a_l \mathbf{hl}, & \exists hl \\ 0, & c.c. \end{cases} \\ &= a_g \mathbf{g} \cdot (a_h \mathbf{h} \cdot a_l \mathbf{l}).\end{aligned}$$

Por simplicidade, vamos denotar $\mathbf{g} \cdot \mathbf{h} = [s(g) = t(h)]\mathbf{gh}$, onde $\mathbf{gh}$ é um símbolo sem significado quando não existe $gh \in \mathcal{G}$, e neste caso $[s(g) = t(h)]\mathbf{gh} = 0\mathbf{gh} = 0 = \mathbf{g} \cdot \mathbf{h}$.

Como observado anteriormente, se $(g, h) \in \mathcal{G}^2$, então g e h são conectados. Por contrapositiva, se g e h pertencem a componentes conexas distintas, então $(g, h) \notin \mathcal{G}^2$, de onde $\alpha_g \mathbf{g} \cdot \alpha_h \mathbf{h} = 0$. Assim, podemos considerar $k\mathcal{G} = k(\coprod_{i \in I} \mathcal{G}_i) = \bigoplus_{i \in I} k\mathcal{G}_i$, onde $\{\mathcal{G}_i \colon i \in I\}$ são as componentes conexas de $\mathcal{G}$ e $\prod$ denota o produto cartesiano de anéis. Com isso, existe $1_{k\mathcal{G}}$ se, e somente se, I é finito e existe $1_{k\mathcal{G}_i}$, para todo $i \in I$, e nesse caso $1_{k\mathcal{G}} = \sum_{i\in I} 1_{k\mathcal{G}_i}$. Portanto, é suficiente considerar $\mathcal{G}$ um grupóide conexo. Seja $X = \sum_{e\in\mathcal{G}_0} \mathbf{e}$, então, para todo $h \in \mathcal{G}$, temos

$$\begin{aligned} X\mathbf{h} &= \sum_{e\in\mathcal{G}_0} \mathbf{e}\cdot\mathbf{h} & \mathbf{h}X &= \sum_{e\in\mathcal{G}_0} \mathbf{h}\cdot\mathbf{e} & \\ &= \sum_{e\in\mathcal{G}_0} [s(e)=t(h)]\mathbf{eh} & &= \sum_{e\in\mathcal{G}_0} [s(h)=t(e)]\mathbf{he} & 3.3.3(i) \\ &= \sum_{e\in\mathcal{G}_0} [e=t(h)]\mathbf{eh} & &= \sum_{e\in\mathcal{G}_0} [s(h)=e]\mathbf{he} & 3.3.3(iv) \\ &= \mathbf{h}, & &= \mathbf{h}. & (G3) \end{aligned}$$

Isso mostra que, para um grupóide conexo $\mathcal{G}$ com finitas identidades, $1_{k\mathcal{G}} = \sum_{e\in\mathcal{G}_0} \mathbf{e}$. Com isso, segue que $\mathcal{G}$ admite uma estrutura de álgebra (equivalentemente, um morfismo unidade) se, e somente se, $\mathcal{G}$ possui finitas identidades. Agora, considere Δ, ϵ e S como no enunciado. Então Δ é coassociativa e multiplicativa, pois

$$(\Delta\otimes id_{k\mathcal{G}})\Delta(\mathbf{g}) = (\mathbf{g}\otimes\mathbf{g})\otimes\mathbf{g} = \mathbf{g}\otimes(\mathbf{g}\otimes\mathbf{g}) = (id_{k\mathcal{G}}\otimes\Delta)\Delta(\mathbf{g}),$$

e

$$\Delta(\mathbf{g})\Delta(\mathbf{h}) = (\mathbf{g}\otimes\mathbf{g})(\mathbf{h}\otimes\mathbf{h}) = [s(g)=t(h)](\mathbf{gh}\otimes\mathbf{gh}) = \Delta(\mathbf{gh}).$$

A tripla $(k\mathcal{G},\Delta,\epsilon)$ é counitária, pois, para todo $g\in\mathcal{G}$,

$$\begin{aligned} \mu(u\epsilon\otimes id_{k\mathcal{G}})\Delta(\mathbf{g}) &= u\epsilon(\mathbf{g})\cdot\mathbf{g} & \mu(id_{k\mathcal{G}}\otimes u\epsilon)\Delta(\mathbf{g}) &= \mathbf{g}\cdot u\epsilon(\mathbf{g}) \\ &= u(1_k)\cdot\mathbf{g} & &= \mathbf{g}\cdot u(1_k) \\ &= 1_{k\mathcal{G}}\cdot\mathbf{g} & &= \mathbf{g}\cdot 1_{k\mathcal{G}} \\ &= \mathbf{g}, & &= \mathbf{g}. \end{aligned}$$

O morfismo ϵ é fracamente multiplicativo, pois dados $g,h,l\in\mathcal{G}$, temos

$$\begin{aligned} \epsilon(\mathbf{g}\cdot\mathbf{h_1})\epsilon(\mathbf{h_2}\cdot\mathbf{g}) &= \epsilon(\mathbf{g}\cdot\mathbf{h})\epsilon(\mathbf{h}\cdot\mathbf{l}) \\ &= [s(g)=t(h), s(h)=t(l)]\epsilon(\mathbf{gh})\epsilon(\mathbf{hl}) \\ &= [s(g)=t(h), s(h)=t(l)] \\ &= [s(g)=t(h), s(h)=t(l)]\epsilon(\mathbf{ghl}) \\ &= \epsilon(\mathbf{g}\cdot\mathbf{h}\cdot\mathbf{l}), \end{aligned}$$

e

$$\begin{aligned} \epsilon(\mathbf{g}\cdot\mathbf{h_2})\epsilon(\mathbf{h_1}\cdot\mathbf{g}) &= \epsilon(\mathbf{g}\cdot\mathbf{h})\epsilon(\mathbf{h}\cdot\mathbf{l}) \\ &= \epsilon(\mathbf{g}\cdot\mathbf{h_1})\epsilon(\mathbf{h_2}\cdot\mathbf{g}) \\ &= \epsilon(\mathbf{g}\cdot\mathbf{h}\cdot\mathbf{l}). \end{aligned}$$

De onde $(k\mathcal{G},\mu,u,\Delta,\epsilon)$ é uma biálgebra fraca. Por fim, o morfismo S satisfaz os axiomas de (W5). De fato, para todo $g\in\mathcal{G}$ segue que

$$\begin{aligned} \epsilon(1_1\cdot\mathbf{g})1_2 &= \sum_{e\in\mathcal{G}_0}\epsilon(\mathbf{e}\cdot\mathbf{g})\mathbf{e} & (id_{k\mathcal{G}}*S)(\mathbf{g}) &= \mathbf{g}S(\mathbf{g}) \\ &= \sum_{e\in\mathcal{G}_0}[e=t(g)]\epsilon(\mathbf{eg})\mathbf{e} & &= \mathbf{gg^{-1}} \end{aligned}$$

$$= \epsilon(\mathbf{t}(\mathbf{g})\mathbf{g})\mathbf{t}(\mathbf{g}) \qquad\qquad = \mathbf{t}(\mathbf{g}),$$
$$= \mathbf{t}(\mathbf{g}),$$

$$\begin{aligned} 1_1\epsilon(g\cdot 1_2) &= \sum_{e\in\mathcal{G}_0} \mathbf{e}\epsilon(\mathbf{g}\cdot\mathbf{e}) & (S * id_{k\mathcal{G}})(\mathbf{g}) &= S(\mathbf{g})\mathbf{g} \\ &= \sum_{e\in\mathcal{G}_0} [e = s(g)]\mathbf{e}\epsilon(\mathbf{ge}) & &= \mathbf{g}^{-1}\mathbf{g} \\ &= \epsilon(\mathbf{gs}(\mathbf{g}))\mathbf{s}(\mathbf{g}) = \mathbf{s}(\mathbf{g}), & &= \mathbf{s}(\mathbf{g}), \end{aligned}$$

e

$$(S * id_{k\mathcal{G}} * S)(\mathbf{g}) = S(\mathbf{g})\mathbf{g}S(\mathbf{g}) = \mathbf{g^{-1}gg^{-1}} = \mathbf{s}(\mathbf{g})\mathbf{g^{-1}} = \mathbf{t}(\mathbf{g^{-1}})\mathbf{g^{-1}} = \mathbf{g^{-1}} = S(\mathbf{g}).$$

Portanto $(k\mathcal{G}, \mu, u, \Delta, \epsilon, S)$ é uma álgebra de Hopf fraca. □

Observamos que, se $\mathcal{G}$ é um grupóide que não é um grupo, então existem $g, h \in \mathcal{G}$ tais que $(g, h) \notin \mathcal{G}^2$, ou seja, tais que $s(g) \neq t(h)$. Com isso,

$$\epsilon(\mathbf{g})\epsilon(\mathbf{h}) = 1_k^2 = 1_k \neq 0 = [s(g) = t(h)]\epsilon(\mathbf{gh}) = \epsilon(\mathbf{g}\cdot\mathbf{h}).$$

Ou seja, ϵ não é multiplicativo, portanto $k\mathcal{G}$ não pode ser uma álgebra de Hopf. Por outro lado, se $\mathcal{G}$ for um grupo, então a estrutura de álgebra de Hopf fraca em $k\mathcal{G}$ coincide com a estrutura álgebra de Hopf sobre a álgebra de grupo definida no Exemplo 1.4.2(2).

Exemplo 3.3.7. Sejam $I_n = \{1, \ldots, n\}$ e $\mathcal{G} = \mathcal{G}(I_n)$ o grupóide do Exemplo 3.3.2(5). Considere $M_n(k)$ com a estrutura de álgebra de Hopf fraca dada pelo 1.4.4(2). Então $k\mathcal{G} \simeq M_n(k)$ como álgebras de Hopf fracas.

Demonstração. Como $\mathcal{G}^2 = \{((i, j), (j, r)), : i, j, r = 1, \ldots, n\}$ e a operação em $\mathcal{G}$ é definida por $(i, j)(j, r) = (i, r)$, segue que $\mathcal{G}_0 = \{(i, i) \colon i = 1, \ldots, n\}$ possui n elementos. Mais ainda, dados $(i, j), (r, s) \in \mathcal{G}$, existe o produto $(i, j)(j, r)(r, s)$, ou seja, quaisquer dois elementos de $\mathcal{G}$ são conectados. Portanto $\mathcal{G}$ é um grupóide conexo com finitas identidades.

Segue do Lema 3.3.6 que $k\mathcal{G}$ possui uma estrutura de álgebra de Hopf fraca, onde

$$\Delta((\mathbf{i}, \mathbf{j})) = (\mathbf{i}, \mathbf{j}) \otimes (\mathbf{i}, \mathbf{j}), \qquad \epsilon((\mathbf{i}, \mathbf{j})) = 1_k \qquad \text{e} \qquad S((\mathbf{i}, \mathbf{j})) = (\mathbf{i}, \mathbf{j})^{-1} = (\mathbf{j}, \mathbf{i}).$$

Defina $\Phi \colon k\mathcal{G} \to M_n(k)$ por $\Phi((\mathbf{i}, \mathbf{j})) = e_{ij}$. Então Φ é um isomorfismo, pois os conjuntos $\{(\mathbf{i}, \mathbf{j}) \colon i, j = 1 \ldots, n\}$ e $\{e_{ij} \colon i, j = 1, \ldots, n\}$ são bases de $k\mathcal{G}$ e $M_n(k)$, respectivamente. Por fim, Φ é um morfismo de álgebras de Hopf fracas, pois

$$\Phi((\mathbf{i}, \mathbf{j}) \cdot (\mathbf{r}, \mathbf{s})) = [j = r]\Phi((\mathbf{i}, \mathbf{s})) = [j = r]e_{is} = e_{ij}e_{rs} = \Phi((\mathbf{i}, \mathbf{j}))\Phi((\mathbf{r}, \mathbf{s})),$$
$$\Phi(1_{k\mathcal{G}}) = \sum_{i=1}^{n} \Phi((\mathbf{i}, \mathbf{i})) = \sum_{i=1}^{n} e_{ii} = 1_{M_n(k)},$$

de onde Φ é um morfismo de álgebras,

$$(\Delta \circ \Phi)((\mathbf{i}, \mathbf{j})) = \Delta(e_{ij}) = e_{ij} \otimes e_{ij} = \Phi((\mathbf{i}, \mathbf{j})) \otimes \Phi((\mathbf{i}, \mathbf{j})) = (\Phi \otimes \Phi)\Delta((\mathbf{i}, \mathbf{j})),$$
$$(\epsilon \circ \Phi)((\mathbf{i}, \mathbf{j})) = \epsilon(e_{ij}) = 1_k = \epsilon((\mathbf{i}, \mathbf{j})),$$

de onde Φ é um morfismo de coálgebras, e

$$(\Phi \circ S)((\mathbf{i}, \mathbf{j})) = \Phi((\mathbf{j}, \mathbf{i})) = e_{ji} = S(e_{ij}) = (S \circ \Phi)((\mathbf{i}, \mathbf{j})),$$

de onde Φ preserva a antípoda. Assim, Φ é um isomorfismo de álgebras de Hopf fracas. □

Lema 3.3.8. *Sejam $\mathcal{G}$ e $\mathcal{H}$ grupóides com finitas identidades. Considere $\mathcal{G} \times \mathcal{H}$ com a estrutura de grupóide do Exemplo 3.3.2(6) e $k\mathcal{G} \otimes k\mathcal{H}$ com a estrutura de álgebra de Hopf fraca do Exemplo 1.4.4(3). Então $k(\mathcal{G} \times \mathcal{H}) \simeq k\mathcal{G} \otimes k\mathcal{H}$, como álgebras de Hopf fracas.*

Demonstração. Como a operação em $\mathcal{G} \times \mathcal{H}$ é definida coordenada a coordenada, temos que $(g,h)(\mathcal{G} \times \mathcal{H})_0$ se, e somente se, $(g,h) = t(g,h) = (t(g), t(h))$ e $(g,h) = s(g,h) = (s(g), s(h))$, ou seja, o conjunto das identidades de $\mathcal{G} \times \mathcal{H}$ é precisamente $\mathcal{G}_0 \times \mathcal{H}_0$, o qual é finito pois $\mathcal{G}_0$ e $\mathcal{H}_0$ são finitos. Assim, a estrutura de álgebra de Hopf fraca em $k(\mathcal{G} \times \mathcal{H})$ está bem definida.

Como $k\mathcal{G}$ e $k\mathcal{H}$, como módulos sobre k, são livres de base $\mathcal{G}$ e $\mathcal{H}$, respectivamente, segue da Proposição 1.2.6, com $A = B = k$, que $k\mathcal{G} \otimes k\mathcal{H}$ é um $k \otimes k \simeq k$ módulo livre com base $\{\mathbf{g} \otimes \mathbf{h} \colon g \in \mathcal{G}, h \in \mathcal{H}\}$. Assim, definindo $\Phi \colon k(\mathcal{G} \times \mathcal{H}) \to k\mathcal{G} \otimes k\mathcal{H}$ por $\Phi((\mathbf{g}, \mathbf{h})) = \mathbf{g} \otimes \mathbf{h}$, obtemos que Φ é um isomorfismo de módulos livres, pois leva base em base. Observando que $(\mathcal{G} \times \mathcal{H})_0 = \mathcal{G}_0 \times \mathcal{H}_0$, temos

$$\begin{aligned}
\Phi((\mathbf{g}, \mathbf{h}) \cdot (\mathbf{g}', \mathbf{h}')) &= [s(g) = t(g'), s(h) = t(h')]\Phi((\mathbf{g}\mathbf{g}', \mathbf{h}\mathbf{h}')) \\
&= [s(g) = t(g'), s(h) = t(h')](\mathbf{g}\mathbf{g}' \otimes \mathbf{h}\mathbf{h}') \\
&= (\mathbf{g} \otimes \mathbf{h})(\mathbf{g}' \otimes \mathbf{h}') \\
&= \Phi((\mathbf{g}, \mathbf{h}))\Phi((\mathbf{g}', \mathbf{h}')),
\end{aligned}$$

e

$$\begin{aligned}
\Phi(1_{k(\mathcal{G} \times \mathcal{H})}) &= \sum_{(e,f) \in \mathcal{G}_0 \times \mathcal{H}_0} \Phi((\mathbf{e}, \mathbf{f})) = \sum_{(e,f) \in \mathcal{G}_0 \times \mathcal{H}_0} \mathbf{e} \otimes \mathbf{f} \\
&= \left(\sum_{e \in \mathcal{G}_0} \mathbf{e} \right) \otimes \left(\sum_{f \in \mathcal{H}_0} \mathbf{f} \right) = 1_{k\mathcal{G}} \otimes 1_{k\mathcal{H}} = 1_{k\mathcal{G} \otimes k\mathcal{H}}.
\end{aligned}$$

Portanto Φ é um morfismo de álgebras. Note agora que

$$\begin{aligned}
(\Delta \circ \Phi)((\mathbf{g}, \mathbf{h})) &= \Delta(\mathbf{g} \otimes \mathbf{h}) \\
&= (\mathbf{g} \otimes \mathbf{h}) \otimes (\mathbf{g} \otimes \mathbf{h}) \\
&= \Phi((\mathbf{g}, \mathbf{h})) \otimes \Phi((\mathbf{g}, \mathbf{h})) \\
&= (\Phi \otimes \Phi)\Delta((\mathbf{g}, \mathbf{h})).
\end{aligned}
\qquad
\begin{aligned}
(\epsilon \circ \Phi)((\mathbf{g}, \mathbf{h})) &= \epsilon(\mathbf{g} \otimes \mathbf{h}) \\
&= \epsilon(\mathbf{g})\epsilon(\mathbf{h}) \\
&= 1_k \\
&= \epsilon((\mathbf{g}, \mathbf{h}))
\end{aligned}$$

Portanto Φ é um morfismo de coálgebras. Por fim,

$$\begin{aligned}
(S \circ \Phi)((\mathbf{g}, \mathbf{h})) &= S(\mathbf{g} \otimes \mathbf{h}) \\
&= S(\mathbf{g}) \otimes S(\mathbf{h}) \\
&= \mathbf{g}^{-1} \otimes \mathbf{h}^{-1} \\
&= \Phi((\mathbf{g}^{-1}, \mathbf{h}^{-1})) \\
&= (\Phi \circ S)((\mathbf{g}, \mathbf{h})).
\end{aligned}$$

Assim, Φ é um isomorfismo de álgebras de Hopf fracas. Logo $k(\mathcal{G} \times \mathcal{H}) \simeq k\mathcal{G} \otimes k\mathcal{H}$. □

Como corolário dos Lemas 3.3.5, 3.3.6 e 3.3.8 e do Exemplo 3.3.7, se $\mathcal{G}$ é um grupóide conexo com finitas identidades, então $k\mathcal{G} \simeq kG \otimes M_n(k)$, onde $G \simeq G_e$, para qualquer $e \in \mathcal{G}_0$, e $n = |\mathcal{G}_0|$. Mais ainda, $kG \otimes M_n(k) \simeq M_n(kG)$, como módulos sobre k, através do isomorfismo $\mathbf{g} \otimes e_{ij} \mapsto ge_{ij}$. Assim, podemos considerar $M_n(kG)$ como uma álgebra de Hopf fraca sobre k com a estrutura induzida pelo isomorfismo, ou seja, com morfismos

$$ge_{ij} \cdot he_{rs} = [j = r]ghe_{is}, \qquad u(1_k) = \sum_{i=1}^{n} e_G e_{ii},$$
$$\Delta(ge_{ij}) = ge_{ij} \otimes ge_{ij}, \qquad \epsilon(ge_{ij}) = 1_k,$$

e antípoda definida por $S(ge_{ij}) = g^{-1}e_{ji}$. Como $\Delta(ge_{ij}) = (\tau \circ \Delta)(ge_{ij})$ para todo elemento da base de $M_n(kG)$, segue que $\Delta(x) = (\tau \circ \Delta)(x)$, para todo $x \in M_n(kG)$, ou seja, esta álgebra de Hopf fraca é cocomutativa. Assim, para classificarmos as extensões de Hopf-Ore primitivas fracas de $H = M_n(kG)$, vide Teorema 2.4.8 e Lema 2.4.12, devemos caracterizar os elementos group-like fracos centrais e inversíveis g; os caracteres à esquerda fracos que definem automorfismos τ_χ^l e as τ_χ^l-derivações que são $(g, 1_H)$-coderivações.

Lema 3.3.9. *Seja $H = M_n(kG)$. Então $x \in H$ é um elemento group-like fraco, central e inversível se, e somente se, $x = \sum_{i,j} r_j g_j e_{ii}$, onde $g_1, \ldots, g_m \in Z(G)$ e $\{r_1, \ldots, r_m\} \subseteq k$ é uma família de idempotentes ortogonais satisfazendo $\sum_{j=1}^{m} r_j = 1_k$.*

Demonstração. Seja $x = \sum_{i,j,g} \alpha_{ij}^g ge_{ij}$ um elemento genérico de $M_n(kG)$. Se x é um elemento central, então, em particular, deve valer $xe_{ll} = e_{ll}x$, para todo $l = 1, \ldots, n$. Assim, deve valer a igualdade

$$\sum_{i,g} \alpha_{il}^g ge_{il} = \sum_{i,j,g} \alpha_{ij}^g ge_{ij} \cdot e_{ll} = xe_{ll} = e_{ll}x = \sum_{i,j,g} e_{ll} \cdot \alpha_{ij}^g ge_{ij} = \sum_{j,g} \alpha_{lj}^g ge_{lj}.$$

Como H é um módulo livre sobre k com base $\{ge_{ij} : g \in G, i, j = 1, \ldots, n\}$, existe um morfismo $q_l : H \to H$ tal que $q_l(ge_{ij}) = ge_{ij}$, se $j \neq l$, e $q_l(ge_{il}) = 0$. Aplicando este morfismo à igualdade acima, obtemos

$$0 = \sum_{i,g} \alpha_{il}^g q_l(ge_{il}) = \sum_{j,g} \alpha_{lj}^g q_l(ge_{lj}) = \sum_{j \neq l, g} \alpha_{lj}^g ge_{lj}.$$

Como o conjunto $\{ge_{lj} : g \in G, j = 1, \ldots, n\}$ é linearmente independente à esquerda sobre k, segue que $\alpha_{lj}^g = 0$, para todo $j \neq l$. Analogamente, definindo $p_l : H \to H$ por $p_l(ge_{ij}) = ge_{ij}$, se $i \neq l$, e $p_l(ge_{lj}) = 0$, obtemos

$$\sum_{i \neq l, g} \alpha_{il}^g ge_{il} = \sum_{i,g} \alpha_{il}^g p_l(ge_{il}) = \sum_{j,g} \alpha_{lj}^g p_l(ge_{lj}) = 0.$$

Portanto $\alpha_{il}^g = 0$, para todo $i \neq l$. Assim, $\alpha_{ij}^g = 0$, sempre que $(i,j) \neq (l,l)$, de onde $x = \sum_{i,g} \alpha_{ii}^g ge_{ii}$. Mais ainda, deve valer $x(h1_{M_n(k)}) = (h1_{M_n(k)})x$, para todo $h \in G$, de onde

$$\sum_{i,g} \alpha_{ii}^g ghe_{ii} = \sum_{i,j,g} \alpha_{ii}^g ge_{ii} \cdot he_{jj} = x(h1_{M_n(k)}) = (h1_{M_n(k)})x = \sum_{i,j,g} he_{jj} \cdot \alpha_{ii}^g ge_{ii} = \sum_{i,g} \alpha_{ii}^g hge_{ii}.$$

Por outro lado, temos que $H = M_n(kG)$ é um módulo à esquerda livre sobre kG com base $\{e_{ij} : i, j = 1, \ldots, n\}$. Assim, comparando as escritas acima, obtemos que $\alpha_{ii}^g gh = \alpha_{ii}^g hg$, para todo $i = 1, \ldots, n$. Como kG é um módulo livre sobre k com base $\{g : g \in G\}$, segue que $\alpha_{ii}^g = 0$, para todo $i = 1, \ldots, n$, sempre que $gh \neq hg$. Ou seja, os termos ge_{ii} na escrita de x com coeficiente não necessariamente nulo ocorrem quando $g \in Z(G)$. Mais ainda, como $x \in Z(H)$, devem ser iguais

$$x \cdot e_{1j} = \sum_{i=1}^{n} \sum_{g \in Z(G)} \alpha_{ii}^{g} g e_{ii} \cdot e_{1j} = \sum_{g \in Z(G)} \alpha_{11}^{g} g e_{1j}$$

e

$$e_{1j} \cdot x = \sum_{i=1}^{n} \sum_{g \in Z(G)} e_{1j} \cdot \alpha_{ii}^{g} g e_{ii} = \sum_{g \in Z(G)} \alpha_{jj}^{g} g e_{1j},$$

logo, comparando os coeficientes de ge_{1j} em cada escrita, obtemos que $\alpha_{jj}^{g} = \alpha_{11}^{g} =: r_g$, para cada $g \in Z(G)$. Como x é um elemento central de H, $x \otimes x$ é um elemento central de $H \otimes H$, de onde $\Delta(1_H)(x \otimes x) = (x \otimes x)\Delta(1_H)$ e vale

$$\begin{aligned}
\Delta(1_H)(x \otimes x) &= \left(\sum_{l=1}^{n} e_{ll} \otimes e_{ll}\right) \left(\left(\sum_{i,g} r_g g e_{ii}\right) \otimes \left(\sum_{j,h} r_h h e_{jj}\right)\right) \\
&= \sum_{i,j,l,g,h} r_g r_h (e_{ll} \cdot g e_{ii} \otimes e_{ll} \cdot h e_{jj}) \\
&= \sum_{l,g,h} r_g r_h (g e_{ll} \otimes h e_{ll}).
\end{aligned}$$

Se $x \in Z(H)$ for um elemento group-like fraco, então

$$\sum_{l,g,h} r_g r_h (g e_{ll} \otimes h e_{ll}) = \Delta(1_H)(x \otimes x) = \Delta(x) = \sum_{l,g} r_g \Delta(g e_{ll}) = \sum_{l,g} r_g (g e_{ll} \otimes g e_{ll}).$$

Como $H \otimes H$ é um módulo livre sobre k com base $\{g e_{ij} \otimes h e_{rs}\}$, podemos comparar os termos $g e_{ll} \otimes h e_{ll}$ na igualdade acima, obtendo $r_g r_h = [g = h] r_g$. Assim, os elementos r_g, $g \in Z(G)$, são idempotentes ortogonais. Por fim, se $x \in Z(H) \cap G_w(H)$ é inversível, temos do Lema 2.2.5 que $x^{-1} = S(x)$. Logo

$$\begin{aligned}
\sum_{i=1}^{n} e e_{ii} = 1_H = x S(x) \\
&= \sum_{i,j,g,h} r_g g e_{ii} \cdot r_h S(h e_{jj}) \\
&= \sum_{i,j,g,h} r_g g e_{ii} \cdot r_h h^{-1} e_{jj} \\
&= \sum_{i,g,h} r_g r_h g h^{-1} e_{ii} \\
&= \sum_{i,g} r_g e e_{ii},
\end{aligned}$$

onde, na última igualdade, utilizamos que os escalares r_g, $g \in Z(G)$, são idempotentes ortogonais. Assim, comparando os coeficientes de $e e_{ii}$ na igualdade acima, obtemos que $\sum_g r_g = 1_k$. Em suma, se $g_1, \ldots, g_q \in Z(G)$ são os elementos tais que $r_{g_j} \neq 0$, então, denotando $r_j = r_{g_j}$, temos que

$$x = \sum_{i=1}^{n} \sum_{j=1}^{q} r_j g_j e_{ii}.$$

Reciprocamente, suponha que $x = \sum_{i,j} r_j g_j e_{ii}$, onde $g_j \in Z(G)$ e $\{r_1, \ldots, r_q\} \subseteq k$ é uma família de idempotentes ortogonais tal que $\sum_j r_j = 1_k$. Então x é um elemento central de H, pois, dado um elemento base he_{ps}, temos

$$\begin{aligned}
x \cdot he_{ps} &= \sum_{i,j} r_j g_j e_{ii} \cdot he_{ps} \\
&= \sum_{j} r_j g_j he_{ps} \\
&= \sum_{j} r_j h g_j e_{ps} && (g_j \in Z(G)) \\
&= \sum_{i,j} he_{ps} \cdot r_j g_j e_{ii} \\
&= he_{ps} \cdot x,
\end{aligned}$$

de onde $x \in Z(H)$. O elemento x é group-like fraco, pois,

$$\begin{aligned}
\Delta(1_H)(x \otimes x) &= \sum_{i,j,p,q,l} (e_{ll} \otimes e_{ll})(r_j g_j e_{ii} \otimes r_q g_q e_{pp}) \\
&= \sum_{j,q,l} r_j r_q (g_j e_{ll} \otimes g_q e_{ll}) \\
&= \sum_{j,l} r_j (g_j e_{ll} \otimes g_j e_{ll}) = \sum_{i,j} r_j \Delta(g_j e_{ii}) = \Delta(x),
\end{aligned}$$

onde, na terceira igualdade, utilizamos que $\{r_j\}_j \subseteq k$ é uma família de idempotentes ortogonais. Como $x \in Z(H)$, $x \otimes x$ é um elemento central em $H \otimes H$, de onde vale $\Delta(x) = \Delta(1_H)(x \otimes x) = (x \otimes x)\Delta(1_H)$. Portanto $x \in G_w(H)$. Por fim, $x \in \mathcal{U}(H)$, pois

$$\begin{aligned}
S(x)x = xS(x) &= \sum_{i,j,l,s} r_j g_j e_{ii} \cdot r_s S(g_s e_{ll}) \\
&= \sum_{i,j,l,s} r_j g_j e_{ii} \cdot r_s g_s^{-1} e_{ll} \\
&= \sum_{i,j,s} r_j r_s g_j g_s^{-1} e_{ii} \\
&= \sum_{i,j} r_j g_j g_j^{-1} e_{ii} \\
&= \sum_{i,j} r_j e e_{ii} \\
&= \sum_{i} \left(\sum_{j} r_j \right) e e_{ii} \\
&= \sum_{i} 1_k e e_{ii} \\
&= 1_H,
\end{aligned}$$

onde, na quarta igualdade, utilizamos que $\{r_j\}_j \subseteq k$ é uma família de idempotentes ortogonais e, na sexta igualdade, utilizamos que $\sum_j r_j = 1_k$. □

Quando k não possui idempotentes não triviais, a condição $r_j r_s = [j = s]r_j$ implica em $r_j \in \{0, 1_k\}$, para todo $j = 1, \ldots, q$. Mais ainda, $\sum_j r_j = 1_k$ implica que existe $j \in \{1, \ldots, q\}$ tal que $r_j \neq 0$, de onde $r_j = 1_k$ e $r_s = r_s r_j = 0$, para todo $s \neq j$. Neste caso, os elementos group-like fracos, centrais e inversíveis de $M_n(kG)$ são da forma $\sum_{i=1}^n g_i e_{ii}$, onde $g_i \in Z(G)$. Ou seja,

$$G_w(M_n(kG)) \cap Z(M_n(kG)) \cap \mathcal{U}(M_n(kG)) = \bigoplus_{i=1}^{n} Z(G)e_{ii}. \qquad (*)$$

Por outro lado, sejam k um anel comutativo que possui um idempotente não trivial f e G um grupo com pelo menos um elemento central $h \neq e$. Então, pelo lema acima, $x = [fe + (1-f)h]1_{M_n(k)}$ é um elemento group-like fraco, central e inversível em $M_n(kG)$. Ou seja, vale $(*)$ se, e somente se, k não possui idempotentes não triviais ou $Z(G) = \{e\}$.

Quando $n = 1$, $H = M_1(kG) = kG$ é uma álgebra de Hopf e a igualdade $(*)$ torna-se $G(kG) \cap Z(kG) = Z(G)1_H$. Esta igualdade foi utilizada em [20, Proposition 2.2] para realizar a classificação das extensões de Hopf-Ore das álgebras de grupo. Assim, é possível que esta classificação não seja completa, uma vez que, sob a hipótese de k ser um anel comutativo, existem elementos group-like centrais que não foram considerados.

Para apresentar a caracterização dos caracteres à esquerda fracos das álgebras de grupóide conexo, lembramos que, como $M_n(kG)$ é uma álgebra de Hopf fraca cocomutativa, vale $\tau_\chi^l = \tau_\chi^r$, para todo $\chi \in Hom_k(H, k)$. Assim, χ é um caracter à esquerda fraco se, e somente se, é um caracter à direita fraco. Diremos que $\chi \in X_w^l(H) \cap X_w^r(H)$ é, simplesmente, um **caracter fraco**. Neste caso, denotaremos $\tau_\chi^l = \tau_\chi^r = \tau_\chi$. Assim, todo caracter à esquerda fraco de $M_n(kG)$ é um caracter fraco.

Lema 3.3.10. *Seja $H = M_n(kG)$. Então $\chi \in Hom_k(H, k)$ é um caracter fraco de H se, e somente se, $\chi(ge_{ij}) = \rho(g)\lambda_i\lambda_j^{-1}$, onde $\rho\colon G \to \mathcal{U}(k)$ é um morfismos de grupos, $\lambda_i \in \mathcal{U}(k)$, para todo $i = 1, \ldots, n$, e $\lambda_1 = 1_k$.*

Demonstração. Suponha que $\rho\colon G \to \mathcal{U}(k)$ é um morfismo de grupos e $\lambda_i \in \mathcal{U}(k)$, onde $\lambda_1 = 1_k$. Defina $\chi\colon H \to k$ por $\chi(ge_{ij}) = \rho(g)\lambda_i\lambda_j^{-1}$. Então, dados ge_{ij} e he_{rs} elementos base de H, temos

$$\begin{aligned}
\tau_\chi(ge_{ij})\tau_\chi(he_{rs}) &= \chi(ge_{ij})ge_{ij} \cdot \chi(he_{rs})he_{rs} \\
&= [j = r]\chi(ge_{ij})\chi(he_{js})ghe_{is} \\
&= [j = r]\rho(g)\lambda_i\lambda_j^{-1}\rho(h)\lambda_j\lambda_s^{-1}ghe_{is} \\
&= [j = r]\rho(g)\rho(h)\lambda_i\lambda_s^{-1}ghe_{is} \\
&= [j = r]\rho(gh)\lambda_i\lambda_s^{-1}ghe_{is} \\
&= [j = r]\chi(ghe_{is})ghe_{is} \\
&= [j = r]\tau_\chi(ghe_{is}) \\
&= \tau_\chi(ge_{ij} \cdot he_{rs}),
\end{aligned}
\qquad
\begin{aligned}
\tau_\chi(1_H) &= \sum_{i=1}^n \tau_\chi(e_G e_{ii}) \\
&= \sum_{i=1}^n \chi(e_G e_{ii})e_G e_{ii} \\
&= \sum_{i=1}^n \rho(e_G)\lambda_i\lambda_i^{-1}e_G e_{ii} \\
&= \sum_{i=1}^n 1_k e_G e_{ii} \\
&= 1_H,
\end{aligned}$$

ou seja, $\tau_\chi \in End_k(H)$ é um morfismo de álgebras, portanto χ é um caracter fraco de H. Reciprocamente, suponha que χ é um caracter fraco de H. Como τ_χ é unitário,

$$\sum_{i=1}^{n} e_G e_{ii} = 1_H = \tau_\chi(1_H) = \sum_{i=1}^{n} \tau_\chi(e_G e_{ii}) = \sum_{i=1}^{n} \chi(e_G e_{ii}) e_G e_{ii}.$$

Como $\{ge_{ii} \colon g \in G, i = 1, \dots, n\}$ é um conjunto linearmente independente sobre k, segue que $\chi(e_G e_{ii}) = 1_k$, para todo $i = 1, \dots, n$. Mais ainda, dados $i, j = 1, \dots, n$, temos

$$\begin{aligned}
\chi(e_G e_{ij}) e_G e_{ij} &= \tau_\chi(e_G e_{i1} \cdot e_G e_{1j}) \\
&= \tau_\chi(e_G e_{i1}) \tau_\chi(e_G e_{1j}) \\
&= \chi(e_G e_{i1}) e_G e_{i1} \cdot \chi(e_G e_{1j}) e_G e_{1j} \\
&= \chi(e_G e_{i1}) \chi(e_G e_{1j}) e_G e_{ij}.
\end{aligned}$$

Comparando os coeficientes de $e_G e_{ij}$ obtemos $\chi(e_G e_{ij}) = \chi(e_G e_{i1})\chi(e_G e_{1j})$. Em particular, tomando $i = j$, segue que $1_k = \chi(e_G e_{i1})\chi(e_G e_{1i})$, ou seja, $\chi(e_G e_{i1}) = \chi(e_G e_{1i})^{-1}$. Denotando $\lambda_i = \chi(e_G e_{i1}) \in \mathcal{U}(k)$, segue que

$$\chi(e_G e_{ij}) = \chi(e_G e_{i1})\chi(e_G e_{1j}) = \chi(e_G e_{i1})\chi(e_G e_{j1})^{-1} = \lambda_i \lambda_j^{-1}.$$

Sejam $g, h \in G$ e $i, j \in \{1, \dots, n\}$, então, para todo $l = 1, \dots, n$, temos

$$\begin{aligned}
\chi(ghe_{ij}) ghe_{ij} &= \tau_\chi(ghe_{ij}) \\
&= \tau_\chi(ge_{il} \cdot he_{lj}) \\
&= \tau_\chi(ge_{il}) \tau_\chi(he_{lj}) \\
&= \chi(ge_{il}) ge_{il} \cdot \chi(he_{lj}) he_{lj} \\
&= \chi(ge_{il}) \chi(he_{lj}) ghe_{ij}.
\end{aligned}$$

Comparando os coeficientes de ghe_{ij} obtemos que $\chi(ghe_{ij}) = \chi(ge_{il})\chi(he_{lj})$, para todo $l = 1, \dots, n$. Tomando $i = j = l = 1$ segue que $\chi(ghe_{11}) = \chi(ge_{11})\chi(he_{11})$ e $\chi(e_G e_{11}) = \lambda_1 = 1_k$. Em particular $1_k = \chi(e_G e_{11}) = \chi(ge_{11})\chi(g^{-1}e_{11})$, ou seja, $\chi(g^{-1}e_{11}) = \chi(ge_{11})^{-1}$. Assim, $\rho(g) := \chi(ge_{11}) \in \mathcal{U}(k)$ define um morfismo de grupos. Mais ainda

$$h = e_G, j = i, l = 1 \implies \chi(ge_{ii}) = \chi(ge_{i1})\chi(e_G e_{1i}),$$

e

$$g = e_G, j = i = 1 \implies \chi(ge_{11}) = \chi(e_G e_{1l})\chi(ge_{l1}).$$

Como k é um anel comutativo e a segunda identidade vale para todo $l = 1, \dots, n$, temos

$$\chi(ge_{ii}) = \chi(ge_{i1})\chi(e_G e_{1i}) = \chi(e_G e_{1i})\chi(ge_{i1}) = \chi(ge_{11}) = \rho(g).$$

Por fim, tomando $h = e_G$ e $l = i$, segue que

$$\chi(ge_{ij}) = \chi(ge_{ii})\chi(e_G e_{ij}) = \rho(g)\lambda_i \lambda_j^{-1}.$$

□

Como consequência do lema acima, todo caracter fraco $\chi \in Hom_k(H, k)$ é inversível no anel de convolução, com inverso $\chi \circ S$. De fato, temos

$$(\chi * (\chi \circ S))(ge_{ij}) = \chi(ge_{ij})\chi(S(ge_{ij}))$$

$$\begin{aligned}
&= \chi(ge_{ij})\chi(g^{-1}e_{ji}) \\
&= \rho(g)\lambda_i\lambda_j^{-1} \cdot \rho(g^{-1})\lambda_j\lambda_i^{-1} \\
&= \rho(g)\rho(g^{-1}) \cdot \lambda_i\lambda_i^{-1} \cdot \lambda_j^{-1}\lambda_j \\
&= \rho(e_G) = 1_k = \epsilon(ge_{ij}),
\end{aligned}$$

e analogamente $(\chi \circ S) * \chi = \epsilon$. Pelo Lema 2.3.4, temos que τ_χ é sempre um automorfismo.

Exemplo 3.3.11. Sejam G um grupo, $n \geq 1$, $H = M_n(kG)$, $\chi \in X_w^l(H)$ e $g \in Z(G)$. Suponha que $\alpha\colon H \to k$ seja um morfismo de k-módulos satisfazendo $\alpha(e_{ii}) = 0$, para todo $i = 1, \dots, n$, e

$$\alpha(ab) = \alpha(a)\epsilon(b) + \chi(a)\alpha(b), \quad \forall a, b \in H.$$

Considere $\delta\colon H \to H$, dada por $\delta(a) = (1_H - g)\tau_\alpha^l(a)$, para todo $a \in H$. Então δ é uma τ_χ^l-derivação, uma $(g, 1_H)$-coderivação e $H[X; \sigma, \delta]$ é uma extensão de Hopf-Ore primitiva fraca de H.

Demonstração. Se $g \in Z(G)$, então $g := g1_H \in H$ é um elemento group-like fraco, central e inversível. Como $H_s = \bigoplus_{i=1}^n ke_{ii}$, a hipótese $\alpha(e_{ii}) = 0$, para todo $i = 1, \dots, n$, implica em $\alpha(H_s) = 0$, ou seja, $\alpha \circ \epsilon_s = 0$. Como observado acima, $\chi \in X_w^l(H)$ implica em $\chi \circ S = \chi^{-1}$ na álgebra de convolução $End_k(H)$. Assim, o exemplo segue da Proposição 2.4.14. □

Este exemplo foi apresentado em [16, Theorem 5.2]. Quando $n = 1$ (neste caso $H = kG$ é uma álgebra de Hopf) e k não possui idempotentes não triviais, o exemplo acima contém todas as derivações que definem extensões de Hopf-Ore primitivas de kG (vide [20, Proposition 2.2] ou Corolário 3.3.15 adiante). O próximo resultado desta seção caracteriza as derivações de $M_n(kG)$ que definem extensões de Hopf-Ore primitivas fracas de $M_n(kG)$.

Dados g um elemento group-like fraco, central e inversível, e χ um caracter fraco satisfazendo $\chi^{-1} = \chi \circ S$, para obtermos as extensões de Hopf-Ore do Teorema 2.4.13, resta determinar os morfismos $\delta \in End_k(H)$ que são τ_χ-derivações, $(g, 1_H)$-coderivações, satisfazem $\delta(H_s) = 0$ e

$$(S \circ \delta)(x) = S(g)(\delta \circ S \circ \sigma)(x), \quad \forall x \in H.$$

Definição 3.3.12. Sejam G um grupo, A um grupo abeliano e $\rho\colon G \to Aut(A)$ um morfismo de grupos. Dizemos que $\gamma\colon G \to A$ é um **1-cociclo** associado a ρ se, para quaisquer $g, h \in G$, vale $\gamma(gh) = \gamma(g) + (\rho_g \circ \gamma)(h)$.

Se G é um grupo e k é um anel comutativo, então $\mathcal{U}(k)$ com a multiplicação é um grupo abeliano. Mais ainda, $\Gamma\colon \mathcal{U}(k) \to Aut(k)$, definida por $\Gamma(u)(r) = ur$, para todo $u \in \mathcal{U}(k)$ e $r \in k$, define um monomorfismo de grupos. Assim, podemos considerar $\mathcal{U}(k) \subseteq Aut(k)$, via multiplicação. Nesse caso, com $A = (k, +)$, um 1-cociclo associado a $\rho\colon G \to \mathcal{U}(k) \subseteq Aut(k)$ é uma função $\gamma\colon G \to k$, tal que $\gamma(gh) = \gamma(g) + (\Gamma_{\rho(g)} \circ \gamma)(h) = \gamma(g) + \rho(g)\gamma(h)$.

Proposição 3.3.13. *Sejam $H = M_n(kG)$, $\chi = (\rho, \lambda_1, \dots, \lambda_n) \in X_w^l(H)$ um caracter fraco e $x = \sum_{i=1}^n \sum_{j=1}^m r_j g_j e_{ii} \in G_w(H)$ um elemento group-like fraco, central e inversível. Então $\delta \in End_k(H)$ é uma τ_χ-derivação e uma $(x, 1_H)$-coderivação se, e somente se, para cada $q \in \{1, \dots, m\}$, existem 1-cociclos $\gamma_q\colon G \to r_q k$ associados a ρ e elementos $\omega_{qi} \in r_q k$, onde $\omega_{q1} = 0$, tais que*

$$\delta(a) = \sum_{q=1}^m (e - g_q)\tau_{\alpha_q}(a), \quad \forall a \in H, \quad \textit{onde} \quad \alpha_q(ge_{ij}) = \lambda_i\gamma_q(g) + \omega_{qi} - \rho(g)\lambda_i\lambda_j^{-1}\omega_{qj}.$$

Demonstração. Esta demonstração será feita em quatro partes. Na primeira parte, vamos utilizar um método semelhante ao apresentado por Panov em [20, Proposition 2.2], obtendo uma expressão para δ nos conjuntos $Ge_{ii} \simeq G$. Em seguida, vamos utilizar que $M_n(kG)$ é um módulo à esquerda livre sobre kG, com base $B = \{e_{ij} \colon i, j = 1, \ldots, n\}$, para obter uma expressão para δ nos elementos de B. Na terceira parte, utilizamos as propriedades de δ para relacionar as expressões de $\delta(ae_{ii})$ e $\delta(e_{ij})$, obtendo a equação geral para δ. Na última parte, mostramos a recíproca do enunciado.

Parte 1. Seja $a \in G$, então $a^{-1} = \sum_i a^{-1}e_{ii}$ é um elemento group-like fraco de H. Fixado $p \in \{1, \ldots, n\}$, denote $c = \delta(ae_{pp})a^{-1}$. Então

$$\begin{aligned}
\Delta(c) &= \Delta(\delta(ae_{pp}))\Delta(a^{-1}) \\
&= (xae_{pp} \otimes \delta(ae_{pp}) + \delta(ae_{pp}) \otimes ae_{pp})(a^{-1} \otimes a^{-1})\Delta(1_H) \qquad (\delta\ (x,1) - cod.) \\
&= (xe_{pp} \otimes c + c \otimes e_{pp})\Delta(1_H).
\end{aligned}$$

Como $\Delta(1) \in Z(H \otimes H)$, segue que c é um elemento (xe_{pp}, e_{pp})-primitivo fraco. Pelo Lema 3.3.9, o elemento $x \in G_w(H)$ é da forma $\sum_{i=1}^n \sum_{j=1}^m r_j g_j e_{ii}$. Assim, a igualdade acima pode ser reescrita como

$$\begin{aligned}
\Delta(c) &= \left(\sum_{i=1}^{n} \sum_{j=1}^{m} r_j g_j e_{ii} e_{pp} \otimes c + c \otimes e_{pp} \right) \Delta(1_H) \\
&= \left(\left(\sum_{j=1}^{m} r_j g_j \right) e_{pp} \otimes c + c \otimes e_{pp} \right) \Delta(1_H).
\end{aligned}$$

Fixado $q \in \{1, \ldots, m\}$, multiplicando a igualdade acima por r_q obtemos

$$\begin{aligned}
\Delta(r_q c) &= r_q \left(\left(\sum_{j=1}^{m} r_j g_j \right) e_{pp} \otimes c + c \otimes e_{pp} \right) \Delta(1_H) \\
&= (g_q e_{pp} \otimes r_q c + r_q c \otimes e_{pp})\Delta(1_H) \\
&= g_q e_{pp} \otimes r_q c e_{pp} + r_q c e_{pp} \otimes e_{pp}.
\end{aligned}$$

Assim, $r_q c$ é um elemento $(g_q e_{pp}, e_{pp})$-primitivo fraco. Como $M_n(kG)$ é um módulo livre sobre k com base $\{ge_{ij} \colon g \in G, i, j = 1, \ldots, n\}$, podemos considerar morfismos $\pi^b_{rs} \in Hom_k(H, k)$ tais que $\pi^b_{rs}(ge_{ij}) = [i = r, j = s, g = b]$. Denotando $r_q c = \sum_{i,j,g} \alpha^g_{ij} g e_{ij} \in H$, se $r \neq p$, $s \neq p$ ou $b \notin \{e, g_q\}$, segue que

$$\begin{aligned}
\alpha^b_{ij} = \mu(\pi^b_{rs} \otimes \pi^b_{rs}) \left(\sum_{i,j,g} \alpha^b_{ij} (ge_{ij} \otimes ge_{ij}) \right) &= (\pi^b_{rs} * \pi^b_{rs})(r_q c) \\
= r_q \pi^b_{rs}(g_q e_{pp}) \pi^b_{rs}(ce_{pp}) + r_q \pi^b_{rs}(ce_{pp}) \pi^b_{rs}(ee_{pp}) &= 0,
\end{aligned}$$

ou seja, $r_q c = (\alpha^e_{pp} e + \alpha^{g_q}_{pp} g_q) e_{pp} = r_q(\alpha^e_{pp} e + \alpha^{g_q}_{pp} g_q) e_{pp}$. Substituindo na identidade anterior, temos

$$\begin{aligned}
&\alpha^e_{pp}(ee_{pp} \otimes ee_{pp}) + \alpha^{g_q}_{pp}(g_q e_{pp} \otimes g_q e_{pp}) \\
&= \Delta(r_q c) \\
&= g_q e_{pp} \otimes r_q c e_{pp} + r_q c e_{pp} \otimes e_{pp}
\end{aligned}$$

$$= g_q e_{pp} \otimes r_q((\alpha^e_{pp} e + \alpha^{g_q}_{pp} g_q)e_{pp})e_{pp} + r_q((\alpha^e_{pp} e + \alpha^{g_q}_{pp} g_q)e_{pp})e_{pp} \otimes e_{pp}$$
$$= r_{pq}[\alpha^e_{pp} + \alpha^{g_q}_{pp}](g_q e_{pp} \otimes ee_{pp}) + [r_q\alpha^{g_q}_{pp}](g_q e_{pp} \otimes g_q e_{pp}) + [r_q\alpha^e_{pp}](ee_{pp} \otimes ee_{pp}).$$

Como $M_n(kG) \otimes M_n(kG)$ é um $k \otimes k \simeq k$ módulo livre com base $\{ge_{ij} \otimes he_{rs}\}$, obtemos

$$r_q\alpha^e_{pp} = \alpha^e_{pp}, \quad r_q\alpha^{g_q}_{pp} = \alpha^{g_q}_{pp} \quad \text{e} \quad 0 = r_q(\alpha^e_{pp} + \alpha^{g_q}_{pp}) = \alpha^e_{pp} + \alpha^{g_q}_{pp}.$$

Denotando $\alpha_q(ae_{pp}) = \alpha^e_{pp} = -\alpha^{g_q}_{pp}$, temos $r_q\delta(ae_{pp})a^{-1} = r_q c = \alpha_q(ae_{pp})(e - g_q)e_{pp}$, ou ainda, $r_q\delta(ae_{pp}) = \alpha_q(ae_{pp})(e - g_q)ae_{pp}$. Segue do Lema 2.3.12 que $\delta_q := r_q\delta$ é uma τ_χ-derivação de H. Se $g_q = e$ então $\delta_q = 0$. Suponha que $g_q \neq e$ e sejam $a, b \in G$, então

$$\begin{aligned}
&\alpha_q(abe_{pp})abe_{pp} - \alpha_q(abe_{pp})abg_q e_{pp}\\
&= \alpha_q(abe_{pp})(e - g_q)abe_{pp}\\
&= \delta_q(abe_{pp})\\
&= \delta_q(ae_{pp} \cdot be_{pp})\\
&= \delta_q(ae_{pp})b + \tau_\chi(ae_{pp})\delta_q(be_{pp})\\
&= [\alpha_q(ae_{pp})(e - g_q)ae_{pp}] \cdot b + \chi(ae_{pp})ae_{pp} \cdot [\alpha_q(be_{pp})(e - g_q)be_{pp}]\\
&= [\alpha_q(ae_{pp}) + \chi(ae_{pp})\alpha_q(be_{pp})]abe_{pp} - [\alpha_q(ae_{pp}) + \chi(ae_{pp})\alpha_q(be_{pp})]g_q abe_{pp}.
\end{aligned}$$

Como $g_q \neq e$, temos que $ab \neq abg_q \in G$, logo $\{abe_{pp}, abg_q e_{pp}\}$ é linearmente independente sobre k. Assim, segue da igualdade acima que

$$\alpha_q(abe_{pp}) = \alpha_q(ae_{pp}) + \chi(ae_{pp})\alpha_q(be_{pp}).$$

Em particular, tomando $a = b = e$ e utilizando que $\chi(e_{pp}) = \lambda_p\lambda_p^{-1} = 1_k$, vide Lema 3.3.10, obtemos $\alpha_q(ee_{pp}) = \alpha_q(ee_{pp}) + \alpha_q(ee_{pp})$, de onde $\alpha_q(ee_{pp}) = 0$, ou seja, $\delta_q(ee_{pp}) = 0$, para todo $q = 1, \ldots, m$. Mais ainda

$$\delta(ee_{pp}) = \sum_{q=1}^{m} r_q\delta(ee_{pp}) = \sum_{q=1}^{m} \delta_q(ee_{pp}) = 0.$$

Parte 2. Utilizando que $M_n(kG)$ é um módulo à esquerda livre sobre kG com base $\{e_{ij}\}$, escreva $\delta(e_{rs}) = \sum_{k,l} g^{rs}_{kl} e_{kl}$, onde $g^{rs}_{kl} \in kG$. Como δ é uma τ_χ-derivação, temos

$$\begin{aligned}
\delta(e_{ij}e_{rs}) &= \delta(e_{ij})e_{rs} + \tau_\chi(e_{ij})\delta(e_{rs})\\
&= \delta(e_{ij})e_{rs} + \lambda_i\lambda_j^{-1}e_{ij}\delta(e_{rs}) \qquad 3.3.10\\
&= \sum_{k,l} g^{ij}_{kl}e_{kl} \cdot e_{rs} + \lambda_i\lambda_j^{-1}e_{ij} \cdot g^{rs}_{kl}e_{kl}\\
&= \sum_{k,l} [l = r]g^{ij}_{kr}e_{ks} + [k = j]\lambda_i\lambda_j^{-1}g^{rs}_{jl}e_{il}\\
&= \sum_{k} g^{ij}_{kr}e_{ks} + \lambda_i\lambda_j^{-1}\sum_{l} g^{rs}_{jl}e_{il}.
\end{aligned}$$

No cálculo acima, se $(i, j) = (s, r)$, então $\delta(e_{ij}e_{rs}) = \delta(e_{ij}e_{ji}) = \delta(ee_{ii}) = 0$. Por outro lado, se $j \neq r$, então $\delta(e_{ij}e_{rs}) = [j = r]\delta(e_{is}) = 0$. Em ambos os casos, a igualdade anterior se torna $\sum_k g^{ij}_{kr}e_{ks} = -\lambda_i\lambda_j^{-1}\sum_l g^{rs}_{jl}e_{il}$. Defina morfismos $\pi_{-t}, \pi_{t-} \in Hom_{kG}(H, kG)$, respectivamente, por $\pi_{-t}(e_{rs}) = [s = t]$ e $\pi_{t-}(e_{rs}) = [r = t]$. Assim, se $t \neq s$, então

$$0 = \pi_{-t}\left(\sum_k g^{ij}_{kr}e_{ks}\right) = \pi_{-t}\left(-\lambda_i\lambda_j^{-1}\sum_l g^{rs}_{jl}e_{il}\right) = -\lambda_i\lambda_j^{-1}g^{rs}_{jt}.$$

Como $\lambda_i, \lambda_j \in \mathcal{U}(k)$, segue que $g_{jt}^{rs} = 0$, para todo $t \neq s$. Analogamente, se $t \neq i$, então

$$0 = \pi_{t-}\left(-\lambda_i\lambda_j^{-1}\sum_l g_{jl}^{rs}e_{il}\right) = \pi_{t-}\left(\sum_k g_{kr}^{ij}e_{ks}\right) = g_{tr}^{ij}.$$

Em suma, $(i, j) = (s, r)$ ou $j \neq r$ implicam $g_{jt}^{rs} = 0$, $\forall t \neq s$ e $g_{tr}^{ij} = 0$, $\forall t \neq i$.

Fixe $u, v \in \{1, \ldots, n\}$ e considere $\delta(e_{uv}) = \sum_{k,l} g_{kl}^{uv}e_{kl}$ na sua representação matricial, com coeficientes em kG. Escolhendo $(r, s) = (u, v)$, $j \neq u$ e variando $i \in \{1, \ldots, n\}$, temos que $j \neq r$, de onde segue que $0 = g_{jt}^{rs} = g_{jt}^{uv}$, para todo $t \neq v$, ou seja, todas as entradas de $\delta(e_{uv})$, exceto talvez pela u-ésima linha e pela v-ésima coluna, são nulas. Escolhendo $(i, j) = (u, v)$ e $(r, s) = (v, u)$ temos $(i, j) = (s, r)$, de onde segue que $0 = g_{tr}^{ij} = g_{tv}^{uv}$, para todo $t \neq u$. Ou seja, na v-ésima coluna de $\delta(e_{uv})$, todas as entradas, exceto talvez pela u-ésima linha, são nulas. Escolhendo $(r, s) = (u, v)$ e $(i, j) = (v, u)$, temos $(i, j) = (s, r)$, de onde segue que $0 = g_{jt}^{rs} = g_{ut}^{uv}$, para todo $t \neq v$. Ou seja, na u-ésima linha de $\delta(e_{uv})$, todas as entradas, exceto talvez pela v-ésima coluna, são nulas. Resta que $\delta(e_{uv}) = g_{uv}^{uv}e_{uv}$.

Fixado $w \in \{1, \ldots, m\}$, escreva $r_w g_{uv}^{uv} = \sum_{g\in G}\alpha_g g \in kG$. Então

$$\begin{aligned}
\sum_{g\in G}\alpha_g(ge_{uv}\otimes ge_{uv}) &= \sum_{g\in G}\Delta(\alpha_g ge_{uv}) = \Delta(r_w g_{uw}^{uw}e_{uv}) = \Delta(r_w\delta(e_{uv}))\\
&= r_w x e_{uv}\otimes r_w\delta(e_{uv}) + r_w\delta(e_{uv})\otimes e_{uv}\\
&= \sum_{g\in G} r_w\left(\sum_{i,j} r_j g_j e_{ii}\right)e_{uv}\otimes\alpha_g ge_{uv} + \alpha_g ge_{uv}\otimes e_{uv}\\
&= \sum_{g\in G}\left(\sum_j r_w r_j g_j\right)e_{uv}\otimes\alpha_g ge_{uv} + \alpha_g ge_{uv}\otimes e_{uv}\\
&= \sum_{g\in G} r_w g_w e_{uv}\otimes\alpha_g ge_{uv} + \alpha_g ge_{uv}\otimes e_{uv}.
\end{aligned}$$

Considere os morfismos $\eta_{rs}^b \in Hom_k(H, k)$ definidos por $\eta_{rs}^b(ge_{ij}) = [i = r, j = s, g = b]$. Então, para $b \notin \{e, g_w\}$, temos

$$\begin{aligned}
\alpha_b &= \sum_{g\in G}\alpha_g\eta_{uv}^b(ge_{uv})^2 = (\eta_{uv}^b * \eta_{uv}^b)(\delta(r_v e_{uv}))\\
&= \sum_{g\in G} r_v\alpha_g\eta_{uv}^b(g_w e_{uv})\eta_{uv}^b(ge_{uv}) + \alpha_g\eta_{uv}^b(ge_{uv})\eta_{uv}^b(ee_{uv}) = 0.
\end{aligned}$$

Logo $r_w\delta(e_{uv}) = (\alpha_e e + \alpha_{g_w}g_w)e_{uv} = r_w(\alpha_e e + \alpha_{g_w}g_w)e_{uv}$. Com isso,

$$\begin{aligned}
&\alpha_e(ee_{uv}\otimes ee_{uv}) + \alpha_{gw}(g_w e_{uv}\otimes g_w e_{uv})\\
&= \Delta(r_w\delta(e_{uv})) = r_w\delta(e_{uv})\otimes ee_{uv} + g_w e_{uv}\otimes r_w\delta(e_{uv})\\
&= r_w(\alpha_e e + \alpha_{g_w}g_w)e_{uv}\otimes ee_{uv} + g_w e_{uv}\otimes r_w(\alpha_e e + \alpha_{g_w}g_w)e_{uv}\\
&= r_w\alpha_e ee_{uv}\otimes ee_{uv} + r_w\alpha_{g_w}g_w e_{uv}\otimes ee_{uv}\\
&\quad + r_w g_w e_{uv}\otimes\alpha_e ee_{uv} + r_w ee_{uv}\otimes\alpha_{g_w}g_w e_{uv}\\
&= [r_w\alpha_e](ee_{uv}\otimes ee_{uv}) + [r_w\alpha_{gw}](g_w e_{uv}\otimes g_w e_{uv})\\
&\quad + r_w[\alpha_e + \alpha_{g_w}](g_w e_{uv}\otimes ee_{uv}).
\end{aligned}$$

Igualando os coeficientes na primeira e última escrita acima, segue que

$$r_w\alpha_e = \alpha_e, \quad r_w\alpha_{g_w} = \alpha_{g_w} \quad \text{e} \quad 0 = r_w(\alpha_e + \alpha_{g_w}) = \alpha_e + \alpha_{g_w}.$$

Denotando $\alpha_w(e_{uv}) = \alpha_e = -\alpha_{g_w}$, temos que $r_w\delta(e_{uv}) = \alpha_w(e_{uv})(e - g_w)e_{uv}$.

Parte 3. Neste ponto, sabemos que

$$\delta(ae_{ii}) = \sum_{q=1}^{m} r_q\delta(ae_{ii}) = \sum_{q=1}^{m} \alpha_q(ae_{ii})(e - g_q)ae_{ii}, \qquad \forall a \in G, i = 1, \dots, n,$$
$$\delta(ee_{ij}) = \sum_{q=1}^{m} r_q\delta(e_{ij}) = \sum_{q=1}^{m} \alpha_q(ee_{ij})(e - g_q)ee_{ij}, \qquad \forall i, j = 1, \dots, n,$$

onde $\alpha_q(ae_{ii}) \in r_qk$, $\alpha_q(ee_{ij}) \in r_qk$ e $\alpha_q(ee_{ii}) = 0$, para todo $q = 1, \dots, m$. Quando $g_q = e$, as parcelas $\alpha_q(ee_{ij})(e - g_q)e_{ij}$ e $\alpha_q(ae_{ii})(e - g_q)ae_{ij}$ são nulas, assim, podemos supor $\alpha_q(e_{ij}) = \alpha_q(ae_{ii}) = 0$, de forma que toda identidade cujo todo termo dependa de α_q é (nula, portanto) válida. Caso contrário, ee_{ij} e g_qe_{ij} são linearmente independentes sobre k. Neste caso, tomando $i, j \in \{1, \dots, n\}$, como δ é uma τ_χ-derivação, temos

$$\begin{aligned}
&\sum_{q=1}^{m} \alpha_q(e_{ij})(e - g_q)e_{ij} \\
&= \delta(e_{ij}) = \delta(e_{il} \cdot e_{lj}) \\
&= \delta(e_{il})e_{lj} + \tau_\chi(e_{il})\delta(e_{lj}) \\
&= \delta(e_{il})e_{lj} + \lambda_i\lambda_l^{-1}e_{il}\delta(e_{lj}) \\
&= \sum_{q=1}^{m} \alpha_q(e_{il})(e - g_q)e_{il} \cdot e_{lj} + \lambda_i\lambda_l^{-1}e_{il} \cdot \alpha_q(e_{lj})(e - g_q)e_{lj} \\
&= \sum_{q=1}^{m} [\alpha_q(e_{il}) + \lambda_i\lambda_l^{-1}\alpha_q(e_{lj})](e - g_q)e_{ij}.
\end{aligned} \tag{3.3.10}$$

Ou seja, para todo $l = 1, \dots, n$ e $q = 1, \dots, m$, vale $\alpha_q(e_{ij}) = \alpha_q(e_{il}) + \lambda_i\lambda_l^{-1}\alpha_q(e_{lj})$. Como $\alpha_q(e_{ii}) = 0$, tomando $j = i$ e $l = 1$ no cálculo acima, temos que $\alpha_q(e_{i1}) = -\lambda_i\alpha_q(e_{1i})$, ou ainda, $\alpha_q(e_{1i}) = -\lambda_i^{-1}\alpha_q(e_{i1})$. Assim

$$\alpha_q(ee_{ij}) = \alpha_q(ee_{i1}) - \lambda_i\lambda_j^{-1}\alpha_q(ee_{j1}), \quad \forall q = 1, \dots, m.$$

Agora, dados $a \in G$ e $i, j \in \{1, \dots, n\}$, temos

$$\begin{aligned}
\delta(ae_{ij}) &= \delta(ae_{ii} \cdot ee_{ij}) \\
&= \delta(ae_{ii})e_{ij} + \tau_\chi(ae_{ii})\delta(ee_{ij}) \\
&= \delta(ae_{ii})e_{ij} + \rho(a)\lambda_i\lambda_j^{-1}ae_{ij}\delta(ee_{ij}) \\
&= \sum_{q=1}^{m} \alpha_q(ae_{ii})ae_{ii} \cdot e_{ij} + \rho(a)ae_{ii} \cdot \alpha_q(ee_{ij})ee_{ij} \\
&= \sum_{q=1}^{m} [\alpha_q(ae_{ii}) + \rho(a)\alpha_q(ee_{ij})]ae_{ij}
\end{aligned}$$

$$= \sum_{q=1}^{m} [\alpha_q(ae_{ii}) + \rho(a)[\alpha_q(ee_{i1}) - \lambda_i \lambda_j^{-1} \alpha_q(ee_{j1})] ae_{ij}.$$

Por outro lado, temos

$$\begin{aligned}
\delta(ae_{ij}) &= \delta(e_{i1} \cdot ae_{1j}) \\
&= \delta(e_{i1}) ae_{1j} + \tau_\chi(e_{i1}) \delta(ae_{1j}) \\
&= \delta(e_{i1}) ae_{1j} + \lambda_i e_{i1} \delta(ae_{1j}) \\
&= \sum_{q=1}^{m} \alpha_q(e_{i1})(e - g_q) e_{i1} \cdot ae_{1j} + \lambda_i e_{i1} \cdot \alpha(ae_{1j})(e - g_q) ae_{1j} \\
&= \sum_{q=1}^{m} \alpha_q(e_{i1})(e - g_q) ae_{ij} + \lambda_i [\alpha_q(ae_{11}) - \rho(a) \lambda_j^{-1} \alpha_q(ee_{j1})](e - g_q) ae_{ij} \\
&= \sum_{q=1}^{m} [\alpha_q(e_{i1}) + \lambda_i \alpha_q(ae_{11}) - \rho(a) \lambda_i \lambda_j^{-1} \alpha_q(ee_{j1})](e - g_q) ae_{ij}.
\end{aligned}$$

Igualando os coeficientes em ambas as escritas de $\delta(ae_{ij})$, obtemos as igualdades

$$\begin{gathered}
\alpha_q(ae_{ii}) + \rho(a)\alpha_q(ee_{i1}) - \rho(a)\lambda_i\lambda_j^{-1}\alpha_q(ee_{j1}) = \alpha_q(ee_{i1}) + \lambda_i\alpha_q(ae_{11}) - \rho(a)\lambda_i\lambda_j^{-1}\alpha_q(ee_{j1}), \\
\alpha_q(ae_{ii}) + \rho(a)\alpha_q(ee_{i1}) = \alpha_q(ee_{i1}) + \lambda_i\alpha_q(ae_{11}), \\
\alpha_q(ae_{ii}) = \lambda_i\alpha_q(ae_{11}) + (1_k - \rho(a))\alpha_q(ee_{i1}).
\end{gathered}$$

Substituindo a expressão para $\alpha_q(ae_{ii})$ na primeira escrita do coeficiente de $\delta(ae_{ij})$, temos

$$\begin{aligned}
&\alpha_q(ae_{ii}) + \rho(a)\alpha_q(ee_{i1}) - \rho(a)\lambda_i\lambda_j^{-1}\alpha_q(ee_{j1}) \\
&= [\lambda_i\alpha_q(ae_{11}) + (1_k - \rho(a))\alpha_q(ee_{i1})] + \rho(a)\alpha_q(ee_{i1}) - \rho(a)\lambda_i\lambda_j^{-1}\alpha_q(ee_{j1}) \\
&= \lambda_i\alpha_q(ae_{11}) + \alpha_q(ee_{i1}) - \rho(a)\lambda_i\lambda_j^{-1}\alpha_q(ee_{j1}).
\end{aligned}$$

Em suma, para cada $q = 1, \ldots, m$, defina uma função $\gamma_q \colon G \to r_q k$, um morfismo $\alpha_q \in Hom_k(H, k)$ e elementos $\omega_{qi} \in r_q k$, por

$$\begin{aligned}
\gamma_q(a) &= \alpha_q(ae_{11}), && \forall a \in G, \\
\omega_{qi} &= \alpha_q(ee_{i1}), && \forall i = 1, \ldots, n, \\
\alpha_q(ae_{ij}) &= \lambda_i\alpha_q(ae_{11}) + \alpha_q(ee_{i1}) - \rho(a)\lambda_i\lambda_j^{-1}\alpha_q(ee_{j1}), && \forall a \in G, i, j = 1, \ldots, n.
\end{aligned}$$

Então $\delta(ae_{ij}) = \sum_{q=1}^{m}(e - g_q)\tau_{\alpha_q}(ae_{ij})$. Ainda, para todo $q = 1, \ldots, m$, temos que vale $\omega_{q1} = \alpha_q(ee_{11}) = 0$, e a função γ_q satisfaz

$$\gamma_q(ab) = \alpha_q(abe_{11}) = \alpha_q(ae_{11}) + \chi(ae_{11})\alpha_q(be_{11}) = \gamma_q(a) + \rho(a)\gamma_q(b).$$

Ou seja, cada $\gamma_q \colon G \to r_q k \subseteq k$ é um 1-cociclo associado a ρ. Isso mostra ($\Rightarrow$).

Parte 4. Para a recíproca, sejam $\gamma_q \colon G \to r_q k \subseteq l$ 1-cociclos associados a ρ, para cada $i = 1, \ldots, n$, escolha $\omega_{qi} \in r_q k$, onde $\omega_{q1} = 0$, e defina $\delta(ae_{ij}) = \sum_{q=1}^{m}(e - g_q)\tau_{\alpha_q}(ae_{ij})$, onde

$$\alpha_q(ae_{ij}) = \lambda_i\gamma_q(a) + \omega_{qi} - \rho(a)\lambda_i\lambda_j^{-1}\omega_{qj}.$$

Para todo $g \in G$, temos

$$\begin{aligned}
\Delta(e-g) &= \sum_{i=1}^{n} ee_{ii} \otimes ee_{ii} - ge_{ii} \otimes ge_{ii} \\
&= \sum_{i=1}^{n} (e \otimes e - g \otimes g)\Delta(e_{ii}) \\
&= (e \otimes e - g \otimes g)\Delta\left(\sum_{i=1}^{n} e_{ii}\right) \\
&= (e \otimes e - g \otimes g)\Delta(1_H) \\
&= (e \otimes e - g \otimes e + g \otimes e - g \otimes g)\Delta(1_H) \\
&= ((e-g) \otimes e + g \otimes (e-g))\Delta(1_H).
\end{aligned}$$

Como $\alpha_q(ae_{ij}) \in r_q k$, temos $\alpha_q(ae_{ij}) = \alpha_q(ae_{ij})r_q$, para todo $l = 1, \ldots, n$, logo

$$\alpha_q(ae_{ij})r_t = \alpha_q(ae_{ij})r_q r_t = [t = q]\alpha_q(ae_{ij})r_q.$$

Consequentemente,

$$\alpha_q(ae_{ij})x = \sum_{s=1}^{n}\sum_{t=1}^{m} \alpha_q(ae_{ij})r_t g_t e_{ss} = \sum_{s=1}^{n} \alpha_q(ae_{ij})r_q g_q e_{ss} = \alpha_q(ae_{ij})\sum_{s=1}^{n} g_q e_{ss}.$$

Ou ainda, $\alpha_q(ae_{ij})xae_{ij} = \alpha_q(ae_{ij})g_q ae_{ij}$. Com isso, calculamos

$$\begin{aligned}
\Delta(\delta(ae_{ij})) &= \sum_{q=1}^{m} \alpha_q(ae_{ij})\Delta(e-g_q)\Delta(ae_{ij}) \\
&= \sum_{q=1}^{m} \alpha_q(ae_{ij})((e-g_q) \otimes e + g_q \otimes (e-g_q))\Delta(ae_{ij}) \\
&= \sum_{q=1}^{m} \alpha_q(ae_{ij})((e-g_q)ae_{ij} \otimes ae_{ij} + g_q ae_{ij} \otimes (e-g_q)ae_{ij}) \\
&= \sum_{q=1}^{m} (e-g_q)\alpha_q(ae_{ij})ae_{ij} \otimes ae_{ij} + \alpha_q(ae_{ij})g_q ae_{ij} \otimes (e-g_q)ae_{ij} \\
&= \sum_{q=1}^{m} (e-g_q)\alpha_q(ae_{ij})ae_{ij} \otimes ae_{ij} + \alpha_q(ae_{ij})xae_{ij} \otimes (e-g_q)ae_{ij} \\
&= \sum_{q=1}^{m} (e-g_q)\alpha_q(ae_{ij})ae_{ij} \otimes ae_{ij} + xae_{ij} \otimes (e-g_q)\alpha_q(ae_{ij})ae_{ij} \\
&= \left(\sum_{q=1}^{m} (e-g_q)\tau_{\alpha_q}(ae_{ij})\right) \otimes ae_{ij} + xae_{ij} \otimes \left(\sum_{q=1}^{m} (e-g_q)\tau_{\alpha_q}(ae_{ij})\right) \\
&= \delta(ae_{ij}) \otimes ae_{ij} + xae_{ij} \otimes \delta(ae_{ij}) \\
&= \delta((ae_{ij})_1) \otimes 1_H(ae_{ij})_2 + x(ae_{ij})_1 \otimes \delta((ae_{ij})_2).
\end{aligned}$$

Como $\delta \in End_k(H)$ satisfaz a identidade de $(x, 1_H)$-coderivação para os elementos da base $\{ge_{ij}\}$, segue que δ é uma $(x, 1_H)$-coderivação de H. Para ver que δ é uma τ_χ-derivação, por um lado temos

$$\delta(ae_{ij} \cdot be_{rs}) = [j = r]\delta(abe_{is}) = [j = r]\sum_{q=1}^{m}(e - g_q)\alpha_q(abe_{is})abe_{is},$$

enquanto que

$$\begin{aligned}
&\delta(ae_{ij})be_{rs} + \tau_\chi(ae_{ij})\delta(be_{rs}) \\
&= \sum_{q=1}^{m}\alpha_q(ae_{ij})(e - g_q)ae_{ij} \cdot be_{rs} + \chi(ae_{ij})ae_{ij} \cdot \alpha_q(be_{rs})(e - g_q)be_{rs} \\
&= [j = r]\sum_{q=1}^{m}[\alpha_q(ae_{ij}) + \chi(ae_{ij})\alpha_q(be_{js})](e - g_q)abe_{is}.
\end{aligned}$$

Como $\delta \in End_k(H)$, segue que δ é uma τ_χ-derivação se, e somente se, vale a identidade de τ_χ-derivação para os elementos da base $\{ge_{ij}\}$ se, e somente se,

$$\alpha_q(abe_{is}) = \alpha_q(ae_{ij}) + \chi(ae_{ij})\alpha_q(be_{js}), \quad \forall q = 1, \ldots, m.$$

Para isso, calculamos

$$\begin{aligned}
&\alpha_q(ae_{ij}) + \chi(ae_{ij})\alpha_q(be_{js}) \\
&= [\lambda_i\gamma_q(a) + \omega_{qi} - \rho(a)\lambda_i\lambda_j^{-1}\omega_{qj}] + \rho(a)\lambda_i\lambda_j^{-1}[\lambda_j\gamma_q(b) + \omega_{qj} - \rho(b)\lambda_j\lambda_s^{-1}\omega_{qs}] \\
&= \lambda_i\gamma_q(a) + \omega_{qi} - \rho(a)\lambda_i\lambda_j^{-1}\omega_{qj} + \rho(a)\lambda_i\gamma_q(b) + \rho(a)\lambda_i\lambda_j^{-1}\omega_{qj} - \rho(a)\lambda_i\rho(b)\lambda_s^{-1}\omega_{qs} \\
&= \lambda_i\gamma_q(a) + \omega_{qi} + \rho(a)\lambda_i\gamma_q(b) - \rho(a)\lambda_i\rho(b)\lambda_s^{-1}\omega_{qs} \\
&= \lambda_i[\gamma_q(a) + \rho(a)\gamma_q(b)] + \omega_{qi} - \rho(a)\rho(b)\lambda_i\lambda_s^{-1}\omega_{qs} \\
&= \lambda_i\gamma_q(ab) + \omega_{qi} - \rho(ab)\lambda_i\lambda_s^{-1}\omega_{qs} \\
&= \alpha_q(abe_{is}).
\end{aligned}$$

De onde segue que δ é uma τ_χ-derivação de H. $\square$

De volta à observação anterior, a fim de aplicarmos o Teorema 2.4.8, precisamos saber quais derivações de $H = M_n(kG)$, relevantes para a construção de uma extensão de Hopf-Ore primitiva fraca, satisfazem $\delta(H_s) = 0$ e $(S \circ \delta)(ge_{ij}) = S(x)(\delta \circ S \circ \sigma)(ge_{ij})$, para quaisquer $g \in G$, $i, j = 1, \ldots, n$. Para isso, calculamos

$$(S * id_H)(ge_{ij}) = S(ge_{ij})ge_{ij} = g^{-1}e_{ji} \cdot ge_{ij} = ee_{jj}.$$

De onde $H_s = im(\epsilon_s) = im(S * id_H) = \bigoplus_{i=1}^{n} kee_{ii}$. Ainda, se $\rho\colon G \to \mathcal{U}(k)$ é um morfismo de grupos e $\gamma\colon G \to k$ é um 1-cociclo associado a ρ, então

$$\gamma(e) = \gamma(e^2) = \gamma(e) + \rho(e)\gamma(e) = 2\gamma(e) \quad \therefore \quad \gamma(e) = 0.$$

Seja $\delta \in End_k(H)$ satisfazendo as hipóteses do resultado anterior. Então

$$\begin{aligned}
\delta(ee_{ii}) &= \sum_{q=1}^{m}[\lambda_i\gamma_q(e) + \omega_{qi} - \rho(e)\lambda_i\lambda_i^{-1}\omega_{qi}](e - g_q)ee_{ii} \\
&= \sum_{q=1}^{m}[\lambda_i \cdot 0 + \omega_{qi} - 1_k \cdot \omega_{qi}](e - g_q)ee_{ii} = 0.
\end{aligned}$$

Portanto toda τ_χ-derivação, $\chi \in X_w^l(H)$, que é uma $(x, 1_H)$-coderivação, $x \in G_w(H)$ central e inversível, satisfaz a condição $\delta(H_s) = 0$. Por outro lado, se γ é um 1-cociclo associado a ρ, então

$$0 = \gamma(e) = \gamma(gg^{-1}) = \gamma(g) + \rho(g)\gamma(g^{-1}).$$

De onde $\gamma(g) = -\rho(g)\gamma(g^{-1})$. Consequentemente,

$$\begin{aligned}
\alpha_q(S(ge_{ij}))\chi(ge_{ij}) &= \alpha_q(g^{-1}e_{ji}))\chi(ge_{ij}) \\
&= [\lambda_j\gamma_q(g^{-1}) + \omega_{qj} - \rho(g^{-1})\lambda_j\lambda_i^{-1}\omega_{qi}][\rho(g)\lambda_i\lambda_j^{-1}] \\
&= \lambda_i\rho(g)\gamma_q(g^{-1}) + \rho(g)\lambda_i\lambda_j^{-1}\omega_{qj} - \omega_{qi} \\
&= -\lambda_i\gamma_q(g) - \omega_{qi} + \rho(g)\lambda_i\lambda_j^{-1}\omega_{qj} \\
&= -[\lambda_i\gamma_q(g) + \omega_{qi} - \rho(g)\lambda_i\lambda_j^{-1}\omega_{qj}] \\
&= -\alpha_q(ge_{ij}).
\end{aligned}$$

Pela Parte 4 da demonstração da Proposição 3.3.13, se $x = \sum_{s=1}^n \sum_{t=1}^m r_t g_t e_{ss}$, então $\alpha_q(e_{ij})x = \alpha_q(e_{ij}) \sum_{s=1}^n r_q g_q e_{ss}$. Com isso, calculamos

$$\begin{aligned}
S(x)(\delta \circ S \circ \tau_\chi)(ge_{ij}) &= \chi(ge_{ij})S(x)(\delta \circ S)(ge_{ij}) \\
&= \sum_{q=1}^m \chi(ge_{ij})S(x)\alpha_q(S(ge_{ij}))(e - g_q)S(ge_{ij}) \\
&= \sum_{q=1}^m \sum_{s=1}^n \alpha_q(S(ge_{ij}))\chi(ge_{ij})S(g_q e_{ss})(e - g_q)S(ge_{ij}) \\
&= \sum_{q=1}^m \sum_{s=1}^n \alpha_q(S(ge_{ij}))\chi(ge_{ij})S(g_q e_{ss})S(e - g_q^{-1})S(ge_{ij}) \\
&= \sum_{q=1}^m \sum_{s=1}^n \alpha_q(S(ge_{ij}))\chi(ge_{ij})S(ge_{ij} \cdot (e - g_q^{-1}) \cdot g_q e_{ss}) \\
&= \sum_{q=1}^m \alpha_q(S(ge_{ij}))\chi(ge_{ij})S(g(g_q - e)e_{ij}) \\
&= \sum_{q=1}^m \alpha_q(S(ge_{ij}))\chi(ge_{ij})S((g_q - e)ge_{ij}) \qquad (e, g_q \in Z(G)) \\
&= \sum_{q=1}^m -\alpha_q(S(ge_{ij}))\chi(ge_{ij})S((e - g_q e)ge_{ij}) \\
&= \sum_{q=1}^m \alpha_q(ge_{ij})S((e - g_q e)ge_{ij}) \\
&= S\left(\sum_{q=1}^m (e - g_q e)\alpha_q(ge_{ij})ge_{ij}\right) \\
&= (S \circ \delta)(ge_{ij}).
\end{aligned}$$

Ou seja, toda derivação δ satisfazendo a Proposição 3.3.13 também satisfaz a identidade $S(x)(\delta \circ S \circ \tau_\chi)(a) = (S \circ \delta)(a)$, para todo $a \in H$. Reunindo os resultados desta seção com a Seção 2.4, obtemos o seguinte teorema.

Teorema 3.3.14. *Sejam G um grupo, $n \geq 1$, k um anel comutativo e $H = M_n(kG) \simeq k(G \times \mathcal{G}(I_n))$ com a estrutura de álgebra de Hopf fraca. Sejam $\sigma \in Aut_k(H)$ um morfismo de álgebras e $\delta \in End_k(H)$ uma σ-derivação. As seguintes afirmações são equivalentes:*

(1) $H[X;\sigma,\delta]$ é uma extensão de Hopf-Ore $(x, 1_H)$-primitiva fraca de H;

(2) Valem:

- *(i) $x \in H$ é um elemento group-like fraco, central e inversível;*
- *(ii) $\sigma = \tau_\chi$, para algum caracter fraco χ de H;*
- *(iii) δ é uma $(x, 1_H)$-coderivação;*

(3) Valem:

- *(i) $x = \sum_{i=1}^{n} \sum_{q=1}^{m} r_q g_q e_{ii}$, onde $g_q \in Z(G)$ e $\{r_1, \ldots, r_m\}$ é uma família de idempotentes ortogonais em k satisfazendo $\sum_{q=1}^{m} r_q = 1_k$;*
- *(ii) $\sigma\colon H \to H$ é definida por $\sigma(ge_{ij}) = \rho(g)\lambda_i\lambda_j^{-1} ge_{ij}$, onde $\rho\colon G \to \mathcal{U}(k)$ é um morfismo de grupos, $\lambda_1, \ldots, \lambda_n \in \mathcal{U}(k)$ e $\lambda_1 = 1_k$;*
- *(iii) $\delta\colon H \to H$ é definida por $\delta(ge_{ij}) = \sum_{q=1}^{m} (e - g_q)\tau_{\alpha_q}(ge_{ij})$, onde, para cada $q \in \{1, \ldots, m\}$, $\alpha_q \in Hom_k(H, k)$ é dada por*

$$\alpha_q(ge_{ij}) = \lambda_i \gamma_q(g) + \omega_{qi} - \rho(g)\lambda_i\lambda_j^{-1}\omega_{qj},$$

onde $\gamma_q\colon G \to r_q k$ é um 1-cociclo associado a ρ, $\omega_{q1}, \ldots, \omega_{qn} \in r_q k$ e $\omega_{q1} = 0$.

Demonstração. Como H é uma álgebra de Hopf fraca cocomutativa, se X é um elemento $(x, 1_H)$-primitivo fraco, segue do Lema 2.4.12 que $x \in G_w(H)$ deve ser um elemento central. Pela Proposição 2.4.4 temos que $xS(x) = 1_H$, portanto x é um elemento inversível. Assim, segue do Teorema 2.4.8(2.i) que $\sigma = \tau_\chi^l = Ad_x \circ \tau_\chi^r$, para algum caracter à esquerda fraco χ de H. Mas H é cocomutativa e $x \in Z(H) \cap \mathcal{U}(H)$, de onde

$$\tau_\chi^r(a) = (Ad_x \circ \tau_\chi^r)(a) = xa_1 u\chi(a_2)x^{-1} = u\chi(a_2)a_1 xx^{-1} = u\chi(a_1)a_2 = \tau_\chi^l(a).$$

Ou seja, χ é um caracter fraco de H. Pelo Teorema 2.4.8(2.ii), δ é uma $(x, 1_H)$-coderivação. Isso mostra (1) $\implies$ (2). A implicação (2) $\implies$ (3) segue dos Lemas 3.3.9 e 3.3.10, e da Proposição 3.3.13. Por fim, utilizando estes mesmos três resultados, temos que $x \in H$ é um elemento group-like fraco, central e inversível, $\sigma = \tau_\chi \in Aut_k(H)$ é um morfismo de álgebras e $\delta \in End_k(H)$ é uma σ-derivação que é uma $(x, 1_H)$-coderivação. Neste caso, χ é inversível na álgebra de convolução $Hom_k(H, k)$ com inverso $\chi^{-1} = \chi \circ S$, assim, segue do Lema 2.4.12 que vale

$$Ad_x \circ S = \sigma \circ S \circ \sigma.$$

Por fim, da observação anterior, δ satisfaz $\delta(H_s) = 0$ e

$$(S \circ \delta)(a) = S(x)(\delta \circ S \circ \sigma)(a), \quad \forall a \in H.$$

Aplicando o Teorema 2.4.8 obtemos que $H[X;\sigma,\delta]$ é uma extensão de Hopf-Ore primitiva fraca de H, onde X é um elemento $(x, 1_H)$-primitivo fraco. Logo (3) $\implies$ (1). $\square$

O teorema acima classifica as extensões de Hopf-Ore $(g, 1_H)$-primitivas fracas das álgebras de Hopf fracas sobre anéis comutativos, provenientes de grupóides conexos. Quando o grupóide é, na verdade, um grupo, a álgebra de grupóide é uma álgebra de Hopf. Assim, quando k é um corpo, ou, mais geralmente, um anel comutativo sem idempotentes não triviais, o teorema acima generaliza a classificação das extensões de Hopf-Ore das álgebras de grupo, apresentada por Panov em [20, Proposition 2.2].

Corolário 3.3.15. *Sejam G um grupo e k um anel comutativo sem idempotentes não triviais. Então $kG[X;\sigma,\delta]$ é uma extensão de Hopf-Ore de kG com X um elemento $(r, 1_{kG})$-primitivo se, e somente se, $r \in Z(G)$ e existem: um morfismo de grupos $\rho\colon G \to \mathcal{U}(k)$ e um 1-cociclo $\alpha\colon G \to k$ associado a ρ, tais que*

$$\sigma(g) = \rho(g)g \quad e \quad \delta(g) = \alpha(g)(e - r)g, \quad \forall g \in G.$$

Demonstração. Quando $n = 1$, $H = M_n(kG) = kG$ é uma álgebra de Hopf, assim, um elemento group-like fraco inversível é um elemento group-like e um caracter fraco é um caracter. Se k não possui idempotentes não triviais, segue do Lema 3.3.9 que $G(kG) \cap Z(kG) = Z(G)1_H$. Pelo Lema 3.3.10 temos que todo caracter $\chi\colon kG \to k$ de kG é definido por um morfismo de grupos $\rho\colon G \to \mathcal{U}(k)$. Como $r \in Z(G)1_k$, na Proposição 3.3.13 temos $m = 1$ e, como $n = 1$ e $\omega_{11} = 0$, deve ser

$$\alpha(g) := \alpha_1(g) = \lambda_1\gamma_1(g) + \omega_{11} - \rho(g)\lambda_1\lambda_1^{-1}\omega_{11} = \gamma_1(g).$$

Assim, as τ_χ-derivações que são $(r, 1_H)$-coderivações são definida por $\delta(g) = (e - r)\tau_\alpha(g)$, onde $\alpha = \gamma_1$ é um 1-cociclo associado a ρ. O resultado segue do Teorema 3.3.14. □

Seja $H = M_n(k)$, então, pelo Lema 3.3.9, o único elemento group-like fraco, central e inversível de H é $g = 1_H$. Pela Proposição 3.3.13, se δ é uma τ_χ-derivação, $\chi \in X_w^l(H)$, e uma $(1_H, 1_H)$-coderivação, então $\delta \equiv 0$. Assim, os resultados apresentados condizem com [8, Observação 2.2.3], onde é afirmado que $H = M_n(k)$ é uma coálgebra cosseparável e cocomutativa, e, neste caso todas as $(1_H, 1_H)$-coderivações de H são nulas.

Antes de apresentar exemplos de extensões de Hopf-Ore primitivas fracas utilizando o teorema anterior, gostaríamos de observar que, em posse deste resultado, vemos que, em contraste com o caso $n = 1$, para as álgebras de Hopf fracas $M_n(kG)$ que não são álgebras de Hopf, o Exemplo 3.3.11 não contém todas as derivações que definem extensões de Hopf-Ore primitivas fracas.

Quando k é um anel comutativo, a observação após o Lema 3.3.9 mostra que o Exemplo 3.3.11 não considera todos os elementos group-like fracos, centrais e inversíveis. Por outro lado, quando k não possui idempotentes não triviais, os elementos group-like fracos, centrais e inversíveis são de fato da forma $\sum_{i=1}^n g e_{ii}$, onde $g \in Z(G)$.

Exemplo 3.3.16. Sejam k um anel comutativo, G um grupo, $n > 1$, $H = M_n(kG)$ a álgebra de grupóide conexo, $\chi \in X_w^l(H)$ e $g \in Z(G)$. Suponha que $\alpha \in Hom_k(H, k)$ satisfaz $\alpha \circ \epsilon_s = 0$ e

$$\alpha(ab) = \alpha(a)\epsilon(b) + \chi(a)\alpha(b), \forall a, b \in H. \qquad (*)$$

Seja $\delta \in End_k(H)$ a τ_χ^l-derivação do Exemplo 3.3.11.

Na notação da Proposição 3.3.13, como $x = g1_{M_n(k)}$, temos que $m = 1$. Assim, devem existir: um caracter $\rho\colon G \to k$; um 1-cociclo γ associado a ρ; elementos $\lambda_1, \dots, \lambda_n \in \mathcal{U}(k)$, onde $\lambda_1 = 1_k$; e elementos $\omega_1, \dots, \omega_n \in k$, onde $\omega_1 = 0$, tais que $\chi(ge_{ij}) = \rho(g)\lambda_i\lambda_j^{-1}$ e

$$\delta(ge_{ij}) = (e - g)\tau_\beta(ge_{ij}), \quad \forall g \in G, i, j = 1, \dots, n,$$

onde $\beta\colon H \to k$ é definida por $\beta(ge_{ij}) = \lambda_i\gamma(g) + \omega_i - \rho(g)\lambda_i\lambda_j^{-1}\omega_j$. Por construção, $\beta(ge_{ij})$ é o coeficiente de $(e-g)ge_{ij}$ na escrita de $\delta(ge_{ij})$. Pelo Exemplo 3.3.11, temos que

$$\delta(ge_{ij}) = (e - g)\tau^l_\alpha(ge_{ij}) = \alpha(ge_{ij})(e - g)ge_{ij},$$

ou seja, o coeficiente de $(e - g)ge_{ij}$ na escrita de $\delta(ge_{ij})$ é $\alpha(ge_{ij})$. Portanto $\alpha = \beta$. Com isso, fixado $i > 1$, temos que

$$\begin{aligned} 0 = \alpha(0) = \alpha(e_{i1}^2) & & (i \neq 1) \\ = \alpha(e_{i1})\epsilon(e_{i1}) + \chi(e_{i1})\alpha(e_{ij}) & & (*) \\ = \omega_i + \lambda_i\omega_i & & (\alpha = \beta) \\ = \omega_i(1_k + \lambda_i). & & \end{aligned}$$

Assim, se $H[X; \sigma, \delta]$ é uma extensão de Hopf-Ore primitiva fraca, onde δ é dada como no enunciado, então os parâmetros $\lambda_2, \dots, \lambda_n \in \mathcal{U}(k)$, que definem o caracter $\chi \in X^l_w(H)$, e os parâmetros $\omega_2, \dots, \omega_n \in k$, ficam condicionados à identidade $\omega_i(1_k + \lambda_i) = 0$, para todo $i = 2, \dots, n$. Assim, se $n > 1$, o Exemplo 3.3.11 não contém todas as τ^l_χ-derivações δ que são $(g, 1_H)$-coderivações e tais que $H[X; \sigma, \delta]$ é uma extensão de Hopf-Ore primitiva fraca de $H = M_n(k)$.

No contexto de álgebras de Hopf, os morfismos $\alpha\colon H \to k$ satisfazendo $(*)$ foram chamados, em [20], de *1-cociclos de uma álgebra de Hopf associados ao caracter* χ. Neste caso, os morfismos α generalizam os 1-cociclos de um grupo G associados a um caracter $\rho\colon G \to k$. De fato, se χ é um caracter de kG, então $\chi(g) = \rho(g)$, para algum caracter $\rho\colon G \to k$ e, dados $g, h \in G$, vale $\alpha(gh) = \alpha(g)\epsilon(h) + \chi(g)\alpha(h) = \alpha(g) + \rho(g)\alpha(h)$. Assim, $\alpha|_G$ define um 1-cociclo de G associado a ρ.

Se $G = M_n(kG)$ é uma álgebra de grupóide, então sua base $\{ge_{ij}\} \simeq G \times \mathcal{G}(I_n)$ é um grupóide. Neste caso, pode-se mostrar que, dados $\chi \in X^l_w(H)$, $\alpha_q\colon H \to k$ um morfismo satisfazendo o Teorema 3.3.14 e $(x, y) \in (G \times \mathcal{G}(I_n))^2$, valem $\chi(xy) = \chi(x)\chi(y)$ e $\alpha_q(xy) = \alpha_q(x) + \chi(x)\alpha_q(y)$. Mais ainda, $\chi(e) = 1_k$, para todo $e \in (G \times \mathcal{G}(I_n))_0$. Ou seja, poderíamos dizer que $\rho = \chi|_{(G\times\mathcal{G}(I_n))}$ é um *caracter do grupóide* $G \times \mathcal{G}(I_n)$, enquanto que $\alpha_q|_{G\times\mathcal{G}(I_n)}$ é um *1-cociclo do grupóide* $G \times \mathcal{G}(I_n)$ *associado ao caracter* ρ.

Exemplo 3.3.17. Vejamos um exemplo numérico utilizando o Teorema 3.3.14.

De maneira geral, para construirmos uma extensão de Hopf-Ore primitiva fraca de $H = M_n(kG)$, precisamos encontrar:

1 - O conjunto $\mathcal{U}(k)$ dos elementos inversíveis de k;

2 - Um morfismo de grupo $\rho\colon G \to \mathcal{U}(k)$;

3 - Elementos $g_1, \dots, g_m$ no centro de G;

4 - Uma família $r_1, \dots, r_m$ de idempotentes ortogonais cuja soma é 1_k;

5 - Para cada $q = 1, \dots, m$, um 1-cociclos $\gamma_q\colon G \to r_q k$ associados a ρ;

6 - Elementos $\lambda_1, \dots, \lambda_n \in \mathcal{U}(k)$ e $\omega_{q1}, \dots, \omega_{qn} \in r_q k$, onde $\lambda_1 = 1$ e $\omega_{q1} = 0$.

Sejam $k = \mathbb{Q}$, $G = \langle h \rangle$ um grupo cíclico infinito e $n = 2$.

1 - Como $\mathbb{Q}$ é um corpo, $\mathcal{U}(\mathbb{Q}) = \mathbb{Q} \setminus \{0\} =: \mathbb{Q}^\times$.

2 - Como G é um grupo cíclico infinito, gerado por h, para determinar um morfismo de grupos $\rho\colon G \to \mathbb{Q}^\times$, basta escolher $\rho(h)$. Ainda, o morfismo estará bem determinado independente da escolha. Vamos considerar $\rho(h) = 8$.

3 e 4 - Todo grupo cíclico é abeliano, assim, $Z(G) = G$. Observe que, como $\mathbb{Q}$ é um corpo, os únicos idempotentes de $\mathbb{Q}$ são 0 e 1. Assim, para que $r_1, \dots, r_m$ seja uma família de idempotentes ortogonais satisfazendo $\sum_{q=1}^m r_q = 1$, deve existir $l \in \{1, \dots, m\}$ tal que $r_l = 1$ e $r_q = 0$, para todo $q \neq l$. Ou seja, deve ser necessariamente $m = 1$. Assim, vamos escolher $r = h^5(e_{11} + e_{22})$.

5 - Como G é um grupo cíclico, para determinar um 1-cociclo $\gamma\colon G \to \mathbb{Q}$ associado a ρ, é suficiente determinar $\gamma(h)$. Escolha $\gamma(h) = 4$. Então, para todo $s \geq 0$,

$$\gamma(h^s) = 4\sum_{t=0}^{s} 8^s = \frac{4}{7}(8^s - 1) \quad \text{e} \quad \gamma(h^{-s}) = -\rho(h^{-s})\gamma(h^s) = -\frac{4}{7}\frac{8^s - 1}{8^s}.$$

6 - Por fim, tome $\omega_{11} = 0$ e $\lambda_1 = 1$ e escolha $\omega_{12} = 9 \in \mathbb{Q}$ e $\lambda_2 = 2 \in \mathbb{Q}^\times$.

Assim, $M_2(\mathbb{Q}G)[X; \sigma, \delta]$ admite uma estrutura de álgebra de Hopf fraca sobre $\mathbb{Q}$, onde os elementos $h^s e_{ij}$, $s \in \mathbb{Z}$ e $i, j = 1, 2$, são group-like fracos, X é um elemento $(h^5(e_{11} + e_{22}), 1_H)$-primitivo fraco e a multiplicação é dada por

$$h^s e_{ij} \cdot h^t e_{rs} = [j = r] h^{s+t} e_{is} \quad \text{e} \quad X h^s e_{ij} = \sigma(h^s e_{ij})X + \delta(h^s e_{ij}),$$

onde os morfismos σ e δ são definidos por

$$\begin{aligned} \sigma(h^s e_{11}) &= 2^{3s} h^s e_{11}, & \sigma(h^s e_{12}) &= 2^{3s-1} h^s e_{12}, \\ \sigma(h^s e_{21}) &= 2^{3s+1} h^s e_{21}, & \sigma(h^s e_{22}) &= 2^{3s} h^s e_{22}. \end{aligned}$$

e

$$\begin{aligned}
\delta(h^s e_{11}) &= \frac{4}{7}\left[\frac{8^s - 1}{1 - [s < 0](8^s + 1)}\right](e - h^5) h^s e_{11}, \\
\delta(h^s e_{12}) &= \frac{4}{7}\left[\frac{8^s - 1}{1 - [s < 0](8^s + 1)} - \frac{63}{2^{3(s+1)}}\right](e - h^5) h^s e_{12}, \\
\delta(h^s e_{21}) &= \frac{8}{7}\left[\frac{8^s - 1}{1 - [s < 0](8^s + 1)} + \frac{63}{8}\right](e - h^5) h^s e_{21}, \\
\delta(h^s e_{22}) &= \frac{8}{7}\left[\frac{8^s - 1}{1 - [s < 0](8^s + 1)} + \frac{63}{8} - \frac{63}{8^{s+1}}\right](e - h^5) h^s e_{22}.
\end{aligned}$$

Para terminar esta seção, gostaríamos de voltar ao Exemplo 2.4.2, onde mostramos que, se $B[X; \sigma, \delta]$ é uma extensão de Hopf-Ore de uma álgebra de Hopf B, então $H[X; \sigma, \delta] \otimes H \simeq (B \otimes H)[Y, \overline{\sigma}, \overline{\delta}]$ é uma extensão de Hopf-Ore primitiva fraca da álgebra de Hopf fraca $B \otimes H$. Neste caso, $Y = X \otimes 1_H$, $\overline{\sigma} = \sigma \otimes id_H$, $\overline{\delta} = \delta \otimes id_H$ e, se X é $(g, 1_B)$-primitivo, então Y é $(g \otimes 1_H, 1_{B \otimes H})$-primitivo fraco. Com isso, temos

Exemplo 3.3.18. A extensão de Hopf-Ore primitiva fraca do Exemplo 3.3.17 não pode ser obtida diretamente do Exemplo 2.4.2.

Mais geralmente, sejam G um grupo, $r \in Z(G)$, k um corpo e $n > 1$. Sejam $kG[X; \sigma, \delta]$ uma extensão de Hopf-Ore de kG, onde X é um elemento $(r, 1_H)$-primitivo, e $M_n(kG)[Y; \overline{\sigma}, \overline{\delta}]$ a extensão de Hopf-Ore primitiva fraca como no Exemplo 2.4.2. Utilizando o Corolário 3.3.15 e a notação do Teorema 3.3.14, segue que

$$\rho(g)ge_{i1} = \overline{\sigma}(ge_{i1}) = \rho(g)\lambda_i ge_{i1} \quad \therefore \quad \lambda_i = 1_k, \ \forall i = 1, \ldots, n,$$

enquanto que

$$\begin{aligned} \alpha(g)(e-r)ge_{i1} &= \overline{\delta}(ge_{i1}) \\ &= [\lambda_i \alpha(g) + \omega_{1i} - \rho(g)\lambda_i\lambda_j^{-1}\omega_{11}]ge_{i1} \\ &= [\alpha(g) + \omega_{1i}](e-r)ge_{i1}, \end{aligned}$$

de onde, se $r \neq e$, obtemos $\omega_{1i} = 0$, para todo $i = 1, \ldots, n$. Ou seja, as extensões de Hopf-Ore primitivas fracas de $M_n(kG)$ obtidas diretamente do Exemplo 2.4.2 são aquelas em que $r \in Z(G)I$, $\lambda_1, \ldots, \lambda_n = 1$ e $\omega_{11}, \ldots, \omega_{1n} = 0$.

No Exemplo 3.3.17 temos $\omega_{12} = 9 \neq 0$ e $\lambda_2 = 2 \neq 1$, portanto este não pode ser obtido diretamente tomando o produto tensorial de uma extensão de Hopf-Ore de kG por $M_n(k)$. Mais ainda, neste exemplo temos $\omega_{12}(1_k + \lambda_2) = 9 \cdot 3 \neq 0$, portanto, este também não pode ser obtido diretamente do Exemplo 3.3.16.

Utilizamos o termo "*diretamente*" nas frases acima, pois não são conhecidas as classes de isomorfismo das extensões de Hopf-Ore primitivas fracas de $M_n(kG)$. Assim, pode ocorrer da álgebra de Hopf fraca do Exemplo 3.3.17 ser isomorfa, como álgebra de Hopf fraca, a alguma álgebra de Hopf fraca obtida pelos Exemplos 3.3.16 ou 2.4.2.

Referências Bibliográficas

[1] M. Atiyah and I. MacDonald. *Introduction to commutative algebra.* Addison-Wesley series in mathematics. Avalon Publishing, 1994. ISBN 9780813345444.

[2] D. Bagio, A. Paques, and H. Pinedo. On partial skew groupoids rings. *International Journal of Algebra and Computation*, 31(1):1–17, 2021.

[3] M. Beattie, S. Dăscălescu, and L. Grünenfelder. Constructing pointed Hopf algebras by Ore extensions. *Journal of Algebra*, 225(2):743–770, 2000. doi: 10.1006/jabr.1999.8148.

[4] G. Böhm, F. Nill, and K. Szlachányi. Weak Hopf algebras I: integral theory and C^*-structure. *Journal of Algebra*, 221(2):385–438, 1999. doi: 10.1006/jabr.1999.7984.

[5] Z. Chebel and A. Makhlouf. Kaplansky's construction type and classification of weak bialgebras and weak Hopf algebras. *Journal of Generalized Lie Theory and Applications*, 2015. doi: 10.4172/1736-4337.S1-008.

[6] S. Dascalescu, C. Nastasescu, and S. Raianu. *Hopf algebras: an introduction.* Pure and applied mathematics. Taylor & Francis Inc, 2000. ISBN 0-8247-0481-9.

[7] G. R. de Quadros. *Partial (co)actions of weak Hopf algebras: globalizations, Galois theory and Morita theory.* Tese de doutorado, Universidade Federal do Rio Grande de Sul, 2015. URL `lume.ufrgs.br/handle/10183/207208`.

[8] R. L. dos Santos. *Extensões de Ore e álgebras de Hopf fracas.* Tese de doutorado, Universidade Federal do Rio Grande do Sul, 2017. URL `lume.ufrgs.br/handle/10183/171352`.

[9] C. M. Garcia. *Extensões de Hopf-Ore e a décima conjectura de Kaplansky.* Dissertação de mestrado, Universidade Federal de Santa Maria, 2019. URL `repositorio.ufsm.br/handle/1/19102`.

[10] A. Gonçalves. *Introdução à Álgebra.* Projeto Euclides. IMPA, 6 edition, 2017. ISBN 9788524404306.

[11] K. Goodearl and R. Warfield. *An introduction to noncommutative noetherian rings.* London Mathematical Society Student Texts. Cambridge University Press, 2 edition, 2004. ISBN 0521836875,9780521836876.

[12] V. Gould and T. Stokes. Constellations and their relationship with categories. *Algebra Universalis*, 77(2):271–304, 2017. doi: 10.1007/s00012-017-0432-5.

[13] H. Huang, C. Walton, E. Wicks, and R. Won. Universal quantum semigroupoids. *Journal of Pure and Applied Algebra*, 227(2):107193, 2023. doi: 10.1016/j.jpaa.2022.107193.

[14] T. Y. Lam. *Lectures on modules and rings*. Graduate Texts in Mathematics. Springer, 1 edition, 1998. ISBN 978-1-4612-6802-4.

[15] T. Y. Lam. *A first course in noncommutative rings*. Graduate Texts in Mathematics. Springer, 2 edition, 2001. ISBN 978-0-387-95325-0.

[16] C. Lomp, A. Sant'Ana, and R. L. dos Santos. Panov's theorem for weak Hopf algebras. *Contemporary Mathematics*, 727:277–292, 2019.

[17] F. C. P. Milies. *Anéis e módulos*. Editora Livraria da Física, 2 edition, 2018. ISBN 978-85-7861-562-8.

[18] A. Nenciu. Quasitriangular pointed Hopf algebras constructed by Ore extensions. *Algebras and Representation Theory*, 7:159–172, 2004.

[19] O. Ore. Theory of non commutative polinomials. *Annals os Mathematics*, 34(3): 480–508, 1933.

[20] A. N. Panov. Ore extensions of Hopf algebras. *Mathematical Notes*, 74(3):401–410, 2003. doi: 10.1023/A:1026115004357.

[21] D. E. Radford. *Hopf algebras*, volume 49 of *Series on Knots and Everything*. World Scientific, 1 edition, 2012. ISBN 978-981-4335-99-7.

[22] S. Yang and Y. Zhang. Ore extensions for the Sweedler's Hopf algebra H_4. *Mathematics*, 8(8):1293, 2020. doi: 10.3390/math8081293.