UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA

Extensões H-cleft distinguidas por H-identidades polinomiais

Abel Gomes de Oliveira Júnior

Maio de 2022

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA

Extensões H-cleft distinguidas por H-identidades polinomiais

Abel Gomes de Oliveira Júnior

Orientador: Prof. Dr. Waldeck Schützer

Tese apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de São Carlos como parte dos requisitos para a obtenção do título de Doutor em Matemática.

Maio de 2022

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Matemática

Folha de Aprovação

Defesa de Tese de Doutorado do candidato Abel Gomes de Oliveira Júnior, realizada em 27/05/2022.

Comissão Julgadora:

Prof. Dr. Waldeck Schutzer (UFSCar)

Prof. Dr. Ivan Shestakov (USP)

Prof. Dr. Plamen Emilov Kochloukov (UNICAMP)

Prof. Dr. Diogo Diniz Pereira da Silva e Silva (UFCG)

Prof. Dr. Eliezer Batista (UFSC)

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Matemática.

Agradecimentos

Aos meus pais, Abel e Emília, pelo imensurável apoio e por toda a confiança que sempre tiveram em cada decisão da minha vida.

Aos meus sete irmãos e irmãs por todo o carinho e cuidado com seu irmão caçula.

À minha parceira Beatriz que, apesar de agora distante, compartilhou e continua a compartilhar comigo cada momento dos últimos seis anos dessa jornada.

Agradeço aos meus amigos e colegas, tanto aos de longa data, com os quais compartilhei a infância ou a adolescência, quanto aos mais recentes, com os quais compartilhei salas de aula, moradias e principalmente vários debates de ideias.

Agradeço, é claro, ao Prof. Dr. Waldeck Schützer por todo o seu tempo dedicado a me orientar nestes muitos anos.

Agradeço também aos membros da banca que disponibilizaram seu tempo a ler, corrigir e com isso contribuir com este texto.

Finalmente, agradeço à CAPES: O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Resumo

Nosso principal objeto de estudo é a conhecida questão: O conjunto das identidades polinomiais distingue as PI-álgebras a menos de isomorfismo? Seja H uma álgebra de Hopf monomial não semissimples sobre um corpo algebricamente fechado de característica zero. Mostramos que os objetos H-Galois são determinados a menos de isomorfismo de H-comódulo álgebras por suas H-identidades polinomiais. Em seguida, mostramos também que se H_N^q é uma álgebra de Taft sobre um anel finito R comutativo com unidade e N é um elemento invertível em R então as extensões H_N^q-cleft são determinadas a menos de isomorfismo de H_N^q-comódulo álgebras por suas H_N^q-identidades polinomiais.

Palavras-chave: Álgebras de Hopf, Extensões H-Cleft, Identidades Polinomiais.

Abstract

Our main object of study is the well-known question asking whether the set of polynomials identities distinguishes PI-algebras up to isomorphism. Let k be an algebraically closed field of characteristic 0 and H a non-semisimple monomial Hopf algebra. We prove that H-Galois objects over k are determined up to H-comodule algebra isomorphism by their polynomial H-identities. Afterwards we show that if H_N^q is a Taft algebra over a finite commutative unital ring R and N is an invertible element in R, then the H_N^q-cleft extensions over R are determined up to H_N^q-comodule R-algebra isomorphism by their polynomial H_N^q-identities.

Keywords: Hopf Algebras, H-Cleft Extensions, Polynomial Identities.

Sumário

Introdução

As álgebras de Hopf, assim chamadas em homenagem a Heinz Hopf por seu trabalho pioneiro em 1941 [23], foram usadas com esse nome pela primeira vez por Armand Borel [12] em 1953. No trabalho de Hopf, são introduzidos os, assim chamados, H-espaços. Estes caracterizam-se por possuírem uma operação produto e uma estrutura adicional de H em $H \otimes H$, com condições de compatibilidade, que Hopf observou impor fortes restrições à estrutura de H, a partir das quais ele deduziu vários resultados topológicos.

Uma visão mais algébrica das álgebras de Hopf surgiu algum tempo depois, notavelmente no livro [14] de Chase e Sweedler (1969). Já sua expansão e popularização ocorreu nas décadas seguintes, com as aplicações obtidas por Drinfeld, por exemplo o artigo Quantum Groups, baseado na sua palestra no ICM (1986) em Berkley [21].

Generalizando o conceito de ação de grupo, as ações e co-ações de álgebras de Hopf em uma álgebra podem ser definidas. Neste contexto surgem as H-extensões *cleft* e Galois. Tais objetos foram amplamente estudados nas décadas seguintes como em [11], [18], [19], [33] e [37] e têm papel central neste trabalho.

Já a teoria de identidades polinomiais (PI), apesar de ter sua abordagem moderna dada por Kaplansky em 1948, tem artigos publicados anteriormente, como o trabalho de Sylvester em 1988 ou Dehn em 1922 e desde então tem sido generalizada. Como exemplo de generalização do conceito de identidade polinomial podemos citar as identidades polinomiais graduadas por um grupo G.[†]

Partindo de uma álgebra de Hopf H, pode-se definir o conceito de H-identidade polinomial, que é o conceito de identidade polinomial que é "compatível" com os H-comódulo álgebras. É nessa interseção entre álgebras de Hopf e identidades polinomiais que este trabalho pode ser situado.

[†] Para mais informação sobre a parte histórica recomendo os artigos "Polynomial Identities" de Amitsur [4] e "The beginnings of the theory of Hopf algebras" de Andruskiewitsch e Santos [5].

Considere duas PI-álgebras. Não é difícil mostrar que se tais álgebras forem isomorfas (como álgebras) então elas possuem as mesmas identidades polinomiais. Considere a questão contrária: se duas PI-álgebras possuem as mesmas identidades polinomiais então elas são isomorfas (como álgebras)? Uma variação desta questão considerando H-identidades polinomiais, com H uma álgebra de Hopf é o centro deste trabalho.

O teorema de Amitsur-Levitzky [4] garante que o chamado polinômio *standard* de grau $2n$ distingue as álgebras associativas simples de dimensão finita sobre um corpo algebricamente fechado. Ademais, se as álgebras são simples, existem diversos resultados, não só no sentido estrito de álgebras, mas também para álgebras graduadas, álgebras de Lie, álgebras de Jordan dentre outras. Podemos citar, Kushkulei e Razmyslov [34], Drensky e Racine [20], Koshlukov e Zaicev [32], Aljadeff e Haile [1], Shestakov e Zaicev [44], Bahturin e Yasumura [7], Razmyslov [42], Karasik [28] e Bianchi e Diniz [9].

Sem a hipótese do corpo k ser algebricamente fechado, as identidades polinomiais podem não ser capazes de distinguir as álgebras. Por exemplo, os quatérnios $\mathbb{H}$ são álgebras centrais simples de dimensão 4 sobre $\mathbb{R}$ e $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathbb{C} \otimes_{\mathbb{R}} M_2(\mathbb{R})$. Logo, $\mathbb{H}$ e $M_2(\mathbb{R})$ tem as mesmas identidades polinomiais, mesmo não sendo isomorfas [6]. Por outro lado, as álgebras A e $A \oplus A$ tem as mesmas identidades polinomiais mesmo não sendo isomorfas, o que justifica pedir que as álgebras sejam simples [41], [17].

Quando H é uma álgebra de Hopf, em [2] e [31] Aljadeff e Kassel consideram as H-identidades polinomiais, que estendem o conceito de identidades polinomiais graduadas. De forma natural, o problema do isomorfismo para álgebras graduadas se torna um problema sobre os H-comódulo álgebras. Kassel mostrou que sobre um corpo algebricamente fechado de característica zero as H-identidades polinomiais distinguem objetos H-Galois a menos de isomorfismo sendo H o tipo I dentre os 6 tipos de álgebras monomiais não semissimples. Motivados pelo resultado de Kassel, mostraremos o seguinte resultado, que se encontra em Teorema 5.1.8 e que está também publicado em [43]:

Teorema. *Seja k um corpo algebricamente fechado de característica zero e H uma álgebra monomial não semissimples. Sejam B e B' objetos H-Galois. Se as H-identidades polinomiais de B e B' coincidem então B e B' são isomorfos como H-comódulo álgebras.*

Passamos a investigar a seguir as extensões H-cleft sobre um anel comutativo R. Para que pudéssemos usar algum critério de isomorfismo entre as extensões H-cleft, tomamos H como a álgebra de Taft sobre R, cujas extensões H-cleft foram caracterizadas por Masuoka em [37]. Denotando por H_N^q uma álgebra de Taft sobre

R de dimensão N^2, obtemos o seguinte resultado, que se encontra em Teorema 5.2.7 e que tem uma versão prévia no *arXiv* [39]:

Teorema. *Sejam R um anel finito e H_N^q uma álgebra de Taft. Sejam B e B' extensões H_N^q-cleft de R. Se $N \in R^\times$ e as H_N^q-identidades polinomiais de B e B' coincidem então B e B' são isomorfos como H_N^q-comódulo álgebras.*

A leitura deste trabalho requer do leitor conhecimentos sobre as estruturas algébricas básicas (grupos, anéis, corpos, módulos, ideais, espaços vetoriais e álgebras). De toda forma, definiremos módulos e álgebras, com o objetivo de fazer contraposição, respectivamente, a comódulos e coálgebras.

Ao leitor familiarizado com os principais objetos universais da álgebra e com os conceitos envolvendo álgebras de Hopf os dois primeiros capítulos talvez sejam dispensáveis para a boa compreensão deste texto.

Capítulo 1

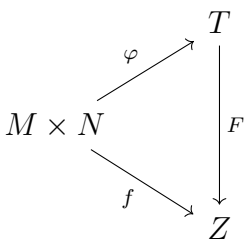
Conceitos Preliminares

Neste trabalho, salvo menção contrária, R será um anel comutativo com unidade e expressões como linear, bilinear, base, álgebra, 1 e $\otimes$ significarão R-linear, R-bilinear, R-base, R-álgebra, 1_R e $\otimes_R$.

Neste capítulo reunimos alguns conceitos e resultados elementares, aqui dispostos com a finalidade de fixar a notação e servir como referência ao leitor. Os resultados são apresentados sem demonstração. Tais conceitos e resultados podem ser encontrados, por exemplo, em [3], [22], [25] e [30].

O Produto Tensorial

Definição 1.1 (Produto Tensorial)**.** Sejam M e N R-módulos. Dizemos que (T, φ), no qual T é um R-módulo e $\varphi\colon M \times N \longrightarrow T$ é uma aplicação bilinear, é um *produto tensorial* entre M e N se para todo R-módulo Z e para toda aplicação bilinear $f\colon M \times N \longrightarrow Z$, existe única aplicação linear $F\colon T \longrightarrow Z$ tal que o seguinte diagrama é comutativo:



Tendo sido definido por propriedade universal, obviamente o produto tensorial é único a menos de isomorfismos, e é necessário apenas construir um modelo de produto

tensorial para garantir sua existência. Tal construção é encontrada, por exemplo, em [3, Capítulo VIII], [22, Capítulo 10] ou [25, Capítulo IV] e pode ser feita da seguinte forma:

Seja X um conjunto. Se $X = \emptyset$, definimos $RX = \{0\}$. Se $X \neq \emptyset$, definimos

$$RX = \{f \colon X \longrightarrow R \mid \text{supp}(f) \text{ é finito}\},$$

com $\text{supp}(f) = \{x \in X \mid f(x) \neq 0\}$. RX é um R-módulo com operações

- $(f+g)(x) = f(x) + g(x)$ para todo $f, g \in RX$ e $x \in X$,
- $(\lambda f)(x) = \lambda f(x)$ para todo $\lambda \in R$, $f \in RX$ e $x \in X$.

É corriqueiro mostrar que RX é um R-módulo livre sobre X, com base $\{e_x \mid x \in X\}$ em que $e_x \colon X \longrightarrow R$ é dada por

$$e_x(y) = \delta_{x,y} := \begin{cases} 1, & \text{se } y = x \\ 0, & \text{se } y \neq x \end{cases}$$

para todo $x, y \in X$.

Sejam M e N R-módulos. Considere $X = M \times N$ (como produto cartesiano de conjuntos) então $RX = R(M \times N)$ é um R-módulo livre com base

$$B = \left\{ e_{(m,n)} \mid \ m \in M,\ n \in N \right\}.$$

Seja U o R-submódulo de $R(M \times N)$ gerado pela união dos seguintes conjuntos:

$$U_1 = \{e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)},\ m_1, m_2 \in M,\ n \in N\},$$

$$U_2 = \{e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)},\ m \in M,\ n_1, n_2 \in N\},$$

$$U_3 = \{re_{(m,n)} - e_{(rm,n)},\ r \in R,\ m \in M, n \in N\},$$

$$U_4 = \{re_{(m,n)} - e_{(m,rn)},\ r \in R,\ m \in M, n \in N\}.$$

É rotineiro mostrar que o R-módulo quociente

$$T = \frac{R(M \times N)}{U}$$

com a aplicação bilinear $\varphi \colon M \times N \longrightarrow T$ dada por $\varphi(m,n) = e_{(m,n)} + U$, para todo $m \in M$ e $n \in N$, atende as condições da definição Definição 1.1, logo T é um produto tensorial. É usual denotar T por $M \otimes N$ e os elementos $e_{(m,n)} + U$ por $m \otimes n$.

As condições sobre $U_1, \ldots, U_4$ se traduzem respectivamente em:

1. $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$, para todo $m_1, m_2 \in M$ e $n \in N$,
2. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$, para todo $m \in M$ e $n_1, n_2 \in N$,
3. $r(m \otimes n) = (rm) \otimes n$, para todo $m \in M$, $n \in N$ e $r \in R$,
4. $r(m \otimes n) = m \otimes (rn)$, para todo $m \in M$, $n \in N$ e $r \in R$.

Os elementos da forma $m \otimes n$ $(m \in M, n \in N)$ são chamados tensores simples (também ditos puros ou canônicos). Note, porém, que $M \otimes N$ não consiste somente de tensores simples mas de combinações lineares de tensores simples. Por exemplo, tome $R = \mathbb{R}^2$ e seja $\{e_1, e_2\}$ a base canônica de $\mathbb{R}^2$. Então $e_1 \otimes e_2 + e_2 \otimes e_1 \in \mathbb{R}^2 \otimes \mathbb{R}^2$ mas tal tensor não é igual a um tensor simples. O sistema linear resultante de tal tentativa é um sistema impossível.

Os tensores simples são, contudo, particularmente úteis e convenientes pois é comum que para se verificar uma certa propriedade expressa em termos do produto tensorial seja suficiente verificar tal propriedade apenas nos tensores simples. Por exemplo, se duas aplicações lineares $f, g\colon M \otimes N \longrightarrow P$ coincidem nos tensores simples, então segue facilmente que $f = g$. Para isso, basta mostrar que $\{t \in M \otimes N \mid f(t) = g(t)\}$ é um R-submódulo gerado por $m \otimes n$ $(m \in M, n \in N)$.

Proposição 1.2. *[22, 10.4, Teorema 13] Sejam M_1, M_2, N_1 e N_2 R-módulos. Se $f_1\colon M_1 \longrightarrow N_1$ e $f_2\colon M_2 \longrightarrow N_2$ são aplicações lineares então existe uma única aplicação linear $g\colon M_1 \otimes M_2 \longrightarrow N_1 \otimes N_2$ tal que $g(m_1 \otimes m_2) = f_1(m_1) \otimes f_2(m_2)$ para todo $m_1 \in M_1$ e $m_2 \in M_2$.*

A aplicação g desta proposição é única e será denotada por $f_1 \otimes f_2$.

Um elemento $t \in M \otimes N$ não possui uma representação que seja única, ou mesmo preferível, como soma de tensores simples. Isto muda completamente se M ou N for livre:

Proposição 1.3. *[25, IV,Teorema 5.11] Sejam M e N R-módulos e suponha que N seja livre com base B. Então todo elemento $t \in M \otimes N$ pode ser escrito unicamente na forma*

$$t = \sum_{i=1}^{n} m_i \otimes b_i,$$

com $m_i \in M$ e os $b_i \in B$ distintos. Em particular, se $t = 0$ então $m_i = 0$, para todo $i = 1, \ldots, n$.

Corolário 1.4. *[25, Corolário 5.12] Sejam M e N dois R-módulos livres. Se $B = \{m_i, i \in I\}$ e $C = \{n_j, j \in J\}$ são, respectivamente, bases de M e N, então $\{m_i \otimes n_j, i \in I, j \in J\}$ é uma base de $M \otimes N$. Em particular,* $\dim_R(M \otimes N) = (\dim_R M)(\dim_R N)$.

Dados M, M_1, M_2 e N R-módulos, é usual considerar os seguintes conjuntos:

$$\begin{aligned} \mathrm{Hom}_R(M, N) &= \{f\colon M \longrightarrow N \mid f \text{ linear}\} \\ \mathrm{Bil}_R(M_1, M_2; N) &= \{f\colon M_1 \times M_2 \longrightarrow N \mid f \text{ bilinear}\} \\ \mathrm{Mult}_R(M, N, n) &= \{f\colon \underbrace{M \times \ldots \times M}_{n\text{-vezes}} \longrightarrow N \mid f \ n\text{-linear}\} \end{aligned}$$

É fácil ver que estes conjuntos são R-módulos de maneira natural e que são livres se os R-módulos envolvidos são livres.

A próxima proposição relaciona os operadores Bil e Hom:

Proposição 1.5. *[22, 10.4 Corolário 12] Sejam M_1, M_2 e N R-módulos. Então existe uma correspondência bijetora*

$$\mathrm{Bil}_R(M_1, M_2; N) \longleftrightarrow \mathrm{Hom}_R(M_1 \otimes M_2, N).$$

Podemos estender o conceito de produto tensorial para vários R-módulos. No caso $n = 3$, dados M, N e P R-módulos, obtemos $(M \otimes N) \otimes P$ e $M \otimes (N \otimes P)$, porém estes R-módulos são canonicamente isomorfos, como afirma a seguinte proposição:

Proposição 1.6. *[22, 10.4 Corolário 15] Sejam M, N e P R-módulos. Então*

$$(M \otimes N) \otimes P \cong M \otimes (N \otimes P).$$

como R-módulos.

Em virtude da associatividade expressa pela proposição anterior, faz sentido introduzir a seguinte notação para o R-módulo associado ao múltiplo produto tensorial do R-módulo M por si mesmo n vezes ($n \geq 0$):

$$M^{\otimes n} := \begin{cases} R, & \text{se } n = 0, \\ \underbrace{M \otimes \ldots \otimes M}_{n\text{-vezes}}, & \text{se } n > 0. \end{cases}$$

Proposição 1.7. *[22, 10.4 Exemplo 7] Seja M um R-módulo. Então*

$$R \otimes M \cong M \cong M \otimes R,$$

como R-módulos.

Cabe lembrar que o isomorfismo $R \otimes M \cong M$ é dado naturalmente pela aplicação $r \otimes m = 1 \otimes (rm) \mapsto rm$, para todo $r \in R$ e $m \in M$.

A seguinte proposição mostra que o produto tensorial é distributivo sobre a soma direta de R-módulos:

Proposição 1.8. *[22, 10.4 Teorema 17] Sejam M, N e P R-módulos. Então existe único isomorfismo de R-módulos*

$$M \otimes (N \oplus P) \cong (M \otimes N) \oplus (M \otimes P).$$

tal que $m \otimes (n, p) \mapsto (m \otimes n, m \otimes p)$, para todo $m \in M$, $n \in N$ e $p \in P$.

O resultado anterior pode claramente ser estendido por indução a uma soma direta finita de R-módulos.

A proposição a seguir nos permite trocar a ordem dos fatores em $M \otimes N$.

Proposição 1.9. *[22, 10.4 Proposição 20] Se $M \otimes N$ e $N \otimes M$ são produtos tensoriais entre os R-módulos M e N então existe único isomorfismo de R-módulos*

$$M \otimes N \cong N \otimes M.$$

que leva $m \otimes n$ em $n \otimes m$, para todo $m \in M$ e $n \in N$.

A partir daqui, em todo o texto, τ irá denotar o isomorfismo da proposição anterior, a saber, $\tau \colon M \otimes N \longrightarrow N \otimes M$ dado por $\tau(m \otimes n) = n \otimes m$, para todo $m \in M$ e $n \in N$.

Com o intuito de enunciar um último resultado para o produto tensorial, lembremos da definição de uma álgebra.

Definição 1.10 (Álgebra)**.** Uma *álgebra* associativa e unitária é um anel A com 1_A junto com um homomorfismo de anéis $\varphi \colon R \longrightarrow A$ que leva 1 em 1_A e tal que $\mathrm{Im}(\varphi)$ está contida no centro de A.

Lembremos também que um homomorfismo (unital) de álgebras é um homomorfismo de anéis e de R-módulos.

Proposição 1.11. *[22, Proposição 10.21] Sejam A e B duas álgebras. Então o produto tensorial $A \otimes B$ munido de uma multiplicação dada por*

$$\begin{array}{rccc} f\colon & (A\otimes B)\times(A\otimes B) & \longrightarrow & A\otimes B \\ & (a\otimes b, a'\otimes b') & \longmapsto & aa'\otimes bb' \end{array}$$

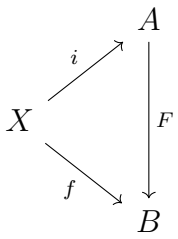
e unidade $1_A \otimes 1_B$ é uma álgebra, com $\varphi\colon R \longrightarrow A\otimes B$ dado por $\varphi(1_R) = 1_A \otimes 1_B$.

A álgebra $A\otimes B$ da proposição anterior é chamada de *produto tensorial das álgebras A e B.*

A Álgebra Associativa Livre

Um dos conceitos mais básicos na álgebra contemporânea é o de objeto livre, que pode ser pensado como sendo um tipo de estrutura algébrica genérica, na qual as únicas relações algébricas entre os seus elementos são as que essencialmente definem a estrutura, ou ainda, uma estrutura algébrica "mais livre possível" de relações entre os seus elementos. Tais objetos são muito úteis na construção de outros objetos da mesma classe ou na caracterização de um conjunto de propriedades intrínsecas que os distinguem. Interessam-nos aqui os objetos livres na classe das álgebras associativas e unitárias:

Definição 1.12 (Álgebra Associativa Livre)**.** Sejam A uma álgebra, X um conjunto e $i\colon X \longrightarrow A$ uma função. Dizemos que A é uma *álgebra associativa livre sobre X* se, para toda álgebra B e para toda aplicação $f\colon X \longrightarrow B$, existe único homomorfismo de álgebras $F\colon A \longrightarrow B$ tal que o seguinte diagrama é comutativo



Sendo dada por propriedade universal, uma álgebra associativa livre em X é única a menos de isomorfismo. Um modelo para essa álgebra pode ser encontrado em [30, Capítulo I], e é construído do seguinte modo:

Seja X um conjunto. Considere o R-módulo livre $R\langle X\rangle$ com base consistindo de todas as palavras $x_{i_1}\ldots, x_{i_p}$ no alfabeto X, incluindo a palavra vazia $\varnothing$. A concatenação de palavras define uma multiplicação (associativa) em $R\langle X\rangle$ dada por

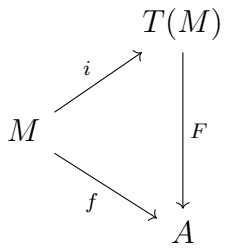
$$(x_{i_1}\ldots, x_{i_p})(x_{i_{p+1}}\ldots x_{i_n}) = x_{i_1}\ldots x_{i_p}x_{i_{p+1}}\ldots x_{i_n}$$

com relação à qual, a palavra vazia $1_{R\langle X\rangle} = \varnothing$ serve como unidade. Considere $A = R\langle X\rangle$ e $i\colon X \longrightarrow R\langle X\rangle$ a inclusão. É rotineiro verificar que $(R\langle X\rangle, i)$ satisfaz a propriedade universal acima, e portanto é uma álgebra associativa livre em X.

Note que $R\langle X\rangle$ também é chamada álgebra dos polinômios em variáveis não comutativas de X, denominação que se justifica pelo fato de $R\langle X\rangle$ ser desprovida de qualquer relação de comutação na multiplicação, de não haver cancelamento de letras na formação das palavras a não ser o cancelamento óbvio da palavra vazia e da possibilidade de interpretar as palavras como monômios. Assim, por exemplo, se $X = \{x_1, x_2\}$, então $x_1x_2 - x_2x_1$ pode ser pensado como um polinômio em $R\langle X\rangle$ distinto do polinômio nulo, bem como o monômio $x_1x_2x_1x_2$ é distinto do monômio $x_1x_1x_2x_2$, etc.

A Álgebra Tensorial

Definição 1.13 (Álgebra Tensorial)**.** Seja M um R-módulo. Dizemos que $(T(M), i)$, no qual $T(M)$ é uma álgebra e $i\colon M \longrightarrow T(M)$ é uma aplicação linear, é uma *álgebra tensorial de* M se, para toda álgebra A e toda aplicação linear $f\colon M \longrightarrow A$, existe único homomorfismo de álgebras $F\colon T(M) \longrightarrow A$ tal que o seguinte diagrama é comutativo:



Obviamente $T(M)$ é única a menos de isomorfismo e um modelo pode ser encontrado em [22, Seção 11.5], construído do seguinte modo:

Seja M um R-módulo. Considere o R-módulo

$$T(M) = \bigoplus_{n\geq 0} M^{\otimes n}.$$

Os elementos de $T(M)$ são as sequências $(t_0, t_1, t_2, \ldots)$ de elementos $t_n \in M^{\otimes n}$ quase todos nulos e não há risco em denotar o elemento $(0, \ldots, 0, t_n, 0, \ldots)$ simplesmente por t_n, pensado como um elemento de $M^{\otimes n} \subseteq T(M)$. Com disso, definimos $i\colon M \longrightarrow T(M)$ por $i(m) = (0, m, 0\ldots) \equiv m \in M^{\otimes 1}$ para todo $m \in M$. Então, dados $x = m_1 \otimes \ldots \otimes m_n \in M^{\otimes n}$ e $y = m'_1 \otimes \ldots \otimes m'_r \in M^{\otimes r}$, podemos definir a

multiplicação em $T(M)$ por

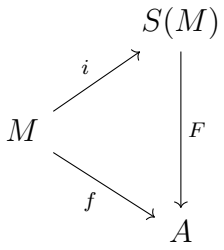
$$x \cdot y = m_1 \otimes \ldots \otimes m_n \otimes m'_1 \otimes \ldots \otimes m'_r \in M^{\otimes n+r}$$

(nos tensores simples). Verifica-se que $T(M)$ é uma álgebra associativa e unitária com essa multiplicação, sendo $1_{T(M)} = (1, 0, 0 \ldots) \equiv 1 \in M^{\otimes 0} = R$ a unidade. $(T(M), i)$ é a álgebra tensorial de M. É comum denotar $x \cdot y$ por $x \otimes y$, devido à existência do isomorfismo de álgebras $M^{\otimes n} \otimes M^{\otimes r} \cong M^{\otimes n+r}$.

Proposição 1.14. *[30, Proposição II.5.1] Seja M um R-módulo livre e B uma base de M. Então $T(M) \cong R\langle B \rangle$ como álgebras.*

A Álgebra Simétrica

Definição 1.15 (Álgebra Simétrica)**.** Seja M um R-módulo. Dizemos que $(S(M), i)$, na qual $S(M)$ é uma álgebra e $i\colon M \longrightarrow S(M)$ uma aplicação linear, é uma *álgebra simétrica de M* se, para toda álgebra A e toda $f\colon M \longrightarrow A$ linear tal que $f(x)f(y) = f(y)f(x)$, para todo $x, y \in M$, existe um único $F\colon S(M) \longrightarrow A$ homomorfismo de álgebras tal que o seguinte diagrama é comutativo:



Sendo dada por propriedade universal, uma álgebra simétrica de um R-módulo M é única a menos de isomorfismo. Um modelo pode ser encontrado em [22, Seção 11.5] como a seguir:

Seja M um R-módulo. Definimos $S(M) = T(M)/I(M)$, com $I(M)$ o ideal bilateral gerado por todos os elementos da forma $x \otimes y - y \otimes x$, com $x, y \in M$.

Proposição 1.16. *[30, Proposição II.5.2] Seja M um R-módulo livre e B uma base de M. Então $S(M) \cong R[B]$ como álgebras, sendo $R[B]$ a álgebra comutativa usual dos polinômios nas variáveis $b \in B$.*

Capítulo 2

Álgebras de Hopf

Neste capítulo, nosso objetivo é introduzir as álgebras de Hopf. Para tanto, definiremos as coálgebras, que são uma estrutura dual às álgebras. Falaremos também dos comódulos que, por sua vez, são estruturas duais aos módulos. Terminaremos o capítulo com exemplos de álgebras de Hopf que são de interesse para este trabalho.

Para muito do que se fará neste e nos próximos capítulos existe uma bibliografia clássica. Por exemplo [16], [30], [38] e [40]. Porém, tais referências tratam o tema sobre um corpo k, ou seja em associação com espaços vetoriais. Como se sabe, os R-módulos não têm tão boas propriedades quanto os espaços vetoriais. Por isso, tais autores assumem $R = k$. Entretanto, alguns resultados obtidos neste trabalho têm seu valor precisamente por não supor $R = k$. Devido a isso, não usaremos tal hipótese.

Referências para álgebras de Hopf sobre um anel R são mais escassas. Usaremos principalmente [13] ou mesmo [14]. Mesmo assim, alguns dos resultados precisaram ser adaptados das referências que tratam o tema sobre um corpo k.

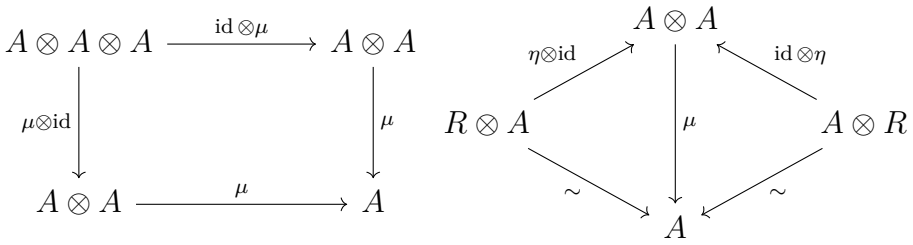
2.1 Álgebras e Coálgebras

Como estamos interessados em álgebras de Hopf, este texto enfatiza resultados que associem álgebras e coálgebras. Porém, há que se dizer que, assim como as álgebras, também as coálgebras podem ser estudadas por si só. Radford [40], por exemplo, dedica vários capítulos do seu livro ao estudo das coálgebras e de suas representações (envolvendo aspectos topológicos).

A definição de coálgebra é feita usando tensores e diagramas. Por isso, para um melhor entendimento da relação entre álgebras e coálgebras, convém redefinir uma

álgebra usando esta linguagem:

Definição 2.1.1 (Álgebra)**.** Uma *álgebra (associativa com unidade)* é uma tripla (A, μ, η) em que A é um R-módulo e $\mu\colon A \otimes A \longrightarrow A$ (multiplicação) e $\eta\colon R \longrightarrow A$ (unidade) são aplicações lineares tais que os seguintes diagramas são comutativos:



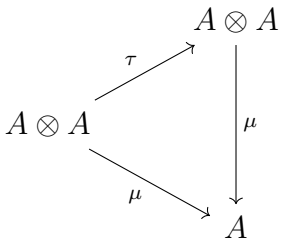
O símbolo $\sim$ nos diagramas irá sempre representar um dos isomorfismos (canônicos) da Proposição 1.7.

A comutatividade do primeiro diagrama diz que, $(ab)c = a(bc)$, para todo $a, b, c \in A$. Se denotarmos $\eta(1) = 1_A$, então o segundo diagrama diz que $ar = ra$, $ra = (r1_A)a$ e $ar = a(r1_A)$, para todos $a \in A$ e $r \in R$.

As definições de álgebra dadas em Definição 1.10 e Definição 2.1.1 são equivalentes. De fato, admitindo a Definição 2.1.1, defina o produto $ab = \mu(a \otimes b)$ e $1_A = \eta(1)$. A linearidade de μ e η e a comutatividade dos diagramas irão garantir o resultado. Por outro lado, admitindo a Definição 1.10, defina $\mu(a \otimes b) = ab$ e $\eta = \varphi$. As propriedades da definição clássica de álgebra com o fato de f ser um homomorfismo garantem a linearidade de μ e η bem como a comutatividade dos diagramas.

Com isso, usaremos a notação mais conveniente em cada situação tanto para a multiplicação quanto para a unidade.

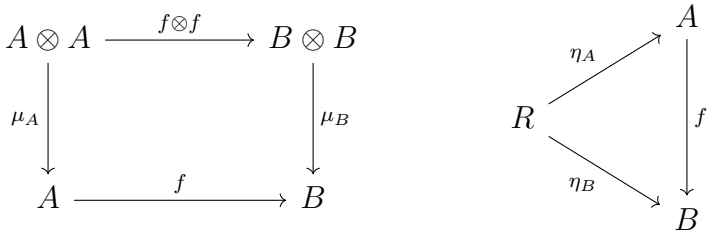
Definição 2.1.2 (Álgebra Comutativa)**.** Uma álgebra (A, μ, η) é dita *comutativa* se o seguinte diagrama é comutativo:



em que τ é a aplicação definida na proposição Proposição 1.9. Note que a comutatividade do diagrama acima diz que $ab = ba$ para todo $a, b \in A$, como era de se esperar.

Trazemos também uma definição de homomorfismo de álgebras usando diagramas comutativos:

Definição 2.1.3 (Homomorfismo de Álgebras)**.** Sejam (A, μ_A, η_A) e (B, μ_B, η_B) álgebras e $f\colon A \longrightarrow B$ uma aplicação linear. Dizemos que f é um *homomorfismo de álgebras* se os seguintes diagramas são comutativos:



Ou seja, se

$$f(a_1a_2) = f(a_1)f(a_2)$$
$$f(1_A) = 1_B$$

para todo $a_1, a_2 \in A$.

Além dos importantes exemplos de álgebras que apareceram no capítulo anterior, construímos a seguir mais um exemplo clássico:

Exemplo 2.1.4 (Álgebra de monoide)**.** Seja M um monoide e RM o R-módulo com base $\{m \mid m \in M\}$. Neste caso é conveniente olhar para RM como o R-módulo cujos elementos são combinações lineares finitas do tipo

$$\sum_{m\in M} \alpha_m m$$

em que $\{\alpha_m\}_{m\in M}$ é uma família de elementos em R quase todos nulos. O R-módulo RM tem estrutura de álgebra com multiplicação dada pela operação do monoide e estendida por linearidade. Ou seja, se

$$x = \sum_{m\in M} \alpha_m m \text{ e } y = \sum_{n\in M} \beta_n n$$

então

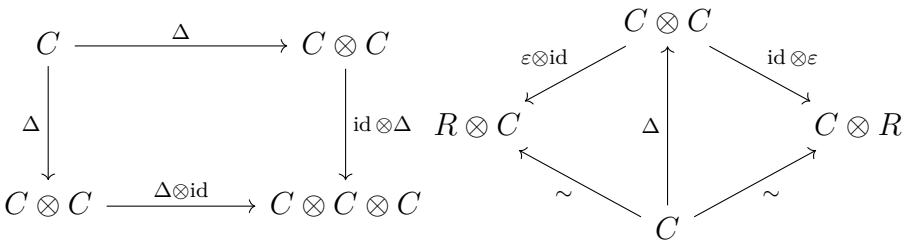
$$xy = \sum_{p\in M} \gamma_p p, \text{ com } \gamma_p = \sum_{mn=p} \alpha_m\beta_n.$$

A unidade de RM é o elemento neutro do monoide. Estaremos mais interessados no caso RG, em que G é um grupo. RG é dita *álgebra de grupo*.

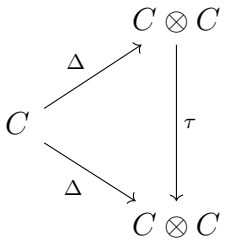
As álgebras de grupo tem um papel fundamental (e motivacional) tanto para o estudo das álgebras de Hopf em geral, quanto para o tipo de problema que estamos interessados.

Definimos, a seguir, as coálgebras. Como já dissemos, tal definição é motivada pela ideia da dualização das aplicações que definem a estrutura de uma álgebra, revertendo as flechas.

Definição 2.1.5 (Coálgebra)**.** Uma *coálgebra* é uma tripla (C, Δ, ε) em que C é um R-módulo, $\Delta\colon C \longrightarrow C \otimes C$ (comultiplicação) e $\varepsilon\colon C \longrightarrow R$ (counidade) são aplicações lineares tais que os seguintes diagramas são comutativos:



Definição 2.1.6 (Coálgebra Cocomutativa)**.** Uma coálgebra (C, Δ, ε) é dita cocomutativa se o seguinte diagrama é comutativo:



O exemplo a seguir garante que todo R-módulo livre possui estrutura de coálgebra.

Exemplo 2.1.7. Seja $S \neq \varnothing$ um conjunto e RS o R-módulo livre com base S. $(RS, \Delta, \varepsilon)$ é uma coálgebra com a comultiplicação $\Delta\colon RS \longrightarrow RS \otimes RS$ dada por $\Delta(s) = s \otimes s$ para todo $s \in S$ e counidade $\varepsilon\colon RS \longrightarrow R$ dada por $\varepsilon(s) = 1$ para todo $s \in S$.

Em particular, R é uma coálgebra. Um caso particular do exemplo acima, mas que merece ser destacado é a coálgebra de monoides:

Exemplo 2.1.8. Seja M um monoide e RM o R-módulo com base M. $(RM, \Delta, \varepsilon)$ é uma coálgebra com a comultiplicação $\Delta\colon RM \longrightarrow RM \otimes RM$ dada por $\Delta(m) = m \otimes m$ para todo $m \in M$ e counidade $\varepsilon\colon RM \longrightarrow R$ dada por $\varepsilon(m) = 1$ para todo $m \in M$. Em particular, se G é um grupo, então o R-módulo RG admite uma estrutura de coálgebra.

Seja C uma coálgebra. Dizemos que um elemento $c \in C$ é *grouplike* se $\Delta(c) = c \otimes c$ e $\varepsilon(c) = 1$. Além disso, se $g, h \in C$ são elementos *grouplike* em C, dizemos que $x \in C$ é (g, h)-*primitivo* se $\Delta(x) = g \otimes x + x \otimes h$ e $\varepsilon(x) = 0$.

O R-módulo subjacente à álgebra de matrizes também admite a seguinte estrutura de coálgebra:

Exemplo 2.1.9. Seja $n \geq 1$ e $(e_{ij})_{1\leq i,j\leq n}$ a base canônica da álgebra de matrizes $M_n(R)$. Seja $C_n(R)$ o R-módulo livre de base $(e_{ij})_{1\leq i,j\leq n}$. $C_n(R)$ é uma coálgebra com comultiplicação $\Delta\colon C_n(R) \longrightarrow C_n(R) \otimes C_n(R)$ dada por

$$\Delta(e_{ij}) = \sum_{1\leq p\leq n} e_{ip} \otimes e_{pj}$$

e counidade $\varepsilon\colon C_n(R) \longrightarrow R$ dada por $\varepsilon(e_{ij}) = \delta_{i,j}$. $C_n(R)$ é chamada de coálgebra de matrizes.

Assim como é feito com álgebras, podemos definir uma estrutura de coálgebra no produto tensorial de duas coálgebras:

Exemplo 2.1.10. Sejam $(C, \Delta_C, \varepsilon_C)$ e $(D, \Delta_D, \varepsilon_D)$ duas coálgebras. Então $C \otimes D$ tem estrutura de coálgebra dada por

$$\Delta = (\mathrm{id} \otimes \tau \otimes \mathrm{id}) \circ (\Delta_C \otimes \Delta_D)$$

e

$$\varepsilon = \varepsilon_C \otimes \varepsilon_D.$$

Seja (C, Δ, ε) uma coálgebra. Introduzimos a seguinte notação:

$$\begin{aligned}
\Delta_1 &= \Delta, \\
\Delta_2 &= (\Delta \otimes \mathrm{id}) \circ \Delta, \\
\Delta_3 &= (\Delta \otimes \mathrm{id} \otimes \mathrm{id}) \circ \Delta_2, \\
&\vdots \qquad\qquad \vdots \\
\Delta_n &= (\Delta \otimes \mathrm{id}^{n-1}) \circ \Delta_{n-1}.
\end{aligned}$$

O próximo lema generaliza a coassociatividade e pode ser demonstrado por indução finita.

Proposição 2.1.11. *Seja (C, Δ, ε) uma coálgebra. Então para todo $n \geq 2$ e todo $p \in \{0, \ldots, n-1\}$*

$$\Delta_n = \mathrm{id}^p \otimes \Delta \otimes \mathrm{id}^{n-1-p} \circ \Delta_{n-1}.$$

Ao contrário do que ocorre na multiplicação que "leva dois elementos em um só", a comultiplicação leva um elemento em uma soma finita de tensores, o que pode tornar os cálculos um tanto complicados. Para facilitar, existe uma notação clássica para

a comultiplicação chamada de Notação de Sweedler (ou Notação Sigma): Dada uma coálgebra (C, Δ, ε) denotaremos

$$\Delta(c) = \sum_{i=1}^{n} c_{i1} \otimes c_{i2}$$

por

$$\Delta(c) = \sum c_1 \otimes c_2.$$

Com isso, pela coassociatividade generalizada, podemos escrever, para $n \geq 1$,

$$\Delta_n(c) = \sum c_1 \otimes \cdots \otimes c_{n+1}.$$

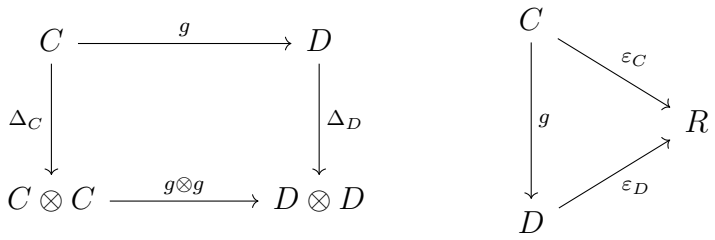
Usando essa notação podemos também reescrever o segundo diagrama da definição de coálgebra da seguinte forma

$$\sum \varepsilon(c_1)c_2 = \sum c_1\varepsilon(c_2) = c.$$

Já o diagrama da definição de coálgebra cocomutativa é expresso por

$$\sum c_1 \otimes c_2 = \sum c_2 \otimes c_1.$$

Definição 2.1.12 (Homomorfismo de Coálgebras)**.** Sejam $(C, \Delta_C, \varepsilon_C)$ e $(D, \Delta_D, \varepsilon_D)$ coálgebras e $g\colon C \longrightarrow D$ uma aplicação linear. Dizemos que g é um *homomorfismo de coálgebras* se os seguintes diagramas são comutativos:



Usando a notação de Sweedler, a comutatividade do primeiro diagrama acima pode ser escrita, para todo $c \in C$, como:

$$\sum g(c)_1 \otimes g(c)_2 = \sum g(c_1) \otimes g(c_2).$$

2.2 Dualidade entre Álgebras e Coálgebras

Seja M um R-módulo. Então $M^* := \mathrm{Hom}_R(M, R)$ é um R-módulo, chamado de *dual de* M. Seja $\varphi\colon M \longrightarrow N$ uma aplicação linear. Denote por φ^* a aplicação linear

(dual) $\varphi^*\colon N^* \longrightarrow M^*$ dada por $\varphi^*(f)(m) = f(\varphi(m))$ para todo $f \in N^*$ e $m \in M$.

Veremos nesta seção que se C é uma coálgebra então C^* é uma álgebra. Por outro lado, se A é uma álgebra, nem sempre vale que A^* é uma coálgebra. Para tanto, é suficiente pedir que A^* seja um R-módulo livre e finitamente gerado.

Esta dualidade entre álgebras e coálgebras é dada pelos seguintes resultados adaptados de [13, 1.12]:

Lema 2.2.1. *Seja M um R-módulo. A aplicação linear $\varphi\colon M^* \otimes M^* \longrightarrow (M \otimes M)^*$ dada por $\varphi(f \otimes g)(m \otimes n) = f(m)g(n)$ é injetora. Além disso, se M for finitamente gerado e livre então φ é um isomorfismo.*

A injetividade de φ no lema anterior é usada para provar a proposição a seguir.

Proposição 2.2.2. *Se (C, Δ, ε) é uma coálgebra então C^* possui estrutura de álgebra dada por $\mu = \Delta^* \circ \varphi$ e $\eta = \varepsilon^*$, com φ dada no Lema 2.2.1.*

A próxima proposição usa não só a injetividade da aplicação φ mas também sua sobrejetividade.

Proposição 2.2.3. *Seja (A, μ, η) é uma álgebra. Se A é um R-módulo finitamente gerado e livre, então A^* possui estrutura de coálgebra dada por $\Delta = \varphi^{-1} \circ \mu^*$ e $\varepsilon = \eta^*$, com φ dada no Lema 2.2.1.*

Exemplo 2.2.4. Dada a coálgebra RS do Exemplo 2.1.7, $(RS)^*$ é uma álgebra com multiplicação

$$f * g(s) = f(s)g(s)$$

para todo $f, g \in (RS)^*$ e $s \in S$. A unidade de $(RS)^*$ é dada por $\eta(1)(s) = 1$ para todo $s \in S$. Obviamente, o mesmo vale para $(RG)^*$, com G um grupo.

2.3 Módulos e Comódulos

Da mesma forma que as coálgebras são definidas em um sentido dual às álgebras, nessa seção serão definidos os C-comódulos (com C uma coálgebra) de modo dual aos A-módulos (com A uma álgebra).

Definição 2.3.1 (A-Módulo à Esquerda)**.** Seja A uma álgebra. Um *A-módulo à esquerda* é um par (X, ν), com X um R-módulo e $\nu\colon A \otimes X \longrightarrow X$ linear tal que os seguintes diagramas são comutativos:

$$\begin{array}{ccc} A \otimes A \otimes X & \xrightarrow{\mathrm{id} \otimes \nu} & A \otimes X \\ \downarrow{\scriptstyle \mu \otimes \mathrm{id}} & & \downarrow{\scriptstyle \nu} \\ A \otimes X & \xrightarrow{\nu} & X \end{array} \qquad \begin{array}{ccc} R \otimes X & \xrightarrow{\eta \otimes \mathrm{id}} & A \otimes X \\ & \searrow^{\sim} & \downarrow{\scriptstyle \nu} \\ & & X \end{array}$$

É comum denotarmos $\nu(a \otimes x) = a \cdot x$. Note que, usando essa notação, os diagramas anteriores nos garantem que:

$$a \cdot (b \cdot x) = ab \cdot x, \text{ para todo } a, b \in A \text{ e } x \in X,$$
$$1_A \cdot x = x, \text{ para todo } x \in X.$$

Definição 2.3.2 (Homomorfismo de A-Módulos à Esquerda)**.** Seja A uma álgebra e (X, ν), (Y, ϑ) dois A-módulos. Dizemos que a aplicação linear $f\colon X \longrightarrow Y$ é um *homomorfismo de A-módulos à esquerda* se o seguinte diagrama é comutativo:

$$\begin{array}{ccc} A \otimes X & \xrightarrow{\mathrm{id} \otimes f} & A \otimes Y \\ \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \vartheta} \\ X & \xrightarrow{\quad f \quad} & Y \end{array}$$

Note que o diagrama anterior nos diz que:

$$f(a \cdot x) = a \cdot f(x), \text{ para todo } a \in A \text{ e } x \in X.$$

De modo análogo é possível definir A-módulos à direita e homomorfismos de A-módulos à direita.

Para cada álgebra A, denotaremos o conjunto dos homomorfismos de A-módulos à esquerda $f\colon X \longrightarrow Y$ por $\mathrm{Hom}_A(X, Y)$.

Neste texto não usaremos A-módulos à direita. Por isso, a partir daqui, o termo A-módulo irá se referir a um A-módulo à esquerda.

De forma simétrica aos A-módulos, que costumam ser tomados à esquerda, os C-comódulos costumam ser tomados à direita:

Definição 2.3.3 (C-Comódulos à Direita)**.** Seja C uma coálgebra. Um *C-comódulo à direita* é um par (M, ρ), com M um R-módulo e $\rho\colon M \longrightarrow M \otimes C$ uma aplicação linear tal que os seguintes diagramas são comutativos:

$$\begin{array}{ccc} M & \xrightarrow{\quad \rho \quad} & M \otimes C \\ \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \mathrm{id} \otimes \Delta} \\ M \otimes C & \xrightarrow{\rho \otimes \mathrm{id}} & M \otimes C \otimes C \end{array} \qquad \begin{array}{ccc} M & & \\ \downarrow{\scriptstyle \rho} & \searrow^{\sim} & \\ M \otimes C & \xrightarrow{\mathrm{id} \otimes \varepsilon} & M \otimes R \end{array}$$

Definição 2.3.4 (Homomorfismo de C-Comódulos à Direita)**.** Seja C uma coálgebra e (M, ρ), (N, δ) dois C-comódulos à direita. Dizemos que a aplicação linear $g\colon M \longrightarrow N$

é um *homomorfismo de C-comódulos à direita* se o seguinte diagrama é comutativo:

$$\begin{array}{ccc} M & \xrightarrow{\quad g \quad} & N \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle\delta} \\ M \otimes C & \xrightarrow{\quad g\otimes \mathrm{id} \quad} & N \otimes C \end{array}$$

De modo análogo, é possível definir C-comódulos à esquerda e homomorfismos de C-comódulos à esquerda.

Para cada coálgebra C denotaremos o conjunto dos homomorfismos de C-comódulos à direita $f\colon X \longrightarrow Y$ por $\mathrm{Hom}_R^C(X,Y)$.

Neste texto não usaremos C-comódulos à esquerda. Por isso, a partir daqui, o termo C-comódulo irá se referir a um C-comódulo à direita.

De modo análogo às coálgebras, há uma notação conveniente para os C-comódulos. Se (M,ρ) é um C-comódulo então denotaremos

$$\rho(m) = \sum m_{(0)} \otimes m_{(1)}, \text{ com } m_{(0)}\text{'s } \in M \text{ e } m_{(1)}\text{'s } \in C$$

para todo $m \in M$.

Usando essa notação, a comutatividade dos diagramas da Definição 2.3.3 pode ser reescrita como

$$\sum (m_{(0)})_{(0)} \otimes (m_{(0)})_{(1)} \otimes m_{(1)} = \sum m_{(0)} \otimes (m_{(1)})_1 \otimes (m_{(1)})_2, \tag{2.1}$$

$$\sum \varepsilon(m_{(1)}) m_{(0)} = m. \tag{2.2}$$

para todo $m \in M$.

A equação (2.1) nos leva a definir:

$$\sum m_{(0)} \otimes m_{(1)} \otimes m_{(2)} := \sum (m_{(0)})_{(0)} \otimes (m_{(0)})_{(1)} \otimes m_{(1)} = \sum m_{(0)} \otimes (m_{(1)})_1 \otimes (m_{(1)})_2.$$

Note que, nesta notação, a comutatividade do diagrama da Definição 2.3.4 é expressa por

$$\sum g(m)_{(0)} \otimes g(m)_{(1)} = \sum g(m_{(0)}) \otimes m_{(1)}, \text{ para todo } m \in M.$$

Consideremos agora alguns exemplos de C-comódulos:

Exemplo 2.3.5. Toda coálgebra (C,Δ,ε) é um C-comódulo com $\rho = \Delta$.

Exemplo 2.3.6. Seja (C,Δ,ε) uma coálgebra e M um R-módulo. Então $M \otimes C$ é um

C-comódulo com $\rho\colon M \otimes C \longrightarrow M \otimes C \otimes C$ dada por

$$\rho(m \otimes c) = \sum m \otimes c_1 \otimes c_2$$

para todo $m \in M$ e $c \in C$.

Exemplo 2.3.7. Dado $S \neq \varnothing$ um conjunto, considere a coálgebra $C = RS$ (como no Exemplo 2.1.7). Se $(M_s)_{s\in S}$ é uma família de C-comódulos então

$$M = \bigoplus_{s\in S} M_s$$

é um C-comódulo com $\rho\colon M \longrightarrow M \otimes C$ dado por $\rho(m_s) = m_s \otimes s$,para todo $s \in S$ e $m_s \in M_s$.

Dada uma coálgebra C, existe uma relação entre os C-comódulos e os C^*-módulos. Tal relação é dada por:

Proposição 2.3.8. *[13, 4.1] Sejam C uma coálgebra, C^* a álgebra dual a C e M um R-módulo. Se (M, ρ) é um C-comódulo então $(M, \cdot)$ é um C^*-módulo, com*

$$\begin{array}{rccc} \cdot\colon & C^* \otimes M & \longrightarrow & M \\ & f \otimes m & \longmapsto & \sum m_{(0)} f(m_{(1)}) \end{array}$$

Demonstração. De fato, para todo $f, g \in C^*$ e para todo $m \in M$,

$$\begin{aligned} f \cdot (g \cdot m) &= f \cdot \left(\sum m_{(0)} g(m_{(1)})\right) \\ &= \sum (f \cdot m_{(0)}) g(m_{(1)}) \\ &= \sum (m_{(0)})_{(0)} f(m_{(0)})_{(1)} g(m_{(1)}) \\ &= \sum (m_{(0)}) f(m_{(1)}) g(m_{(2)}) \\ &= \sum (m_{(0)}) fg(m_{(1)}) \\ &= (fg) \cdot m. \end{aligned}$$

e

$$1_{C^*} \cdot m = \varepsilon \cdot m = \sum m_{(0)} \varepsilon m_{(1)} = m.$$

■

2.4 Biálgebras e Álgebras de Hopf

Comecemos com uma proposição:

Proposição 2.4.1. *Seja H um R-módulo tal que (H, μ, η) é uma álgebra e (H, Δ, ε) é uma coálgebra. São equivalentes:*

a) μ e η são homomorfismos de coálgebras;

b) Δ e ε são homomorfismos de álgebras.

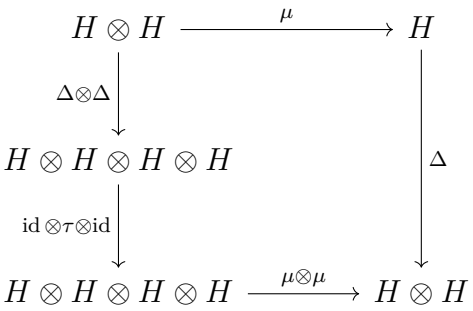
Demonstração. Pela Proposição 1.11, $H \otimes H$ é uma álgebra com

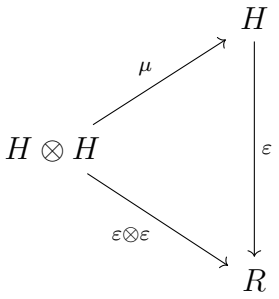
$$\mu_{H\otimes H} = (\mu \otimes \mu) \circ (\mathrm{id} \otimes \tau \otimes \mathrm{id})$$
$$\eta_{H\otimes H} = \eta \otimes \eta.$$

Por outro lado, pelo Exemplo 2.1.10, $H \otimes H$ também é uma coálgebra com

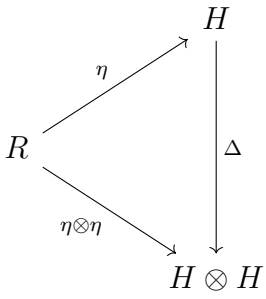
$$\Delta_{H\otimes H} = (\mathrm{id} \otimes \tau \otimes \mathrm{id}) \circ (\Delta \otimes \Delta)$$
$$\varepsilon_{H\otimes H} = \varepsilon \otimes \varepsilon.$$

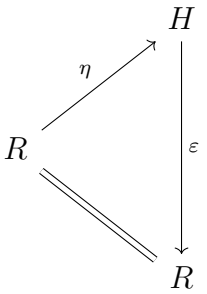
A aplicação μ é um homomorfismo de coálgebras se, e somente se, os seguintes diagramas são comutativos:





Por sua vez, η é um homomorfismo de coálgebras se, e somente se, os seguintes diagramas comutam:





Com isso, basta notar que esses diagramas são os mesmos que garantem que Δ e ε são homomorfismos de álgebras. ∎

Usando a notação de Sweedler, o fato de Δ e ε serem homomorfismos de álgebras pode ser interpretada da seguinte forma:

$$\begin{aligned}\Delta(xy) &= \sum x_1y_1 \otimes x_2y_2\\ \varepsilon(xy) &= \varepsilon(x)\varepsilon(y)\\ \Delta(1) &= 1 \otimes 1\\ \varepsilon(1) &= 1.\end{aligned}$$

Definição 2.4.2 (Biálgebra)**.** Dizemos que $(H, \mu, \eta, \Delta, \varepsilon)$ é uma *biálgebra* se (H, μ, η) é uma álgebra, (H, Δ, ε) é uma coálgebra e vale uma das condições equivalentes da Proposição 2.4.1.

Consideremos alguns exemplos de biálgebras.

Exemplo 2.4.3. Seja M um monoide. O R-módulo livre RM é uma biálgebra com $\Delta(m) = m \otimes m$ e $\varepsilon(m) = 1$, para todo $m \in M$. Em particular RG é uma biálgebra, com G um grupo. De modo ainda mais particular, R é uma biálgebra.

Exemplo 2.4.4. Sejam H_1 e H_2 biálgebras. Então $H_1 \otimes H_2$ é naturalmente uma biálgebra com estrutura dada pelo produto tensorial de álgebras e de R- coálgebras.

Proposição 2.4.5. *Seja $(H, \mu, \eta, \Delta, \varepsilon)$ uma biálgebra tal que H é um R-módulo livre finitamente gerado. Então $(H^*, \bar{\mu}, \bar{\eta}, \bar{\Delta}, \bar{\varepsilon})$ é uma biálgebra com $\bar{\mu} = \Delta^* \circ \varphi$, $\bar{\eta} = \varepsilon^*$, $\bar{\Delta} = \varphi^{-1} \circ \mu^*$ e $\bar{\varepsilon} = \eta^*$, com φ dada no Lema 2.2.1.*

Demonstração. Pela Proposição 2.2.2, $(H^*, \bar{\mu}, \bar{\eta})$ é uma álgebra e, pela Proposição 2.2.3, $(H^*, \bar{\Delta}, \bar{\varepsilon})$ é uma coálgebra. Mostremos que $\bar{\Delta}$ e $\bar{\varepsilon}$ são homomorfismos de álgebras. Lembre-se de que $\bar{\varepsilon}(h^*) = h^*(1_H)$ e que $\bar{\Delta}(h^*) = \sum h_1^* \otimes h_2^*$, com $h^* \in H^*$ tal que para todo $x, y \in H$, $h^*(xy) = \sum h_1^*(x) \otimes h_2^*(y)$.
Se $h^*, g^* \in H^*$ e $\bar{\Delta}(h^*) = \sum h_1^* \otimes h_2^*$ e $\bar{\Delta}(g^*) = \sum g_1^* \otimes g_2^*$, então, para todo $x, y \in H$,

$$\begin{aligned}(h^*g^*)(xy) &= \sum h^*(x_1y_1)g^*(x_2y_2)\\ &= \sum h_1^*(x_1)h_2^*(y_1)g_1^*(x_2)g_2^*(y_2)\\ &= \sum (h_1^*g_1^*)(x)(h_2^*g_2^*)(y).\end{aligned}$$

Portanto,

$$\bar{\Delta}(h^*g^*) = \sum h_1^*g_1^* \otimes h_2^*g_2^* = \bar{\Delta}(h^*)\bar{\Delta}(g^*).$$

Além disso, $\varepsilon(xy) = \varepsilon(x)\varepsilon(y)$, para todo $x, y \in H$. Logo $\bar{\Delta}(\varepsilon) = \varepsilon \otimes \varepsilon$ e, assim, $\bar{\Delta}$ é um homomorfismo de álgebras.

Para mostrar que $\bar{\varepsilon}$ é um homomorfismo de álgebras, basta notar que valem

$$\bar{\varepsilon}(h^*g^*) = (h^*g^*)(1_H) = h^*(1_H)g^*(1_H) = \bar{\varepsilon}(h^*)\bar{\varepsilon}(g^*),$$
$$\bar{\varepsilon}(\varepsilon) = \varepsilon(1_H) = 1.$$

■

Definição 2.4.6 (Homomorfismo de biálgebras)**.** Sejam H_1 e H_2 duas biálgebras. Dizemos que uma aplicação $f\colon H_1 \longrightarrow H_2$ é um *homomorfismo de biálgebras* se f for um homomorfismo de álgebras (na álgebra subjacente) e um homomorfismo de coálgebras (na coálgebra subjacente).

O seguinte exemplo mostra que, apesar de todo R-módulo admitir estrutura de coálgebra (Exemplo 2.1.7), nem toda álgebra admite estrutura de biálgebra.

Exemplo 2.4.7. Seja k um corpo e $n \geq 2$ um número natural. Não existe estrutura de biálgebra para o espaço vetorial das matrizes $M_n(k)$ tal que a estrutura de álgebra subjacente coincida com a álgebra usual de matrizes. Para verificar isso, suponha que $M_n(k)$ tenha estrutura de biálgebra. Logo $\varepsilon\colon M_n(k) \longrightarrow k$ é um homomorfismo de álgebras. Consequentemente, $\ker(\varepsilon)$ é um ideal (bilateral) de $M_n(k)$. Como $M_n(k)$ é simples ([25], cap. IX), então $\ker(\varepsilon) = 0$ ou $\ker(\varepsilon) = M_n(k)$. Como $\varepsilon(1) = 1$, então $\ker(\varepsilon) = \{0\}$, o que é absurdo dado que $\dim(M_n(k)) > \dim(k)$ quando $n \geq 2$. Ou seja, a única álgebra de matrizes $M_n(k)$ que admite estrutura de biálgebra é $M_1(k) \cong k$.

Sejam (A, μ, η) uma álgebra e (C, Δ, ε) uma coálgebra. Considere o R-módulo $\mathrm{Hom}_R(C, A)$.

Proposição 2.4.8. $\mathrm{Hom}_R(C, A)$ *é uma álgebra com multiplicação*

$$(f * g)(c) = (\mu \circ (f \otimes g) \circ \Delta)(c) = \sum f(c_1)g(c_2)$$

para todo $f, g \in \mathrm{Hom}_R(C, A)$ *e* $c \in C$*. A unidade de* $\mathrm{Hom}_R(C, A)$ *é* $\eta \circ \varepsilon$*.*

Demonstração. A multiplicação em $\mathrm{Hom}_R(C, A)$ é associativa pois, para todos $f, g, h \in \mathrm{Hom}_R(C, A)$ e $c \in C$, temos

$$\begin{aligned}((f * g) * h)(c) &= \sum (f * g)(c_1)h(c_2) \\ &= \sum f(c_1)g(c_2)h(c_3) \\ &= \sum f(c_1)(g * h)(c_2) \\ &= (f * (g * h))(c).\end{aligned}$$

Por sua vez, $\eta \circ \varepsilon$ é unidade pois, para todo $f \in \mathrm{Hom}(C, A)$ e $c \in C$,

$$\begin{aligned} f * (\eta \circ \varepsilon)(c) &= \sum f(c_1)(\eta \circ \varepsilon)(c_2) \\ &= \sum f(c_1)\varepsilon(c_2)1_A \\ &= f(c) \end{aligned}$$

e, analogamente, $(\eta \circ \varepsilon) * f = f$. ■

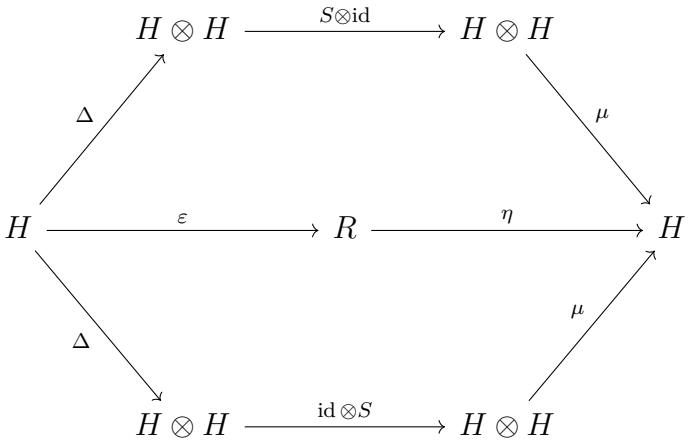
O produto definido na proposição anterior é chamado produto de convolução.

Seja H uma biálgebra. Denote por H_a a álgebra subjacente a H e por H_c a coálgebra subjacente a H. Pela proposição anterior, podemos considerar a álgebra $\mathrm{Hom}_R(H_c, H_a)$. Como a identidade $\mathrm{id}\colon H \longrightarrow H$ pertence à álgebra $\mathrm{Hom}_R(H_c, H_a)$, podemos nos perguntar se id é invertível na álgebra $\mathrm{Hom}_R(H_c, H_a)$ (com o produto $*$), o que motiva a seguinte definição:

Definição 2.4.9 (Antípoda)**.** Seja H uma biálgebra. Dizemos que uma aplicação linear $S\colon H \longrightarrow H$ é uma *antípoda* de H se S for a inversa de id pelo produto de convolução, ou seja, se

$$\mathrm{id} * S = S * \mathrm{id} = \eta \circ \varepsilon.$$

Isso é o equivalente a pedir que o seguinte diagrama seja comutativo:



Ou, na notação de Sweedler,

$$\sum S(x_1)x_2 = \sum x_1 S(x_2) = \varepsilon(x)1_H$$

para todo $x \in H$.

Observe que a antípoda, se existir, é única, pela unicidade do inverso do elemento id na álgebra $\mathrm{Hom}_R(H_c, H_a)$.

Definição 2.4.10 (Álgebra de Hopf)**.** Dizemos que uma biálgebra $(H, \mu, \eta, \Delta, \varepsilon)$ é

uma *álgebra de Hopf* se existe antípoda $S\colon H \longrightarrow H$. Neste caso podemos denotar a estrutura da álgebra de Hopf por $(H, \mu, \eta, \Delta, \varepsilon, S)$.

Definição 2.4.11 (Homomorfismo de Álgebras de Hopf)**.** Sejam H_1 e H_2 álgebras de Hopf. Dizemos que uma aplicação linear $f\colon H_1 \longrightarrow H_2$ é um *homomorfismo de álgebras de Hopf* se f for um homomorfismo de biálgebras.

A definição anterior pode causar certa estranheza ao leitor, por não ser necessário pedir alguma relação de f com as antípodas de H_1 e H_2. Na verdade, homomorfismo de álgebras de Hopf de fato preservam antípodas; não como condição e sim como um resultado, que enunciamos a seguir:

Proposição 2.4.12. *[16, 4.2.5] Sejam $(H_1, \mu_1, \eta_1, \Delta_1, \varepsilon_1, S_1)$ e $(H_2, \mu_2, \eta_2, \Delta_2, \varepsilon_2, S_2)$ álgebras de Hopf. Se $f\colon H_1 \longrightarrow H_2$ é um homomorfismo de álgebras de Hopf então*

$$S_2 \circ f = f \circ S_1.$$

Demonstração. Note que $S_2 \circ f$ e $f \circ S_1$ são elementos de $\mathrm{Hom}_R(H_1, H_2)$. Se mostrarmos que ambos são $*$-invertíveis e tem a mesma inversa, então eles serão iguais. De fato, $S_2 \circ f$ é inversa à esquerda de f pois, dado $x \in H_1$,

$$\begin{aligned}((S_2 \circ f) * f)(x) &= \sum (S_2 \circ f)(x_1) f(x_2) \\ &= \sum S_2((f(x)_1) f(x)_2 \\ &= \varepsilon_2(f(x)) 1_{H_2} \\ &= \varepsilon_1(x) 1_{H_2} \\ &= (\eta_2 \circ \varepsilon_1)(x).\end{aligned}$$

Analogamente, $f * (S_2 \circ f) = \eta_2 \circ \varepsilon_1$.
Por outro lado, $f \circ S_1$ é inversa à direita de f pois, dado $x \in H_1$,

$$\begin{aligned}(f * (f \circ S_1))(x) &= \sum f(x_1)(f \circ S_1)(x_2) \\ &= f\left(\sum x_1 S_1(x_2)\right) \\ &= f(\varepsilon_1(x)) 1_{H_1} \\ &= \varepsilon_1(x) 1_{H_2} \\ &= (\eta_2 \circ \varepsilon_1)(x)\end{aligned}$$

e de modo similar $(f \circ S_1) * f = \eta_2 \circ \varepsilon_1$. Isso completa a prova. ∎

Os próximos resultados trazem propriedades da antípoda.

Proposição 2.4.13. *[13, 15.4] Seja $(H, \mu, \eta, \Delta, \varepsilon, S)$ uma álgebra de Hopf. Então*

a) $S(xy) = S(y)S(x)$ *para todo* $x, y \in H$*;*

b) $S(1_H) = 1_H$*;*

c) $\Delta(S(x)) = \sum S(x_2) \otimes S(x_1)$ *para todo* $x \in H$*;*

d) $\varepsilon(S(x)) = \varepsilon(x)$ *para todo* $x \in H$*.*

Demonstração.

a) Considere a álgebra $\mathrm{Hom}_R(H \otimes H, H)$ com produto de convolução e identidade $\eta_H \circ \varepsilon_{H\otimes H} \colon H \otimes H \longrightarrow H$. Defina, para todo $x, y \in H$,

$$\begin{array}{rccc} F\colon & H \otimes H & \longrightarrow & H \\ & x \otimes y & \longmapsto & S(y)S(x), \end{array}$$

$$\begin{array}{rccc} G\colon & H \otimes H & \longrightarrow & H \\ & x \otimes y & \longmapsto & S(xy), \end{array}$$

$$\begin{array}{rccc} M\colon & H \otimes H & \longrightarrow & H \\ & x \otimes y & \longmapsto & xy. \end{array}$$

Mostremos que F e G são inversas por convolução de M. De fato, dados $x, y \in H$,

$$\begin{aligned} (M * F)(x \otimes y) &= \sum M((x \otimes y)_1)F((x \otimes y)_2) \\ &= \sum M(x_1 \otimes y_1)F(x_2 \otimes y_2) \\ &= \sum x_1 y_1 S(y_2)S(x_2) \\ &= \sum x_1 \varepsilon(y) 1_H S(x_2) \\ &= \varepsilon(x)\varepsilon(y)1_H \\ &= \varepsilon_{H\otimes H}(x \otimes y)1_H \\ &= \eta_H \circ \varepsilon_{H\otimes H}(x \otimes y). \end{aligned}$$

Analogamente, $(F * M) = \eta_H \circ \varepsilon_{H\otimes H}$. Por outro lado,

$$\begin{aligned}(G * M)(x \otimes y) &= \sum G((x \otimes y)_1)M((x \otimes yg)_2) \\ &= \sum G(x_1 \otimes y_1)M(x_2 \otimes y_2) \\ &= \sum S(x_1y_1)x_2y_2 \\ &= \sum S((xy)_1)(xy)_2 \\ &= \varepsilon(xy))1_H \\ &= \eta_H \circ \varepsilon_{H\otimes H}(x \otimes y).\end{aligned}$$

e, de modo similar, $M*G = \eta_H\circ\varepsilon_{H\otimes H}$. Logo, pela unicidade do elemento inverso, $F = G$ e portanto $S(xy) = S(y)S(x)$ para todo $x, y \in H$.

b) De fato,

$$S(1_H) = S(1_H)1_H = (S * \mathrm{id})(1_H) = (\eta \circ \varepsilon)(1_H) = \varepsilon(1_H)1_H = 1_H.$$

c) Considere a álgebra $\mathrm{Hom}_R(H, H \otimes H)$ com produto de convolução e identidade $\eta_{H\otimes H} \circ \varepsilon_H \colon H \longrightarrow H \otimes_H H$. Defina para todo $x \in H$

$$\begin{aligned} F\colon \quad H &\longrightarrow H \otimes H \\ x &\longmapsto \Delta(S(x)), \end{aligned}$$

$$\begin{aligned} G\colon \quad H &\longrightarrow H \otimes H \\ x &\longmapsto \sum S(x_2) \otimes S(x_1). \end{aligned}$$

Mostremos que F e G são inversas por convolução de Δ. De fato, dado $x \in H$,

$$\begin{aligned}(\Delta * F)(x) &= \sum \Delta(x_1)F(x_2) \\ &= \sum \Delta(x_1)\Delta(S(x_2)) \\ &= \Delta\left(\sum x_1S(x_2)\right) \\ &= \Delta(\varepsilon(x)1_H) \\ &= \varepsilon(x)1_H \otimes 1_H \\ &= \eta_{H\otimes H} \circ \varepsilon_H(x)\end{aligned}$$

Analogamente, $(F * \Delta) = \eta_H \circ \varepsilon_{H\otimes H}$. Por outro lado,

$$\begin{aligned}(G * \Delta)(x) &= \sum G(x_1)\Delta(x_2)\\ &= \sum (S((x_1)_2) \otimes S((x_1)_1)((x_2)_1 \otimes (x_2)_2)\\ &= \sum (S(x_2) \otimes S(x_1))(x_3 \otimes x_4)\\ &= \sum S(x_2)x_3 \otimes S(x_1)x_4\\ &= \sum S((x_2)_1)(x_2)_2 \otimes S(x_1)x_3\\ &= \sum \varepsilon(x_2)1_H \otimes S(x_1)x_3\\ &= \sum 1 \otimes S(x_1)\varepsilon((x_2)_1)(x_2)_2\\ &= \sum 1 \otimes S(x_1)x_2\\ &= 1 \otimes \varepsilon(x)1_H\\ &= \eta_{H\otimes H} \circ \varepsilon_H(x)\end{aligned}$$

e, de modo similar, $\Delta * G = \eta_H \circ \varepsilon_{H\otimes H}$. Logo, pela unicidade do elemento inverso, $F = G$. Então, para todo $x \in H$,

$$\Delta(S(x)) = \sum S(x_2) \otimes S(x_1).$$

d) De fato,

$$\varepsilon(S(x)) = \sum \varepsilon(S(x_1))\varepsilon(x_2) = \varepsilon\left(\sum S(x_1)x_2\right) = \varepsilon(\varepsilon(h)1_H) = \varepsilon(x)\varepsilon(1_H) = \varepsilon(x).$$

■

Na proposição anterior, por S satisfazer os itens a) e b), diremos que S é um antihomomorfismo de álgebras e por satisfazer os itens c) e d), diremos que S é um antihomomorfismo de coálgebras.

Proposição 2.4.14. *Seja H uma álgebra de Hopf com antípoda S. Se H é um R-módulo livre finitamente gerado então H^* é uma álgebra de Hopf com antípoda S^*.*

Demonstração. Pela Proposição 2.4.5, H^* é uma biálgebra. Mostremos que S^* é antípoda. Seja $h^* \in H^*$ e $\bar{\Delta}(h^*) = \sum h_1^* \otimes h_2^*$ comultiplicação de H^*. Então para todo $x \in H$

$$\begin{aligned}(S^* * \mathrm{id})(h^*)(x) &= \sum((S^*(h_1^*)h_2^*)(x) \\ &= \sum(S^*(h_1^*))(x_1)h_2^*(x_2) \\ &= \sum h_1^*(S(x_1))h_2^*(x_2) \\ &= \sum h^*(S(x_1)x_2) \\ &= h^*(\varepsilon(x)1_H) \\ &= \varepsilon(x)h^*(1_H) \\ &= \bar{\varepsilon}(h^*)\varepsilon(x)\end{aligned}$$

com $\bar{\varepsilon}$ a counidade de H^*. Com isso, $\sum(S^* \circ h_1^*)h_2^* = \bar{\varepsilon}(h^*)\varepsilon(h^*)\varepsilon$.

Analogamente, é possível mostrar que $\sum h_1^* S^*(h_2^*) = \bar{\varepsilon}(h^*)\varepsilon$. ■

Exemplo 2.4.15. Sejam H_1 e H_2 álgebras de Hopf com antípodas S_1 e S_2 respectivamente. Então $H_1 \otimes H_2$ é uma álgebra de Hopf com antípoda $S_1 \otimes S_2$.

Terminamos esse capítulo com um último exemplo que dá estrutura de álgebra de Hopf às álgebras de grupo:

Exemplo 2.4.16. Seja G um grupo e RG o R-módulo livre com base G. Pelo Exemplo 2.4.3, RG é uma biálgebra. Considere a aplicação linear $S\colon H \longrightarrow H$ dada por $s(g) = g^{-1}$, para todo $g \in G$. Mostremos que S é uma (e portanto a) antípoda que torna RG uma álgebra de Hopf. Com efeito,

$$S * \mathrm{id}(g) = S(g)g = g^{-1}g = 1_G = \varepsilon(g)1_{RG} = \eta \circ \varepsilon(g),$$

para todo $g \in G$. Isto mostra que $S * \mathrm{id} = \eta \circ \varepsilon$. Analogamente, $\mathrm{id} * S = \eta \circ \varepsilon$.

No caso em que G é finito, pela Proposição 2.4.14, $(RG)^*$ será uma álgebra de Hopf com antípoda S^*.

Nesse caso, a comultiplicação, a counidade e a antípoda de $(RG)^*$ adquirem uma forma explícita particularmente simples do seguinte modo: Para cada $g \in G$, defina a aplicação

$$\begin{array}{rccc} p_g\colon & RG & \longrightarrow & R \\ & h & \longmapsto & \delta_{g,h} \end{array}$$

$(p_g)_{g\in G}$ é um sistema completo de idempotentes ortogonais para $(RG)^*$, ou seja,

$$p_g^2 = p_g, p_g p_h = 0 \text{ para todo } g \neq h \text{ e } \sum_{g\in G} p_g = 1_{(RG)^*}$$

e $(RG)^*$ é livre com base $\{p_g \mid g \in G\}$. Com isso, é possível mostrar que a comultiplicação, a counidade e a antípoda de $(RG)^*$ podem ser expressas em termos

da base $\{p_g \mid g \in G\}$ da seguinte forma:

$$\begin{aligned}\Delta^*(p_g) &= \sum_{x\in G} p_x \otimes p_{x^{-1}g}\\ \varepsilon^*(p_g) &= \delta_{1,g}\\ S^*(p_g) &= p_{g^{-1}},\end{aligned}$$

para todo $g \in G$.

2.5 Outros Exemplos de Álgebras de Hopf

Esta seção é motivada por um clássico exemplo de álgebras de Hopf: as álgebras de Taft. As álgebras de Hopf vistas até o momento são cocomutativas, isto é,

$$\Delta(h) = \sum h_1 \otimes h_2 = \sum h_2 \otimes h_1,$$

para todo $h \in H$. Em contrapartida, as álgebras desta seção não são comutativas e nem cocomutativas.

Estamos interessados em duas generalizações da k-álgebra de Taft que consideraremos nesta seção: as álgebras monomiais não semissimples sobre um corpo algebricamente fechado de característica zero [15] e as álgebras de Taft sobre um anel R [37].

2.5.1 Álgebras de Hopf monomiais não semissimples

Seja $R = k$ um corpo algebricamente fechado de característica zero. Introduziremos as álgebras monomiais não semissimples que, sobre um corpo, generalizam as álgebras de Taft. A definição das álgebras monomiais não semissimples foi dada no contexto de álgebras de caminhos e por isso foge do escopo deste trabalho. Porém, tais álgebras foram caracterizadas (de modo mais tratável) por Chen, Huang, Ye e Zhang em [15]. Por simplicidade, adotaremos tal caracterização como a própria definição das álgebras monomiais não semissimples.

Seguindo [15], definimos os dados de grupo:

Definição 2.5.1. Seja k um corpo algebricamente fechado de característica zero. Um *dado de grupo* é uma quádrupla $\mathbb{G} = (G, g, \chi, \mu)$, com:

(i) G um grupo finito e g um elemento no centro de G;

(ii) $\chi\colon G \longrightarrow k^\times$ uma representação de dimensão 1 (um homomorfismo de grupos) com $\chi(g) \neq 1$;

(iii) $\mu \in k$ tal que $\mu = 0$ se $o(g) = o(\chi(g))$ e, se $\mu \neq 0$, então $\chi^{o(\chi(g))} = 1$.

Sempre que estivermos no contexto de dados de grupo, denote $n = o(g)$ e $d = o(\chi(g))$.

Para cada dado de grupo $\mathbb{G} = (G, g, \chi, \mu)$, os autores em [15] associam uma álgebra $A(\mathbb{G})$ dada como o quociente do produto livre $G * k[y]$ pelo ideal gerado pelas relações

$$yx = \chi(x)xy \text{ e } y^d = \mu(1 - g^d),$$

para todo $x \in G$.

Pelo lema do diamante de Bergman [8], o conjunto $\{xy^i \,|\, x \in G, 0 \leq i \leq d-1\}$ é uma base para $A(\mathbb{G})$ [15]. Portanto $\dim_k(A(\mathbb{G})) = |G|d$. $A(\mathbb{G})$ admite estrutura de álgebra de Hopf com comultiplicação Δ, counidade ε e antípoda S dadas por

$$\Delta(y) = 1 \otimes y + y \otimes g,\ \varepsilon(y) = 0,\ S(y) = -yg^{-1},$$
$$\Delta(x) = x \otimes x,\ \varepsilon(x) = 1,\ S(x) = x^{-1},\ \forall x \in G.$$

Em [10] Bichon divide os dados de grupo em seis "tipos" disjuntos. De modo natural, as álgebras monomiais não semissimples também seguem tal divisão. O objetivo por trás dessa divisão é classificar os objetos $A(\mathbb{G})$-Galois (que serão definidos no próximo capítulo). Tanto para a divisão dos tipos de dados de grupo quanto para a posterior classificação dos objetos $A(\mathbb{G})$-Galois, convém uma breve revisão de grupos de cohomologia. Para mais, veja [10] e [29].

Dado G um grupo e $k^\times$ o grupo multiplicativo dos elementos invertíveis em k, chamamos de 2-cociclos (normalizados) de G os elementos de

$$Z^2(G, k^\times) = \{\sigma \colon G \times G \longrightarrow k^\times \mid \sigma(x,y)\sigma(xy,z) = \sigma(x,yz)\sigma(y,z), \sigma(x,1) = \sigma(1,x) = 1\}.$$

Seja $f \colon G \longrightarrow k^\times$ uma aplicação tal que $f(1) = 1$ e seja $\partial(f) \colon G \times G \longrightarrow k^\times$ dada por

$$\partial(f)(x,y) = f(x)f(y)f(xy)^{-1}$$

para todos $x, y \in G$. $\partial(f)$, chamada de *cobordo*. Definimos

$$B^2(G, k^\times) = \{\partial(f) \mid f(1) = 1\}.$$

Como $B^2(G, k^\times)$ é um subgrupo normal de $Z^2(G, k^\times)$, podemos considerar o quociente

$$H^2(G, k^\times) := \frac{Z^2(G, k^\times)}{B^2(G, k^\times)},$$

chamado *segundo grupo de cohomologia de G sobre $k^\times$*. Os elementos de $H^2(G, k^\times)$ são chamados de *classes de cohomologia.*

Se $\sigma, \tau \in Z^2(G, k^\times)$ estão numa mesma classe de cohomologia, ou seja, se existe $f\colon G \longrightarrow k^\times$ tal que $f(1) = 1$ e $\tau = \partial(f)\sigma$, dizemos que σ e τ são *coomólogos*, isto é $[\sigma] = [\tau]$ em $H^2(G, k^\times)$.

Na Seção 5.1.1, a seguinte modificação do conceito de grupos de cohomologia será utilizado: Fixado g um elemento central em G, considere

$$Z^2_g(G, k^\times) = \{\sigma \in Z^2(G, k^\times) \mid \sigma(g, x) = \sigma(x, g) \text{ para todo } x \in G\}$$

e

$$B^2_g(G, k^\times) = \{\partial(f) \in B^2(G, k^\times) \mid f(1) = f(g) = 1\}.$$

$Z^2_g(G, k^\times)$ é um grupo e $B^2_g(G, k^\times)$ é subgrupo normal de $Z^2_g(G, k^\times)$. Com isso, fixados g_1, g_2 no centro de G definimos

$$H^2_{g_1,g_2}(G, k^\times) := \frac{Z^2_{g_1}(G, k^\times)}{B^2_{g_2}(G, k^\times)}.$$

Note que $H^2_{1,1}(G, k^\times) = H^2(G, k^\times)$.

Com isso, seguindo [10] vamos dividir os dados de grupo $\mathbb{G} = (G, g, \chi, \mu)$ (e portanto também as álgebras monomiais não semissimples) em 6 tipos diferentes:

- Tipo I: $\mu = 0$, $d = n$ e $\chi^d = 1$;
- Tipo II: $\mu = 0$, $d = n$ e $\chi^d \neq 1$;
- Tipo III: $\mu = 0$, $d < n$ e $\chi^d = 1$;
- Tipo IV: $\mu = 0$, $d < n$, $\chi^d \neq 1$ e não existe $\sigma \in Z^2(G, k^\times)$, tal que $\sigma(g^d, x) = \chi^d(x)\sigma(x, g^d)$, para todo $x \in G$;
- Tipo V: $\mu = 0$, $d < n$, $\chi^d \neq 1$ e existe $\sigma \in Z^2(G, k^\times)$ com $\sigma(g^d, x) = \chi^d(x)\sigma(x, g^d)$, para todo $x \in G$;
- Tipo VI: $\mu \neq 0$ (e portanto $d < n$ e $\chi^d = 1$).

Consideremos o caso particular do tipo I dado por um gerador g em $G = \mathbb{Z}/N\mathbb{Z}$ para algum $N \geq 2$. Esta é a álgebra de Taft de dimensão N^2 [31], da qual falaremos a seguir.

2.5.2 As álgebras de Taft

Fixe $N \geq 2$ um inteiro. Nesta seção, inicialmente estaremos considerando $R = k$ um corpo possuindo uma raiz N-ésima primitiva da unidade ζ. Em particular, $\operatorname{char} k = 0$ ou $(N, \operatorname{char} k) = 1$. Depois retornaremos ao caso mais geral, no qual R será um anel comutativo com unidade.

A seguinte álgebra definida por geradores e relações

$$H_N^\zeta = \left\langle g, x \mid g^N = 1,\ xg = \zeta gx,\ x^N = 0 \right\rangle$$

é chamada álgebra de Taft. O caso particular $H_2 := H_2^{-1}$ é conhecido como álgebra de Sweedler de dimensão 4. A álgebra de Sweedler é conhecida por ser o exemplo mais simples de álgebra de Hopf que não é comutativa nem cocomutativa. É fácil ver que H_2 tem base $\{1, g, x, gx\}$. Para as álgebras de Taft, temos:

Proposição 2.5.2. *[45] O conjunto $\{g^i x^j \mid 0 \leqslant i, j \leqslant N-1\}$ é uma base de H_N^ζ.*

Proposição 2.5.3. *[45] H_N^ζ é uma álgebra de Hopf com Δ, ε e S definidas por*

$$\begin{aligned} \Delta(g) &= g \otimes g & \Delta(x) &= 1 \otimes x + x \otimes g \\ \varepsilon(g) &= 1 & \varepsilon(x) &= 0 \\ S(g) &= g^{N-1} & S(x) &= -\zeta^{-1} g^{N-1} x. \end{aligned}$$

Com um pouco mais de tecnicidade, as álgebras de Taft podem ser definidas também sobre anéis comutativos com unidade. Regressemos, pois a tal condição para R. Seguindo [37], recordemos a noção de polinômio ciclotômico:

Para cada n inteiro positivo, o *n-ésimo polinômio ciclotômico* é dado em $\mathbb{C}[X]$ por

$$\Phi_n(X) = \prod_{\substack{1 \leqslant m \leqslant n \\ (m,n)=1}} \left(X - e^{2i\pi \frac{m}{n}} \right).$$

Por comparação dos conjuntos de zeros, não é difícil ver que

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

Embora os polinômios ciclotômicos tenham sido definidos sobre $\mathbb{C}[X]$, segue do algoritmo de Euclides para polinômios [36, IV, 1.1], que todos seus coeficientes são de fato inteiros, logo tais polinômios estão em $\mathbb{Z}[X]$. Além disso, o menor polinômio ciclotômico com algum coeficiente diferente de $\{-1, 0, 1\}$ é $\Phi_{105}(X)$ que tem -2 como coeficiente de X^7. É possível mostrar também que, por um lado, existem infinitos

polinômios ciclotômicos somente com coeficientes $\{-1, 0, 1\}$ e, por outro, que existem polinômios ciclotômicos com coeficientes de tamanho arbitrariamente grande, conforme [27].

Os primeiros polinômios ciclotômicos são estes:

$$\begin{aligned}
\Phi_1(X) &= X - 1, \\
\Phi_2(X) &= X + 1, \\
\Phi_3(X) &= X^2 + X + 1, \\
\Phi_4(X) &= X^2 + 1, \\
\Phi_5(X) &= X^4 + X^3 + X^2 + X + 1.
\end{aligned}$$

No contexto dos corpos, há uma relação entre raízes da unidade e polinômios ciclotômicos: Se x é uma raiz N-ésima primitiva da unidade então x é uma raiz de $\Phi_N(X)$. A recíproca não vale. Por exemplo, se $k = \mathbb{Z}/p\mathbb{Z}$, p primo, então $q = 1$ é raiz de $\Phi_p(X)$ mas claramente 1 não é raiz p-ésima primitiva da unidade.

Mais detalhes sobre os polinômios ciclotômicos podem ser encontrados em [36, VI, §3].

Para $N \geq 2$ um inteiro, suponha que exista $q \in R$ uma raiz do N-ésimo polinômio ciclotômico. Em particular, $q^N = 1$ e, dado $\zeta_N \in \mathbb{C}$ uma raiz N-ésima primitiva da unidade em $\mathbb{C}$, então existe um (único) homomorfismo de anéis $\mathbb{Z}[\zeta_N] \longrightarrow R$ tal que $\zeta_N \mapsto q$.

Para tal q, é possível definir o q-análogo do binômio de Newton:

$$\binom{n}{i}_q = \frac{(q^n - 1)\cdots(q^{n-i+1} - 1)}{(q^i - 1)\cdots(q - 1)}.$$

Tal expressão está bem definida pois apesar de aparentemente ser uma divisão, é, na verdade expressa como um "polinômio em q".

De [37, 2.2] e da proposição [30, IV.2.2], resulta que:

Lema 2.5.4. *Seja p uma raiz do N-ésimo polinômio ciclotômico. Se z e w são duas variáveis tais que $zw = pwz$, então*

$$(z + w)^n = \sum_{i=0}^{n} \binom{n}{i}_p z^i w^{n-i}.$$

Em particular, $(z + w)^N = z^N + w^N$.

Para cada par (N, q), com $N \geq 2$ e $q \in R$ uma raiz do N-ésimo polinômio

ciclotômico, definimos a seguinte álgebra dada por geradores e relações:

$$H_N^q = \left\langle g, x \mid g^N = 1,\ xg = qgx,\ x^N = 0 \right\rangle.$$

H_N^q será chamada álgebra de Taft (sobre R).

Decorre do lema do diamante de Bergman [8] que:

Proposição 2.5.5. *[37] O conjunto* $\{g^i x^j \mid 0 \leqslant i, j \leqslant N-1\}$ *é uma base de* H_N^q.

Ademais, verifica-se que:

Proposição 2.5.6. *[37]* H_N^q *é uma álgebra de Hopf com* Δ, ε *e* S *definidas por*

$$\begin{aligned} \Delta(g) &= g \otimes g & \Delta(x) &= 1 \otimes x + x \otimes g \\ \varepsilon(g) &= 1 & \varepsilon(x) &= 0 \\ S(g) &= g^{N-1} & S(x) &= -q^{-1} g^{N-1} x. \end{aligned}$$

Capítulo 3

Extensões H-cleft

Neste capítulo, $(H, \mu, \eta, \Delta, \varepsilon, S)$ denotará sempre uma álgebra de Hopf sobre um anel comutativo com unidade R.

Serão definidos objetos que unem as coálgebras e os H-comódulos. Estes objetos estendem para as álgebras de Hopf a ideia de ação de um grupo finito, motivo pelo qual iniciaremos revendo certos conceitos de ações das álgebras de Hopf em álgebras.

Aqui introduziremos os principais objetos de estudo da nossa pesquisa: As extensões H-cleft e extensões H-Galois. Na primeira seção estudaremos o produto cruzado que será usado em seguida para obter uma caracterização das extensões H-cleft como em [18].

Terminaremos o capítulo com um resultado de Doi e Takeuchi [19] no qual se estabelece que as extensões H-cleft são equivalentes as extensões H-Galois que possuem a propriedade da base normal.

As principais referências para este capítulo são [16] e [38].

3.1 Ações de Álgebras de Hopf em Álgebras

Definição 3.1.1 (H-Módulo álgebra à Esquerda)**.** Seja A uma álgebra. Dizemos que A é um *H-módulo álgebra à esquerda* se valem as seguintes condições:

(MA1) A é um H-módulo à esquerda com ação $\cdot\colon H \otimes A \longrightarrow A$,

(MA2) $x \cdot (ab) = \sum (x_1 \cdot a)(x_2 \cdot b)$,

(MA3) $x \cdot 1_A = \varepsilon(x) 1_A$,

para todo $x \in H$ e $a, b \in A$.

De modo análogo poderíamos definir um H-módulo álgebra à direita. Em geral, omitiremos o termo "à esquerda" na definição anterior.

O lema a seguir é uma tecnicalidade para mostrar que se A tem estrutura de álgebra e de H-comódulo então pedir que μ_A seja um homomorfismo de H-módulos é condição necessária e suficiente para que A seja um H-módulo álgebra.

Lema 3.1.2. *[16, 6.1.3] Seja A uma álgebra e um H-módulo com ação $\cdot : H \otimes A \longrightarrow A$ e que tenha a propriedade (MA2). Então:*

(a) $(x \cdot a)b = \sum x_1 \cdot (a(S(x_2) \cdot b))$,

(b) Se S é bijetora então $a(x \cdot b) = \sum x_2 \cdot ((S^{-1}(x_1) \cdot a)b)$,

para todo $x \in H$ e $a, b \in A$.

Demonstração.

a) De fato,

$$\begin{aligned}
\sum x_1 \cdot (a(S(x_2) \cdot b) &= \sum (x_1 \cdot a)(x_2 \cdot (S(x_3) \cdot b) \\
&= \sum (x_1 \cdot a)(x_2 S(x_3)) \cdot b \\
&= (x_1 \cdot a)(\varepsilon(x_2) 1_H \cdot b) \\
&= \left(\left(\sum x_1 \varepsilon(x_2)\right) \cdot a\right)(1_H \cdot b) \\
&= (x \cdot a)(1_H \cdot b) \\
&= (x \cdot a)b.
\end{aligned}$$

b) Como S é bijetora, então

$$\sum x_2 S^{-1}(x_1) = \sum (S^{-1} \circ S)(x_2) S^{-1}(x_1) = S^{-1}\left(\sum x_1 S(x_2)\right) = \varepsilon(x) 1_H.$$

O restante segue de modo análogo ao item anterior.

■

Proposição 3.1.3. *[16, 6.1.4] Seja A uma álgebra e também um H-módulo com ação $\cdot : H \otimes A \longrightarrow A$. Então A é um H-módulo álgebra se, e somente se, μ_A é um homomorfismo de H-módulos.*

Demonstração. É rotineiro mostrar que o R-módulo $A \otimes A$ é um H-módulo com ação $\rightharpoonup : H \otimes A \otimes A \longrightarrow A \otimes A$ dada por

$$x \rightharpoonup (a \otimes b) = \sum (x_1 \cdot a) \otimes (x_2 \cdot b)$$

para todo $x \in H$ e $a, b \in A$. Note também que a comutatividade do diagrama

$$\begin{array}{ccc} H \otimes A \otimes A & \xrightarrow{\mathrm{id} \otimes \mu} & H \otimes A \\ \downarrow & & \downarrow \\ A \otimes A & \xrightarrow{\mu} & A \end{array}$$

garante que μ é um homomorfismo de H-módulos e que vale (MA2), ou seja as duas afirmações são equivalentes. Com isso, só resta mostrar que, neste caso, podemos deduzir (MA3) de (MA2). Para isso, usaremos o lema anterior com $a = b = 1_A$:

$$\begin{aligned} x \cdot 1_A &= (x \cdot 1_A)1_A \\ &= \sum x_1 \cdot (1_A(S(x_2) \cdot 1_A)) \\ &= \sum x_1 \cdot (S(x_2) \cdot 1_A) \\ &= \left(\sum x_1 S(x_2)\right) \cdot 1_A \\ &= \varepsilon(x)1_A. \end{aligned}$$

■

Seja A um H-módulo álgebra. Considere o conjunto

$$A^H = \{a \in A \mid x \cdot a = \varepsilon(x)a, \text{ para todo } x \in H\}$$

dos elementos de A sobre os quais H age trivialmente.

Proposição 3.1.4. *A^H é uma R-subálgebra de A.*

Demonstração. Só precisamos provar que $x \cdot (ab) = \varepsilon(x)ab$, para todo $x \in H$ e $a, b \in A^H$. De fato,

$$x \cdot (ab) = \sum (x_1 \cdot a)(x_2 \cdot b) = \sum \varepsilon(x_1)a\varepsilon(x_2)b = \sum \varepsilon(x_1\varepsilon(x_2))ab = \varepsilon(x)ab.$$

■

A^H é dita *R-subálgebra de H-invariantes* de A.

Exemplo 3.1.5. H é um H-módulo álgebra com ação $x \cdot y = \sum x_1 y S(x_2)$, para todo $x, y \in H$. Além disso, $H^H = Z(H)$, ou seja, o centro de H.
Já sabemos que H é um H-módulo. A propriedade (MA3) se verifica facilmente.

Verifiquemos(MA2). Para todo $x, y, z \in H$,

$$\begin{aligned}\sum(x_1 \cdot y)(x_2 \cdot z) &= \sum x_1 y S(x_2) x_3 z S(x_4) \\ &= \sum x_1 y \varepsilon(x_2) z S(x_3) \\ &= \sum x_1 y z S(x_2) \\ &= x \cdot (yz)\end{aligned}$$

Logo H é um H-módulo álgebra. Finalmente, $H^H = Z(H)$ pois, se $y \in H^H$, então para todo $x \in H$,

$$xy = \sum x_1 \varepsilon(x_2) y = \sum x_1 y S(x_2) x_3 = \sum (x_1 \cdot y) x_2 = \sum \varepsilon(x_1) y x_2 = yx.$$

Exemplo 3.1.6. H^* (quando existe como álgebra de Hopf) é uma H-módulo álgebra com ação $(x \cdot h^*)(y) = h^*(yx)$, para todo $x, y \in H$ e $h^* \in H^*$.
Já sabemos que H^* é um H-módulo. Verifiquemos (MA3): para todo $x, y \in H$,

$$(x \cdot 1_{H^*})(y) = 1_{H^*}(yx) = \varepsilon(yx) = \varepsilon(y)\varepsilon(x) = \varepsilon(x) 1_{H^*}(y)$$

A propriedade (MA2) se verifica do mesmo modo, pois, para todo $x, y \in H$ e $h, g \in H^*$,

$$\sum (x_1 \cdot h^*)(x_2 \cdot g^*)(y) = \sum h^*(y_1 x_1) g^*(y_2 x_2) = (hg)^*(yx) = (x \cdot (h^* * g^*))(y).$$

Logo H^* é um H-módulo álgebra.

Definição 3.1.7 (Homomorfismo de H-módulo álgebras)**.** Sejam A e B H-módulo álgebras e $f\colon A \longrightarrow B$ linear. Dizemos que f é um *homomorfismo de H-módulo álgebras* se f for um homomorfismo de H-módulos e um homomorfismo de álgebras.

Para o próximo exemplo, será útil recordar a noção de álgebra graduada por um grupo.

Definição 3.1.8 (álgebra G-graduada)**.** Seja G um grupo. Dizemos que A é uma *álgebra G-graduada* se

$$A = \bigoplus_{g \in G} A_g,$$

em que A_g são R-submódulos chamados componentes homogêneas de grau g em A, e tais que, para todo $g, h \in G$, $A_g A_h \subset A_{gh}$.

Se 1_G é o elemento neutro do grupo G, então A_1 é uma R-subálgebra unitária de A contendo os elementos de grau 1 em A. Todo elemento $a \in A$ se expressa unicamente na forma

$$a = \sum_{g \in G} a_g$$

para $a_g \in A_g$ quase todos nulos.

Definição 3.1.9 (Homomorfismo G-graduado de álgebras)**.** Sejam

$$A = \bigoplus_{g\in G} A_g \text{ e } B = \bigoplus_{g\in G} B_g$$

duas álgebras G-graduadas. Dizemos que um homomorfismo de álgebras $\varphi\colon A \longrightarrow B$ é *G-graduado* se $\varphi(A_g) \subset B_g$ para cada $g \in G$.

Exemplo 3.1.10. Seja G um grupo finito e A uma álgebra graduada. Então, A é uma álgebra $(RG)^*$-módulo com a ação

$$\begin{array}{rccc} \cdot\colon & (RG)^* \otimes A & \longrightarrow & A \\ & p_g \otimes a & \longmapsto & a_g. \end{array}$$

Ademais, $A^{(RG)^*} = A_1$, e com isso, A_1 é um $(RG)^*$-submódulo de A.
De fato, A é um $(RG)^*$-módulo com aplicação acima pois, usando os idempotentes do Exemplo 2.4.16 temos que, para todo $p_g, p_h \in (RG)^*$ e para todo $a, b \in A$, a condição (MA1) é satisfeita pois, por um lado,

$$p_g \cdot p_h \cdot a = p_g(a_h) = \begin{cases} a_g, \text{ se } g = h \\ 0, \text{ se } g \neq h \end{cases}$$

e, por outro,

$$(p_g p_h) \cdot a = \begin{cases} p_g \cdot a = a_g, \text{ se } g = h \\ 0 \cdot a = 0, \text{ se } g \neq h. \end{cases}$$

Além disso,

$$1_{(RG)^*} \cdot a = \sum_{g\in G} p_g \cdot a = \sum_{g\in G} a_g = a.$$

A condição (MA2) é satisfeita, pois

$$p_g \cdot (ab) = (ab)_g = \sum_{h\in G} a_h b_{h^{-1}g} = \sum_{h\in G} (p_h \cdot a)(p_{h^{-1}g} \cdot b).$$

A condição (MA3) também, pois

$$p_g \cdot 1_A = \begin{cases} 1_A, \text{ se } g = 1_G \\ 0, \text{ se } g \neq 1_G \end{cases} = \delta_{1_G, g} 1_A = \varepsilon(p_g) 1_A.$$

Finalmente,

$$\begin{aligned} A^{(RG)^*} &= \{a \in A \mid p_g \cdot a = \varepsilon(p_g)a, \text{ para todo } p_g \in (RG)^*\} \\ &= \{a \in A \mid a_g = \delta_{1_G,g}a, \text{ para todo } g \in G\} \\ &= \{a \in A \mid a_{1_G} = a \text{ e } a_g = 0 \text{ para todo } g \in G, g \neq 1_G\} \\ &= A_1. \end{aligned}$$

3.2 Coações de Álgebras de Hopf em Álgebras

Da mesma forma que nos H-módulo álgebras tínhamos uma ação compatível com o produto e com a unidade da álgebra, aqui desejamos uma co-ação que também seja compatível com essas estruturas.

Definição 3.2.1 (H-comódulo álgebra à Direita)**.** Seja H uma álgebra de Hopf e A uma álgebra. Dizemos que A é um *H-comódulo álgebra à direita* se valem as seguintes condições:

(CA1) A é um H-comódulo à direita com coação $\rho\colon A \longrightarrow A \otimes H$, isto é,

$$\rho(a) = \sum a_{(0)} \otimes a_{(1)},$$

(CA2) $\rho(ab) = \rho(a)\rho(b)$, isto é, para todo $a, b \in A$,

$$\sum (ab)_{(0)} \otimes (ab)_{(1)} = \sum a_{(0)}b_{(0)} \otimes a_{(1)}b_{(1)},$$

(CA3) $\rho(1_A) = 1_A \otimes 1_H$.

É comum dizermos que H coage à direita de A por ρ, ou ainda que ρ é uma coação de H à direita em A. Assim como nos H-comódulos, omitiremos o termo "à direita".

De modo análogo, poderíamos definir um H-comódulo álgebra à esquerda.

Note que as condições (CA2) e (CA3) equivalem a pedir que ρ seja um homomorfismo de álgebras.

Dado A um H-comódulo álgebra, seja

$$A^{coH} = \{a \in A \mid \rho(a) = a \otimes 1_H, \text{ para todo } a \in A\}.$$

Em vista de (CA2), A^{coH} é uma subálgebra chamada de *subálgebra de H-coinvariantes* de A.

Exemplo 3.2.2. H é um H-comódulo álgebra. De fato, já sabemos que H é um H-comódulo com Δ, porém, como Δ é homomorfismo de álgebras, obviamente valem (MA2) e (MA3). Além disso, $H^{coH} \cong R$, pois $\varepsilon \otimes \mathrm{id} \circ \Delta(h) = \varepsilon(h)1_A$ para todo $h \in H$.

Lema 3.2.3. *Sejam M e N dois R-módulos em que N é livre com base B e seja $t \in M \otimes N$. Se $(\mathrm{id} \otimes f)(t) = 0$ para todo $f \in N^*$ então $t = 0$.*

Demonstração. Usando a Proposição 1.3, escreva $t = \sum_i m_i \otimes n_i$, com os elementos n_i distintos em B. Considere a família $\{f_i\}$ em N^* dada por $f_i(n_j) = \delta_{ij}$ para todo $n_j \in B$. Então para todo j

$$0 = (\mathrm{id} \otimes f)(t) = \sum_i m_i f_j(n_i) = m_j.$$

■

Proposição 3.2.4. *Seja H uma álgebra de Hopf e A uma álgebra. Se H é um R-módulo livre finitamente gerado então A é um H-comódulo álgebra se, e somente se, A é uma álgebra H^*-módulo. Além disso, $A^{coH} = A^{H^*}$.*

Demonstração. Seja A um H-comódulo álgebra com coação $\rho(a) = \sum a_{(0)} \otimes a_{(1)}$, para todo $a \in A$. Mostremos, primeiramente, que A é um H^*-módulo álgebra com ação

$$\begin{array}{rccc} \cdot : & H \otimes A & \longrightarrow & A \\ & f \otimes a & \longmapsto & \sum a_{(0)} f(a_{(1)}). \end{array}$$

Pela Proposição 2.3.8, $(A, \cdot)$ é um H^*-módulo. Então basta verificar (MA2) e (MA3). Para todo $f \in H^*$ e $a, b \in A$,

$$\begin{aligned} f \cdot (ab) &= \sum (ab)_{(0)} f((ab)_{(1)}) \\ &= \sum a_{(0)} b_{(0)} f(a_{(1)} b_{(1)}) \\ &= \sum a_{(0)} b_{(0)} f(a_{(1)}) f(b_{(1)}) \\ &= \sum a_{(0)} f(a_{(1)}) b_{(0)} f(b_{(1)}) \\ &= \sum (f_1 \cdot a)(f_2 \cdot b) \end{aligned}$$

e

$$f \cdot (1_A) = 1_A f(1_H) = \bar{\varepsilon}(f) 1_A,$$

na qual $\bar{\varepsilon} = \varepsilon^*$ é a counidade de H^*.

Para mostrar a recíproca, como H é livre e finitamente gerado, seja $\{e_i\}$ base de H dada por $e_i^*(e_j) = \delta_{ij}$ [25, 4.11]. Supondo que A seja um H^*-módulo álgebra, mostremos

que A é um H-comódulo álgebra com coação

$$\begin{array}{rccc} \rho\colon & A & \longrightarrow & A\otimes H \\ & a & \longmapsto & \displaystyle\sum_{i=1}^{n}(e_i^*\cdot a)\otimes e_i. \end{array}$$

Não é difícil ver que a aplicação acima é de fato uma coação. Para mostrar (CA2), note que, para todo $f\in H^*$,

$$\begin{aligned} (\mathrm{id}\otimes f)(\rho(ab)) &= \sum_{i=1}^{n} e_i^*\cdot(ab)f(e_i) \\ &= \sum_{i=1}^{n}(e_i^* f(e_i))\cdot(ab) \\ &= f\cdot(ab) \\ &= \sum(f_1\cdot a)(f_2\cdot b) \\ &= \sum_{i,j=1}^{n}((e_i^* f_1(e_i))\cdot a)((e_j^* f_2(e_j))\cdot b) \\ &= \sum_{i,j=1}^{n}(e_i^*\cdot a)(e_j^*\cdot b)f_1(e_i)f_2(e_j) \\ &= \sum_{i,j=1}^{n}(e_i^*\cdot a)(e_j^*\cdot b)f(e_ie_j) \\ &= (\mathrm{id}\otimes f)\left(\sum_{i,j=1}^{n}(e_i^*\cdot a)(e_j^*\cdot b)\otimes e_ie_j\right) \\ &= (\mathrm{id}\otimes f)(\rho(a)\rho(b)). \end{aligned}$$

Logo, pelo Lema 3.2.3, $\rho(ab)=\rho(a)\rho(b)$. A condição (CA3) é dada por

$$\begin{aligned} \rho(1_A) &= \sum_{i=1}^{n}(e_i^*\cdot 1_A)\otimes e_i \\ &= \sum_{i=1}^{n} e_i^*(1_H)1_A\otimes e_i \\ &= 1_A\otimes\left(\sum_{i=1}^{n} e_i^*(1_H)e_i\right) \\ &= 1_A\otimes 1_H. \end{aligned}$$

Por fim,

$$\begin{aligned} A^{H^*} &= \{a \in A \mid f \cdot a = f(1_H)a, \text{ para todo } f \in H^*\} \\ &= \left\{a \in A \;\middle|\; \sum a_{(0)} f(a_{(1)}) = f(1_H)a, \text{ para todo } f \in H^*\right\} \\ &= \{a \in A \mid (\mathrm{id} \otimes f)(\rho(a)) = (\mathrm{id} \otimes f)(a \otimes 1_H), \text{ para todo } f \in H^*\} \\ &= \{a \in A \mid \rho(a) = a \otimes 1_H\} \\ &= A^{coH}. \end{aligned}$$

■

O próximo exemplo mostra que toda álgebra G-graduada pode ser vista como um RG-comódulo álgebra.

Exemplo 3.2.5. Seja G um grupo arbitrário e $A = \bigoplus_{g \in G} A_g$ uma álgebra G-graduada. Denote

$$a = \sum_{g \in G} a_g \in \bigoplus_{g \in G} A_g.$$

Então A é um RG-comódulo álgebra com coação

$$\begin{array}{rccc} \rho\colon & A & \longrightarrow & A \otimes RG \\ & a & \longmapsto & \displaystyle\sum_{g \in G} a_g \otimes g. \end{array}$$

Além disso, $A^{co(RG)} = A_1$.

De fato, A é um RG-comódulo com a coação acima pois, para todo $a, b \in A$ e $g, h \in G$,

$$\begin{aligned} (\rho \otimes \mathrm{id}) \circ \rho(a) &= (\rho \otimes \mathrm{id}) \left(\sum_{g \in G} a_g \otimes g \right) \\ &= \sum_{g \in G} a_g \otimes g \otimes g \\ &= (\mathrm{id} \otimes \Delta) \left(\sum_{g \in G} a_g \otimes g \right) \\ &= (\mathrm{id} \otimes \Delta) \circ \rho(a). \end{aligned}$$

Além disso,

$$(\mathrm{id} \otimes \varepsilon) \circ \rho(a) = \sum_{g \in G} \varepsilon(g) a_g = \sum_{g \in G} a_g = a,$$

o que conclui a verificação de (CA1). A verificação de (CA2) é dada por

$$\begin{aligned}\rho(ab) &= \sum_{g\in G}(ab)_g \otimes g \\ &= \sum_{g\in G}\sum_{h\in H} a_{gh^{-1}}b_h \otimes g \\ &= \sum_{g\in G}\sum_{h\in H} a_{gh^{-1}}b_h \otimes gh^{-1}h \\ &= \sum_{g\in G}\sum_{h\in H} (a_{gh^{-1}} \otimes gh^{-1})(b_h \otimes h) \\ &= \rho(a)\rho(b).\end{aligned}$$

A condição (CA3) é imediata. Além disso, $A^{co(RG)} = A_{1_G}$ pois dado $e_1(g) = \delta_{1,g}$, para todo $g \in G$, $a \in A^{co(RG)}$ se e somente se

$$a = (\mathrm{id} \otimes e_1)(a \otimes 1_G) = (\mathrm{id} \otimes e_1)(\rho(a)) = \sum_{g\in G} e_1(g)a_g = a_{1_G} \in A_{1_G}.$$

Note que, quando tratamos de H-módulos, no Exemplo 3.1.10 para a construção fazer sentido, G precisava ser um grupo finito para que uma álgebra G-graduada A fosse um $(RG)^*$-módulo álgebra, porém, neste exemplo, o grupo G pode ser arbitrário.

Definição 3.2.6 (Homomorfismo de H-comódulo álgebras)**.** Sejam A e B H-comódulo álgebras e $f\colon A \longrightarrow B$ linear. f é um *homomorfismo de H-comódulo álgebras* se for um homomorfismo de H-comódulos e um homomorfismo de álgebras simultaneamente.

3.3 O Produto Cruzado

Seja A um H-comódulo álgebra. A ideia do produto cruzado é deformar o produto usual de $A \otimes H$, porém preservando a unidade. Essa noção será útil na próxima seção para se obter uma caracterização conveniente das extensões H-cleft. Tal deformação é feita usando uma generalização de 2-cociclos:

Definição 3.3.1 (2-cociclo generalizado)**.** Sejam H uma álgebra de Hopf e A uma álgebra. Seja $\alpha\colon H \otimes H \longrightarrow A$ uma aplicação linear invertível por convolução. Dizemos que α é um 2-*cociclo generalizado normalizado à esquerda para* H se satisfizer

1. Condição de cociclo:

$$\sum \alpha(y_1, z_1)\alpha(x, y_2z_2) = \sum \alpha(x_1, y_1)\alpha(x_2y_2, z),$$

2. Condição de normalização:

$$\alpha(1_H, x) = \alpha(x, 1_H) = \varepsilon(x),$$

para todo $x, y, z \in H$ e $a \in A$.

Note que esta noção de 2-cociclo coincide com a usual sobre elementos grouplike de H. Em particular, se $H = RG$, como para todo $g \in G$, g é grouplike, então um 2-cociclo generalizado fica completamente definido por um 2-cociclo $\sigma \in Z^2(G, R^\times)$.

A menos que se diga o contrário, usaremos 2-cociclos generalizados normalizados à esquerda. Por isso, a partir de agora, o termo "α um 2-cociclo generalizado" se refere a "α um 2-cociclo generalizado normalizado à esquerda".

Vale mencionar que é possível interpretar a condição de cociclo em termos do produto de convolução em $\mathrm{Hom}_R(H \otimes H \otimes H, R)$ da seguinte forma:

$$(\varepsilon \otimes \alpha) * (\alpha \circ (\mathrm{id} \otimes \mu)) = (\alpha \otimes \varepsilon) * (\alpha \circ (\mu \otimes \mathrm{id})).$$

Seja A uma álgebra. Se uma aplicação linear $\rightharpoonup \colon H \otimes A \longrightarrow A$ satisfaz as propriedades (MA2) e (MA3) da Definição 3.1.1 dizemos que H *mede* A por $\rightharpoonup$.

Definição 3.3.2 (Produto cruzado)**.** Sejam H uma álgebra de Hopf e A uma álgebra. Suponha que H mede A por $\rightharpoonup$ e que $\alpha \colon H \otimes H \longrightarrow A$ seja invertível por convolução. O *produto cruzado* $A\#_\alpha H$ *de* A *com* H é o R-módulo $A \otimes H$ com multiplicação

$$(a\#x)(b\#y) = \sum a(x_1 \rightharpoonup b)\alpha(x_2, y_1)\#x_3y_2$$

para todo $x, y \in H$ e $a, b \in A$, em que estamos denotando por $a\#x$ o tensor $a \otimes x$.

Lema 3.3.3. *[18, 10] O produto cruzado $A\#_\alpha H$ é uma álgebra associativa com unidade $1_A\#1_H$ se e somente se as seguintes condições são satisfeitas:*

1. *α é um 2-cociclo generalizado,*
2. *$1 \rightharpoonup a = a$ para todo $a \in A$ e*

$$\sum (x_1 \rightharpoonup (y_1 \rightharpoonup a))\alpha(x_2, y_2) = \sum \alpha(x_1, y_1)((x_2y_2) \rightharpoonup a).$$

para todo $x, y \in H$ e $a \in A$.

É importante ter em mente que $\rightharpoonup$ não precisa satisfazer a condição (MA1), isto é, não é necessário que A seja um H-módulo. De fato, antes pensava-se que essa condição fosse essencial (como em [14]), porém mais tarde em [19] verificou-se não ser este o caso.

Se o 2-cociclo generalizado α for trivial, isto é, se $\alpha(x,y) = \varepsilon(x)\varepsilon(y)1_A$, para todo $x, y, \in H$ então, pela condição (2.) do Lema 3.3.3, A será um H-módulo. Neste caso, o produto cruzado assume esta forma mais simples:

$$(a\#x)(b\#y) = \sum a(x_1 \rightharpoonup b)\#x_2y$$

para todo $x, y \in H$ e $a, b \in A$ e o produto cruzado passa a ser chamado de *produto smash*, denotado simplesmente por $A\#H$.

Por outro lado, se $\rightharpoonup$ for uma ação trivial, isto é, $x \rightharpoonup a = \varepsilon(x)a$, então o produto cruzado assume esta outra forma:

$$(a\#x)(b\#y) = \sum ab\alpha(x_1, y_1)\#x_2y_2$$

para todo $a, b \in A$ e $x, y \in H$. Este é chamado de *produto torcido*, denotado por $A_\alpha H$.

Quando $A = R$, $\rightharpoonup$ fica totalmente definido por (MA3), ou seja por $x \rightharpoonup 1 = \varepsilon(x)1$, para todo $x \in H$. Portanto, o produto cruzado é um produto torcido $R_\alpha H$. Devido ao isomorfismo de H-comódulos $R \otimes H \cong H$, o produto torcido $R_\alpha H$ fica bem definido pela fórmula

$$(1\#x)(1\#y) = \sum \alpha(x_1, y_1)\#x_2y_2.$$

Assim, se denotarmos os elementos $1\#x$ por v_x, para todo $x \in H$ e observarmos que $\alpha(x, y) \subseteq R$ para todo $x, y \in H$, então podemos reescrever a fórmula acima da seguinte forma:

$$v_x v_y = \sum \alpha(x_1, y_1)v_{x_2y_2}. \tag{3.1}$$

Nese caso, denotaremos $R_\alpha H$ simplesmente por ${}_\alpha H$.

Obviamente que ${}_\alpha H$ generaliza a noção de álgebra de grupo torcida $R^\sigma G$, com G um grupo, $\sigma\colon G \times G \longrightarrow R^\times$ uma aplicação bilinear e $R^\sigma G$ o R-módulo livre gerado pelos símbolos $v_g (g \in G)$ e multiplicação determinada por $v_g v_h = \sigma(g, h)v_{gh}$, para todo $g, h \in G$. Esta estrutura é associativa e unitária se e somente se σ é um 2-cociclo normalizado.

3.4 Extensões H-cleft

O objetivo desta seção é definir e dar alguma intuição acerca das extensões H-cleft. Para isso, convém iniciarmos com a noção de H-extensão.

Definição 3.4.1 (H-extensão)**.** Sejam A e B álgebras, com A subálgebra de B e H uma álgebra de Hopf. Dizemos que $A \subset B$ é uma *H-extensão (à direita)* se B for um H-comódulo álgebra com $B^{coH} = A$.

Dentre as H-extensões interessam-nos de maneira especial aquelas que se chamam extensões H-cleft:

Definição 3.4.2. Seja A uma álgebra. Uma H-extensão $A \subset B$ é uma *extensão H-cleft sobre A* se existe um homomorfismo de H-comódulos $\gamma\colon H \longrightarrow B$ invertível por convolução, isto é, se existe um homomorfismo de H-comódulos $\gamma^{-1}\colon H \longrightarrow B$ tal que

$$\gamma * \gamma^{-1} := \mu_B \circ \gamma \otimes \gamma^{-1} \circ \Delta_H = \eta_B \circ \varepsilon_H.$$

Nesta definição, podemos sempre assumir que $\gamma(1_H) = 1_B$, bastando substituir γ por $\gamma' = \gamma(1_H)^{-1}\gamma$, se necessário.

Dizemos que tal aplicação γ é uma *seção* e que o par (B, γ) é um *sistema cleft*.

Como um primeiro exemplo de extensão H-cleft, note que do fato da $\mathrm{id}\colon H \longrightarrow H$ ser invertível por convolução (com inversa S) e de $H^{coH} = R$, temos que $R \subset H$ é uma extensão H-cleft.

Em 1986 Doi e Takeuchi mostraram em [19] que toda extensão H-cleft $A \subset B$ é isomorfa a um produto cruzado $A\#_\alpha H$ para certos α e $\rightharpoonup$.

Teorema 3.4.3. *[19, 11] Seja $A \subset B$ uma extensão H-cleft com seção $\gamma\colon H \longrightarrow B$. Então existe uma ação de H em A dada por*

$$x \rightharpoonup a = \sum \gamma(x_1) a \gamma^{-1}(x_2) \tag{3.2}$$

para todo $x \in H$ e $a \in A$, e um 2-cociclo generalizado $\alpha\colon H \otimes H \longrightarrow A$ dado por

$$\alpha(x, y) = \sum \gamma(x_1)\gamma(y_1)\gamma^{-1}(x_2 y_2), \tag{3.3}$$

para todo $x, y \in H$, tal que $A\#_\alpha H$ é um produto cruzado. Além disso, a aplicação $\Phi\colon A\#_\alpha H \longrightarrow B$ dada por $\Phi(a\#x) = a\gamma(x)$ é um isomorfismo de álgebras e de A-módulos. Mais ainda, Φ é um isomorfismo de H-comódulo álgebras com $A\#_\alpha H$ é um H-comódulo via

$$a\#x \mapsto \sum a\#x_1 \otimes x_2.$$

Esboço da prova. Para mostrar que (3.2) é uma ação a parte mais delicada é mostrar que $h \cdot a \in A$. Para isso, mostra-se que $\rho \circ \gamma^{-1} = (\gamma^{-1} \otimes S) \circ \tau \circ \Delta$. Com isso, é possível ver que, para todo $a \in A$ e $b \in B$, $\rho(a \cdot b) = (a. \cdot b) \otimes 1$. Logo $a \cdot b \in B^{coH} = A$.

Para mostrar que (3.3) é um 2-cociclo generalizado, a parte mais delicada é mostrar que, para todo $h, k \in H$, $\sigma(h, k) \in A$. Para isso, mostra-se que para todo $h, k \in H$, $\rho(\sigma(h, k)) = (\sigma(h, k)) \otimes 1$. Logo $\sigma(h, k) \in B^{coH} = A$.

Verificar que Φ é um homomorfismo de A-módulos, de álgebras e de H-comódulos envolve algumas contas, mas é rotineiro. Para mostrar que Φ é bijetora, defina a

aplicação $\Psi\colon B \longrightarrow A\#_\alpha H$ por

$$\Psi(b) = \sum b_{(0)}\gamma^{-1}(b_{(1)})\#b_{(2)}.$$

e mostre que Ψ é a inversa de Φ. ■

Por outro lado, em 1989 Doi mostrou em [18] que todo produto cruzado $A\#_\alpha H$ é uma extensão H-cleft.

Teorema 3.4.4. *[18, 1.1] Seja $A\#_\alpha H$ um produto cruzado e defina $\gamma\colon H \longrightarrow A\#_\alpha H$ por $\gamma(x) = 1\#x$, para todo $x \in H$. Então γ é invertível por convolução com inversa*

$$\gamma^{-1}(x) = \sum \alpha^{-1}(Sx_2, x_3)\#Sx_1,$$

para todo $x \in H$. Em particular, $A\#_\alpha H$ é uma extensão H-cleft.

Portanto:

Corolário 3.4.5. *Seja $A \subset B$ uma H-extensão. $A \subset B$ é H-cleft se e somente se $B \cong A\#_\alpha H$. Em particular, $R \subset B$ é H-cleft se e somente se $B \cong {}_\alpha H$.*

3.5 Extensões H-Galois

Ainda que nosso principal objeto de estudo sejam as extensões H-cleft, não podemos deixar de falar das extensões H-Galois e de como esses dois tipos de H-extensão se relacionam.

Definição 3.5.1 (Extensão H-Galois)**.** Seja $A \subset B$ uma H-extensão com coação dada por $\rho\colon B \longrightarrow B \otimes H$. Dizemos que $A \subset B$ é uma *extensão H-Galois (à direita)* se a aplicação linear

$$\begin{array}{rccc} \beta\colon & B \otimes_A B & \longrightarrow & B \otimes H \\ & a \otimes b & \longmapsto & (a \otimes 1_H)\rho(b) \end{array}$$

é biunívoca. Se $A = R$ diremos que B é um *objeto H-Galois*.

Quando A é uma extensão H-Galois, β é dita aplicação canônica de A.

Usar o nome extensão H-Galois com certeza remete o leitor às extensões de corpos da teoria de Galois. De fato, trata-se de uma generalização, como mostra o seguinte exemplo:

Exemplo 3.5.2. [16, 6.4.3] Seja G um grupo finito agindo por automorfismos sobre um corpo $E \supset k$ e $F = E^G$ (elementos do corpo E fixados por G). Então E/F é uma extensão de Galois no sentido clássico se e somente se $E \subset F$ é uma extensão $(kG)^*$-Galois.

Porém, nem toda extensão H-Galois precisa ser uma extensão de corpos da teoria de Galois no sentido clássico. Um exemplo pode ser encontrado em [38, 8.1.5].

O próximo exemplo mostra que a própria álgebra de Hopf é um objeto H-Galois.

Exemplo 3.5.3. $R \subset H$ é um objeto H-Galois com

$$\begin{array}{rccc} \beta\colon & H \otimes H & \longrightarrow & H \otimes H \\ & x \otimes y & \longmapsto & \sum xy_1 \otimes y_2 \end{array}$$

e inversa

$$\begin{array}{rccc} \beta^{-1}\colon & H \otimes H & \longrightarrow & H \otimes H \\ & x \otimes y & \longmapsto & \sum xS(y_1) \otimes y_2. \end{array}$$

Seja G um grupo e A uma álgebra G-graduada. Pelo Exemplo 3.2.5, A é um RG-comódulo álgebra e $A^{coH} = A_1$. O seguinte resultado de Ulbrich descreve quando estas RG-extensões são objetos RG-Galois:

Teorema 3.5.4. *[46] $A_1 \subset A$ é RG-Galois se e somente se A é fortemente G-graduada, isto é, A é G-graduada e $A_gA_h = A_{gh}$ para todo $g, h \in G$.*

No contexto de teoria de Galois existe um teorema clássico chamado teorema da base normal que diz que se $F \subset E$ é uma extensão de Galois finita de corpos com grupo de Galois G, então E/F tem base normal, isto é, existe $a \in E$ tal que $\{x \cdot a \mid x \in G\}$ é uma base para E sobre F.

Definição 3.5.5. Uma H-extensão $A \subset B$ tem a *propriedade de base normal (à direita)* se $B \cong A \otimes H$ como A-módulos e como H-comódulos.

A definição acima estende o conceito de base normal. Se H for uma álgebra de Hopf sobre um corpo e $\dim_k H < \infty$ então a definição acima coincide com o conceito de base normal clássico, como pode ser visto em [38, 8.2.2]

Segue a caracterização das extensões H-Galois feita por Doi e Takeuchi em [19] combinado com o Corolário 3.4.5.

Teorema 3.5.6. *[19, 9] Seja $A \subset B$ uma H-extensão. São equivalentes:*

1. *$A \subset B$ é uma extensão H-cleft,*
2. *$A \subset B$ é uma extensão H-Galois com a propriedade de base normal,*
3. *$B \cong A\#_\alpha H$.*

$$f'(p) = 0 \text{ e } f''(p) > 0$$

Existem situações nas quais toda extensão H-Galois é H-cleft:

Proposição 3.5.7. *[33] Seja H uma álgebra de Hopf sobre um corpo k. Se $\dim_k(H) < \infty$ então todo objeto H-Galois $k \subset B$ é uma extensão H-cleft.*

Isto também ocorre quando H é um tipo de álgebra de Hopf sobre k chamada pontuada, mas tais álgebras de Hopf fogem do escopo deste trabalho. Para uma abordagem introdutória às álgebras de Hopf pontuadas veja [40].

Capítulo 4

H-Identidades Polinomiais

4.1 Identidades Polinomiais

Esta seção apresenta alguns conceitos básicos da PI-teoria e serve de subsídio para as seções seguintes.

Definição 4.1.1 (Identidade Polinomial)**.** Seja $R\langle X\rangle$ a álgebra associativa livre com $X = \{x_i \mid i \in \mathbb{N}\}$ um conjunto de variáveis. Um polinômio $f(x_1, x_2, \ldots, x_n) \in R\langle X\rangle$ é uma *identidade polinomial* para A quando f está no núcleo de todo homomorfismo de álgebras $\omega\colon R\langle X\rangle \longrightarrow A$.

Denote por $\mathrm{Id}(A)$ o conjunto de todas as identidades polinomiais para uma álgebra A. Então

$$\mathrm{Id}(A) = \bigcap_{\omega\colon R\langle X\rangle \longrightarrow A} \ker(\omega)$$

com ω homomorfismo de álgebras.

Evidentemente $\mathrm{Id}(A)$ é um ideal de $R\langle X\rangle$.

Definição 4.1.2. Seja A uma álgebra. Dizemos que A é uma *PI-álgebra (álgebra com identidade polinomial)* se $\mathrm{Id}(A) \neq \{0\}$.

Exemplo 4.1.3. Toda álgebra comutativa é uma PI-álgebra, dado que o polinômio $f(x, y) = xy - yx \in R\langle X\rangle$ é obviamente uma identidade polinomial para A.

Um polinômio clássico na PI-teoria é o chamado polinômio standard de grau d, definido da seguinte forma: Sejam S_d o grupo de permutações do conjunto $\{1, \ldots, d\}$

e $\mathrm{sgn}(\mathfrak{s})$ o sinal da permutação $\mathfrak{s}$ então

$$S_d(x_1, \ldots, x_d) = \sum_{\mathfrak{s} \in S_d} \mathrm{sgn}(\mathfrak{s}) x_{\mathfrak{s}(1)} \ldots x_{\mathfrak{s}(d)}$$

é o polinômio *standard* de grau d. Usando este polinômio, é possível mostrar que dada uma álgebra A com $\dim_k(A) < d$ então $S_d(x_1, \ldots, x_d)$ é uma identidade polinomial para A, ou seja, toda álgebra de dimensão finita é uma PI-álgebra.

Definição 4.1.4 (T-ideal)**.** Dizemos que um ideal B de uma álgebra A é um T-ideal se $f(B) \subseteq B$, para todo endomorfismo de álgebras $f\colon A \longrightarrow A$.

Note que $\mathrm{Id}(A)$ é um T-ideal de $R\langle X\rangle$. Além disso, todo T-ideal I de $R\langle X\rangle$ é do tipo $\mathrm{Id}(A)$ para alguma álgebra A. Para isso, basta tomar $A = R\langle X\rangle/I$.

Com isso, fica claro que toda álgebra determina um T-ideal, a saber, $\mathrm{Id}(A)$. Porém, é possível que álgebras distintas A e B determinem o mesmo T-ideal, isto é, $\mathrm{Id}(A) = \mathrm{Id}(B)$. É natural que surja a seguinte questão: Sejam A e B duas álgebras. Se $\mathrm{Id}(A) = \mathrm{Id}(B)$ será que $A \cong B$ como álgebras? Este é conhecido como o *problema do isomorfismo para identidades polinomiais*. No caso de uma resposta afirmativa para esta questão, dizemos que as identidades polinomiais *determinam* as álgebras (a menos de isomorfismo).

O presente trabalho é motivado pela busca de uma resposta para esta questão quando as álgebras A e B possuem estrutura adicional, a saber, são H-comódulo álgebras. Mais especificamente, extensões H-cleft para uma certa álgebra de Hopf H. Na PI-teoria, é comum que se considerem identidades polinomiais de álgebras graduadas, com involução, ou com ambas as condições, em cujos casos as identidades polinomiais correspondentes são definidas de acordo com, e recebem a respectiva denominação da estrutura extra a que se referem, a fim de distingui-las das identidades polinomiais ordinárias. Embora tais estruturas tenham sido bem estudadas, parece-nos que o estudo das questões envolvendo as identidades polinomiais dos H-comódulo álgebras, e particularmente das extensões H-cleft, seja ainda incipiente. Tanto mais, quando se permite deixar o caminho, bem batido das estruturas sobre corpos, para percorrer o das estruturas sobre anéis comutativos.

Seja G um grupo e $\{X_g \mid g \in G\}$ uma família de conjuntos disjuntos de variáveis indexados por G, e considere

$$X = \bigcup_{g \in G} X_g.$$

Seja $R\langle X\rangle_g$ o subespaço da álgebra associativa livre $R\langle X\rangle$ gerada por monômios $m = x_1^{(g_1)} \ldots x_p^{(g_p)}$ tais que $x_i^{(g_i)} \in X$ e $g_1 \cdots g_p = g$.

É possível mostrar que

$$R\langle X\rangle = \bigoplus_{g\in G} R\langle X\rangle_g \qquad \text{e} \qquad R\langle X\rangle_g R\langle X\rangle_h \subseteq R\langle X\rangle_{gh}$$

para todo $g, h \in G$, isto é, $R\langle X\rangle$ é uma álgebra G-graduada. Se $f \in R\langle X\rangle_g$ dizemos que f tem grau g e denotamos $\deg(f) = g$. Os elementos não nulos de $R\langle X\rangle_g$ são chamados *polinômios homogêneos de grau g* .

Definição 4.1.5 (Identidade Polinomial G-graduada)**.** Seja A uma álgebra G-graduada. Então um polinômio $f(x_1, x_2, \ldots, x_n) \in R\langle X\rangle$ é uma *identidade polinomial G-graduada* para A quando f está no núcleo de todo homomorfismo de álgebras G-graduadas $\omega\colon R\langle X\rangle \longrightarrow A$.

Denote por $\mathrm{Id}_G(A)$ o conjunto de identidades polinomiais G-graduadas para uma álgebra A. É fácil mostrar que $\mathrm{Id}_G(A) \supseteq \mathrm{Id}(A)$ em $R\langle X\rangle$.

Definição 4.1.6 (PI-álgebra graduada)**.** Seja A uma álgebra G-graduada. Dizemos que A é uma *PI-álgebra graduada (álgebra com identidade polinomial graduada)* se existir $f \in \mathrm{Id}_G(A)$ tal que $f \neq 0$.

Com isso, certamente, faz sentido o *problema do isomorfismo para as PI-álgebras graduadas*: Sejam A e B duas álgebras G-graduadas. Se $\mathrm{Id}_G(A) = \mathrm{Id}_G(B)$ então $A \cong B$ como álgebras G-graduadas?

Como dissemos, estamos interessados no problema do isomorfismo para os H-comódulo álgebras, particularmente as extensões H-cleft, tema da próxima seção.

4.2 H-Identidades Polinomiais

O objetivo principal desta seção é definir um conceito de identidade polinomial para os H-comódulo álgebras que seja análogo e que generalize o das identidades ordinárias e graduadas.

A principal referência para essa seção e também para a próxima é o artigo [31]. De início, desejamos introduzir substitutos convenientes para as variáveis da teoria de PI-álgebras, de maneira a construir as H-identidades polinomiais. Esperamos que os motivos de fazê-lo fiquem claros na discussão que se segue.

Seja H uma álgebra de Hopf e A um H-comódulo álgebra com $\rho\colon A \longrightarrow A \otimes H$ a coação de H em A.

Para cada $i \geq 1$ considere $Z_i^H = \{Z_i^x \mid x \in H\}$ uma cópia de H como R-módulo. Obviamente, a aplicação $x \mapsto Z_i^x$ $(x \in H)$ define um isomorfismo de R-módulos entre

H e Z_i^H. Em particular, note que $x + rx' \mapsto Z_i^{x+rx'} = Z_i^x + rZ_i^{x'}$, para todo $x, x' \in H$ e $r \in R$. Os elementos Z_i^x de Z_i^H serão chamados de Z-símbolos.

Considere então a soma direta das cópias de H:

$$Z_H = \bigoplus_{i \geq 1} Z_i^H$$

e seja T a álgebra tensorial sobre Z_H

$$T = T(Z_H) = \bigoplus_{n \geq 0} Z_H^{\otimes n}.$$

Se H for um R-módulo livre, então a Proposição 1.14 garante que $T \cong R\langle I \rangle$ (como álgebras) no qual I é um conjunto de índices para uma base de Z_H. Assim, fixando uma base B de H podemos usar $C = \{Z_i^x \mid x \in B, i \geq 1\}$ como I. Isso nos permite interpretar os Z-símbolos Z_i^x como variáveis nas quais podemos expressar polinômios. A principal vantagem dessa abordagem é poder usar a propriedade universal dos R-módulos livres, ou seja, para todo R-módulo M e para toda aplicação $f \colon C \longrightarrow M$, existe única aplicação linear $F \colon Z_H \longrightarrow M$ tal que $F(Z_i^x) = f(Z_i^x)$ $(x \in C)$. Por ora, não estamos impondo restrição a H, porém, devido a isso, mais adiante pediremos que H seja livre como R-módulo.

Proposição 4.2.1. *Z_H é um H-comódulo e T é um H-comódulo álgebra.*

Demonstração. Cada Z_i^H é obviamente um H-comódulo com $\rho_i \colon Z_i^H \longrightarrow Z_i^H \otimes H$ a coação dada por $\rho_i(Z_i^x) = \sum Z_i^{x_1} \otimes x_2$. A propriedade universal da soma direta de R-módulos nos dá uma única aplicação linear $\rho_{Z_H} \colon Z_H \longrightarrow Z_H \otimes H$ tal que

$$\rho_{Z_H}(Z_i^x) = \rho_i(Z_i^x) = \sum Z_i^{x_1} \otimes x_2,$$

para todo $x \in H$ e $i \geq 1$.

A aplicação ρ_{Z_H} é uma coação. De fato,

$$\begin{aligned}
(\mathrm{id} \otimes \Delta) \circ \rho_{Z_H}(Z_i^x) &= \sum Z_i^{x_1} \otimes \Delta(x_2) \\
&= \sum Z_i^{x_1} \otimes x_2 \otimes x_3 \\
&= (\rho_{Z_H} \otimes \mathrm{id}) \left(\sum Z_i^{x_1} \otimes x_2 \right) \\
&= (\rho_{Z_H} \otimes \mathrm{id}) \circ \rho_{Z_H}(Z_i^x)
\end{aligned}$$

para todo $x \in H$ e $i \geq 1$.

Do mesmo modo,

$$\begin{aligned}(\mathrm{id}\otimes\varepsilon)\circ\rho_{Z_H}(Z_i^x) &= \sum Z_i^{x_1}\varepsilon(x_2)\\ &= \sum Z_i^{x_1}\varepsilon(x_2)\\ &= Z_i^x\end{aligned}$$

para todo $x \in H$ e $i \geq 1$.

Pela propriedade universal da álgebra tensorial, existe um único homomorfismo de álgebras $\rho_T\colon T \longrightarrow T\otimes H$ tal que $\rho_T(Z_i^x) = \sum Z_i^{x_1}\otimes x_2$ para todo $x \in H$ e $i \geq 1$. Dado que ρ_T satisfaz as três condições da Definição 3.2.1 sobre um conjunto de geradores de T como álgebra, resulta que T é um H-comódulo álgebra. ■

Definição 4.2.2 (H-Identidade Polinomial)**.** Dizemos que $P \in T$, é uma *H-identidade polinomial* para o H-comódulo álgebra A se $\omega(P) = 0$ para todo homomorfismo de H-comódulo álgebras $\omega\colon T \longrightarrow A$.

Denote por $\mathrm{Id}_H(A)$ o conjunto de todas as H-identidades polinomiais para um H-comódulo álgebra A e

$$\mathrm{Id}_H(A) = \bigcap_{\omega}\ker(\omega),$$

com $\omega\colon T \longrightarrow A$ homomorfismo de H-comódulo álgebras.

Sendo $X = \{x_i \mid i \geq 1\}$, pela propriedade universal de $R\langle X\rangle$, a função $x_i \mapsto Z_i^1$ de X em T se estende a um único homomorfismo de álgebras de $R\langle X\rangle$ em T, claramente injetor. Desse modo, pode-se identificar $R\langle X\rangle$ com a sua imagem, uma subálgebra unitária de T. Nesse caso, $\rho(x_i) = \rho(Z_i^{1_H}) = Z_i^{1_h}\otimes 1_H = x_i\otimes 1_H$ e $R\langle X\rangle$ é subálgebra de T^{coH}. Como todo homomorfismo de H-comódulo álgebras é, em particular um homomorfismo de álgebras, se $f \in \mathrm{Id}(A)$, então $\omega(f) = 0$ para todo $\omega\colon T \longrightarrow A$ homomorfismo de H-comódulo álgebras. Logo $\mathrm{Id}(A) \subseteq \mathrm{Id}_H(A)$.

Sendo interseção de ideais de T, obviamente $\mathrm{Id}_H(A)$ é um ideal de T. Ademais, como a composição de homomorfismos de H-comódulos ainda é um homomorfismo de H-comódulos, está claro que $\mathrm{Id}_H(A)$ está fechado para endomorfismos de H-comódulo álgebras de T, logo $\mathrm{Id}_H(A)$ é um T-ideal.

Exemplo 4.2.3. Seja $H = R$. Claro que um R-comódulo álgebra A é simplesmente uma álgebra e $T \cong R\langle\{Z_1^1, Z_2^1, \ldots\}\rangle$. Logo todo elemento P de T é um polinômio nas variáveis não comutativas $Z_i^1 \equiv X_i$ com $i \geq 1$. Além disso, os homomorfismos de R-módulo álgebras são simplesmente homomorfismos de álgebras. Dessa forma P é uma H-identidade polinomial para A se, e somente se, P é uma identidade polinomial ordinária para A. Pelo comentário precedente, está claro que, neste caso, $\mathrm{Id}_H(A) = \mathrm{Id}(A)$, ou seja, as H-identidades coincidem com as identidades ordinárias.

Para mostrar que H-identidades polinomiais generalizam as identidades polinomiais G-graduadas usaremos o seguinte lema adaptado de [38]:

Lema 4.2.4. *Sejam G um grupo, $H = RG$, A uma álgebra G-graduada e $\omega\colon T \longrightarrow A$ um homomorfismo de álgebras. Então ω é um homomorfismo de RG-comódulos se, e somente se, $\omega(Z_i^g) \in A_g$ para todo $g \in G$.*

Demonstração. Sejam ρ e ρ_T as coações que tornam, respectivamente, A e T RG-comódulo álgebras:

$$\begin{array}{rccc} \rho\colon & A & \longrightarrow & A \otimes H \\ & a & \longmapsto & \displaystyle\sum_{g\in G} a_g \otimes g \end{array} \qquad \begin{array}{rccc} \rho_T\colon & T & \longrightarrow & T \otimes H \\ & Z_i^g & \longmapsto & Z_i^g \otimes g \end{array}$$

Suponha que $\omega\colon T \longrightarrow A$ é um homomorfismo de RG-comódulo álgebras. Para cada $g \in G$ fixe $a = \omega(Z_i^g)$. Então

$$\begin{aligned} a \otimes g &= (\omega \otimes \mathrm{id})(Z_i^g \otimes g) \\ &= (\omega \otimes \mathrm{id}) \circ \rho_T(Z_i^g) \\ &= (\rho \circ \omega)(Z_i^g) \\ &= \rho(a) \\ &= \sum_{h\in G} a_h \otimes h. \end{aligned}$$

Ou seja,

$$0 = a \otimes g - \sum_{h\in G} a_h \otimes h = (a - a_g) \otimes g - \sum_{\substack{h\in G \\ h\neq g}} a_h \otimes h.$$

Como $\{g\} \cup \{h \in G, h \neq g\}$ são todos distintos, temos que $(a - a_g) = a_h = 0$ para todo $h \in G, h \neq g$, ou seja, $a = a_g$ e $a_h = 0$, para todo $h \neq g$. Portanto

$$\omega(Z_i^g) = a = \sum_{h\in H} a_h = a_g \in A_g$$

para cada $g \in G$.

Por outro lado, supondo que $\omega(Z_i^g) \in A_g$ para todo $g \in G$, temos

$$\begin{aligned} (\rho \circ \omega)(Z_i^g) &= \rho(a_g) \\ &= a_g \otimes g \\ &= \omega(Z_i^g) \otimes g \\ &= (\omega \otimes \mathrm{id})(Z_i^g \otimes g) \\ &= (\omega \otimes \mathrm{id}) \circ \rho_T(Z_i^g). \end{aligned}$$

Ou seja, ω é um homomorfismo de RG-comódulos e portanto de RG-comódulo álgebras. ■

Como feito para $R\langle X\rangle$, é possível identificar $R\langle X\rangle_G$ com uma subálgebra de T. Disso e do lema anterior segue que:

Proposição 4.2.5. *Seja G um grupo. Então P é uma RG-identidade polinomial para um RG-comódulo álgebra A se, e somente se, P é uma identidade G-graduada para a álgebra G-graduada A. Ou seja,*

$$\mathrm{Id}_G(A) = \mathrm{Id}_{RG}(A).$$

O resultado a seguir garante que dois H-comódulo álgebras isomorfos têm as mesmas H-identidades polinomiais.

Proposição 4.2.6. *Seja A um H-comódulo álgebra. Se $f\colon A \longrightarrow B$ é um homomorfismo de H-comódulo álgebras injetor então $\mathrm{Id}_H(B) \subseteq \mathrm{Id}_H(A)$. Em particular, se f for um isomorfismo então $\mathrm{Id}_H(A) = \mathrm{Id}_H(B)$.*

Demonstração. Sejam $P \in I_H(B)$ e $\omega\colon T \longrightarrow A$ um homomorfismo de H-comódulo álgebras qualquer. Por hipótese, para todo $\alpha\colon T \longrightarrow B$ homomorfismo de H-comódulo álgebras, temos que $\alpha(P) = 0$, em particular $f\circ\omega(P) = 0$. Como f é injetora, $\omega(P) = 0$ (para todo ω). Portanto $P \in I_H(A)$. ■

A proposição acima, em linha com o que já foi discutido para PI-álgebras e PI-álgebras graduadas nos motiva a formular a principal questão a ser considerada no restante desse trabalho:

Sejam A e B dois H-comódulo álgebras. Se $\mathrm{Id}_H(A) = \mathrm{Id}_H(B)$ então quis condições devemos impor sobre A e B a fim de garantir que $A \cong B$ como H-comódulo álgebras?

Determinar se um elemento $P \in T$ é uma H-identidade polinomial para um H-comódulo álgebra A pode ser bastante complicado. Uma forma de fazê-lo é contar com uma caracterização conveniente de todos os homomorfismos de T em A. Felizmente, essa estratégia estará disponível na Seção 5.2. Aljadeff e Kassel em [2] e [31], desenvolvem uma forma alternativa de determinar $\mathrm{Id}_H(A)$. Esse é o tema da próxima seção.

4.3 H-Identidades Polinomiais para extensões H-cleft sobre R

O estudo das H-identidades polinomiais para extensões H-cleft foi iniciado por Aljadeff e Kassel em [2] e [31] no caso em que $R = k$ um corpo infinito. Tal estudo é

facilitado devido à existência de uma aplicação Ω tal que

$$\ker(\Omega) = \mathrm{Id}_H(B)$$

quando $k \subset B$ é uma extensão H-cleft.

Tal aplicação, chamada *aplicação universal de H-comódulo álgebras*, é, obviamente, um valioso recurso que permite testar por meio de cálculo direto se um dado elemento de T é ou não uma H-identidade polinomial.

Tendo-nos proposto a realizar este estudo também no caso em que R é um anel comutativo com unidade, é natural empreendermos um esforço para tentar generalizar tanto quanto possível alguns dos resultados de Kassel e Aljadeff para extensões H-cleft $R \subset B$.

No Corolário 4.3.7, mostraremos que, para o mesmo homomorfismo Ω,

$$\ker(\Omega) \subseteq \mathrm{Id}_H(B),$$

ou seja, que usar tal Ω pode ser uma forma conveniente de mostrar que um certo elemento $P \in \mathrm{Id}_H(B)$.

A aplicação Ω será construída a partir de uma uma versão comutativa de T que construímos a seguir: Para cada $i \geq 2$ considere $t_i^H = \{t_i^x \mid x \in H\}$ uma cópia de H como R-módulo. Os elementos t_i^x de t_i^H serão chamados de t-símbolos.

Defina a soma direta de cópias de H

$$t_H = \bigoplus_{i \geq 1} t_i^H,$$

e considere a álgebra simétrica sobre t_H, denotada por $S = S(t_H)$.

Quando H é um R-módulo livre, pela Proposição 1.16 temos que $S \cong R[I]$, em que I é um conjunto de índices para uma base de t_H. Note que fixando uma base C de H podemos usar $\{t_i^x \mid x \in C, i \geq 1\}$ como I.

Seja $R \subset B$ uma extensão H-cleft com seção γ e considere $S \otimes B$ com estrutura usual de álgebra. Defina a aplicação linear

$$\begin{array}{rccc} \varphi\colon & Z_H & \longrightarrow & S \otimes B \\ & Z_i^x & \longmapsto & \sum t_i^{x_1} \otimes \gamma(x_2). \end{array}$$

Pela propriedade universal da álgebra tensorial, existe um único homomorfismo de álgebras $\Omega\colon T \longrightarrow S \otimes B$ tal que

$$\Omega(Z_i^x) = \sum t_i^{x_1} \otimes \gamma(x_2), \tag{4.1}$$

para todo $x \in H$ e para todo $i \geq 1$.

A fim de que $\ker(\Omega) \subseteq \mathrm{Id}_H(A)$, é preciso que Ω seja um homomorfismo de H-comódulo álgebras. Comecemos, então, por construir uma estrutura de H-comódulo álgebra para $S \otimes B$:

Proposição 4.3.1. *Seja $R \subset B$ uma extensão H-cleft. Então $S \otimes B$ é um H-comódulo álgebra com coação*

$$\begin{array}{rccc} \rho_{SB}\colon & S \otimes B & \longrightarrow & S \otimes B \otimes H \\ & t_i^x \otimes \gamma(y) & \longmapsto & \sum t_i^x \otimes \gamma(y_1) \otimes y_2 \end{array}$$

para todo $x, y \in H$.

Demonstração. Dada a coação ρ_B de B,é óbvio que $\rho_{SB} = \mathrm{id} \otimes \rho_B$ define uma coação para $S \otimes B$. Para verificar que tal coação tem a forma do enunciado, como $\gamma\colon H \longrightarrow B$ é um homomorfismo de H-comódulos, ou seja, $\rho \circ \gamma = (\gamma \otimes \mathrm{id}) \circ \Delta$, então, nos elementos $t_i^x \otimes \gamma(y)$, com $x, y \in H$ e $i \geq 1$,

$$\rho_{SB}(t_i^x \otimes \gamma(y)) = \sum t_i^x \otimes \gamma(y_1) \otimes y_2. \tag{4.2}$$

Porém, pelo isomorfismo do Teorema 3.4.3 e da propriedade da base normal, existe um isomorfismo de H-comódulos $\varphi\colon H \longrightarrow B$ dado por $\varphi(y) = \gamma(y)$, para todo $y \in H$. Logo, todo elemento de $S \otimes B$ se expressa como combinação dos tensores simples $t_i^x \otimes \gamma(y)$, com $x, y \in H$, e isso mostra que (4.2) define ρ_{SB}. ∎

Proposição 4.3.2. *Seja $R \subset B$ uma extensão H-cleft. Então a aplicação $\Omega\colon T \longrightarrow S \otimes B$ como em (4.1) é um homomorfismo de H-comódulo álgebras.*

Demonstração. Bata mostrar que Ω é um homomorfismo de H-comódulos. Sejam ρ_{SB} e ρ_T são as coações que tornam $S \otimes B$ e T, respectivamente, H-comódulos. Então, nos geradores Z_i^x de T, temos

$$\begin{aligned} (\rho_{SB} \circ \Omega)(Z_i^x) &= \rho_{SB}\left(\sum t_i^{x_1} \otimes \gamma(x_2)\right) \\ &= \sum t_i^{x_1} \otimes \gamma(x_2) \otimes x_3 \\ &= (\Omega \otimes \mathrm{id})\left(\sum Z_i^{x_1} \otimes x_2\right) \\ &= ((\Omega \otimes \mathrm{id}) \circ \rho_T)(Z_i^x) \end{aligned}$$

para todo $x \in H$ e $i \geq 1$. Logo $\rho_{SB} \circ \Omega = (\Omega \otimes \mathrm{id}) \circ \rho_T$. ∎

O próximo passo será mostrar que todo homomorfismo de H-comódulo álgebras $\omega\colon T \longrightarrow B$ se fatora através de Ω (conforme Teorema 4.3.6). Para isso, necessitaremos de alguns lemas e convém fixar a seguinte notação:

- $\mathrm{Alg}_R(X, Y)$ denota os homomorfismos de álgebras $X \longrightarrow Y$,
- $\mathrm{Alg}_R^H(X, Y)$ denota os homomorfismos de H-comódulo álgebras $X \longrightarrow Y$,

Lema 4.3.3. *Seja $R \subset B$ uma extensão H-cleft com seção γ. Então a correspondência*

$$\mathrm{Alg}_R^H(T, B) \longleftrightarrow \mathrm{Hom}_R^H(Z_H, H)$$

é biunívoca. Em particular, para todo $\omega \in \mathrm{Alg}_R^H(T, B)$, a restrição de Ω a Z_H é fatorável através da seção γ, isto é, existe único $\alpha \in \mathrm{Hom}_R^H(Z_H, H)$ tal que $\omega(Z_i^x) = (\gamma \circ \alpha)(Z_i^x)$, para todo $x \in H$ e $i \geq 1$.

Demonstração. A propriedade fundamental da álgebra tensorial nos dá uma correspondência biunívoca

$$\mathrm{Alg}_R(T, B) \longleftrightarrow \mathrm{Hom}_R(Z_H, B).$$

De imediato, segue da Proposição 4.2.1 que

$$\mathrm{Alg}_R^H(T, B) \longleftrightarrow \mathrm{Hom}_R^H(Z_H, B).$$

Da propriedade da base normal de B, ou seja do fato de $B \cong R \otimes H \cong H$ como H-comódulos, resulta uma segunda correspondência biunívoca

$$\mathrm{Hom}_R^H(Z_H, B) \longleftrightarrow \mathrm{Hom}_R^H(Z_H, H).$$

Compondo estas bijeções, obtemos a do enunciado.

Para mostrar que $\omega(Z_i^x) = (\gamma \circ \alpha)(Z_i^x)$, para todo $x \in H$ e $i \geq 1$, note que no caso de extensões H-cleft de um anel, o isomorfismo de H-comódulos $\Phi\colon {}_\alpha H \longrightarrow B$ do Teorema 3.4.3 composto com o isomorfismo da propriedade da base normal que garante $H \cong {}_\alpha H$ como H-comódulos, é precisamente γ. Logo, se $\Phi^{-1}\colon B \longrightarrow H$ é a inversa de Φ (a menos do isomorfismo da base normal, que em geral será omitido), considere $\alpha := \Phi^{-1} \circ \omega|_{Z_H} \in \mathrm{Hom}_R^H(Z_H, H)$. Assim,

$$\omega(Z_i^x) = (\gamma \circ \Phi^{-1} \circ \omega)(Z_i^x) = (\gamma \circ \alpha)(Z_i^x).$$

■

Lema 4.3.4. *A correspondência*

$$\mathrm{Alg}_R(S, R) \longleftrightarrow \mathrm{Hom}_R(Z_H, R)$$

é biunívoca. Em particular, para todo $g \in \mathrm{Hom}_R(Z_H, R)$ *existe único* $\chi \in \mathrm{Alg}_R(S, R)$ *tal que* $g(Z_i^x) = \chi(t_i^x)$*, para todo* $x \in H$ *e* $i \geq 1$.

Este lema segue da propriedade universal da álgebra tensorial combinada com o isomorfismo de R-módulos $Z_H \cong t_H$.

O resultado a seguir aplicado a Z_H conecta o Lema 4.3.3 ao Lema 4.3.4.

Lema 4.3.5. *Se* Y *é um* H*-comódulo com coação* $\rho\colon Y \longrightarrow Y \otimes H$*, então a correspondência*

$$\mathrm{Hom}_R^H(Y, H) \longleftrightarrow \mathrm{Hom}_R(Y, R)$$

é biunívoca. Em particular, para todo $f \in \mathrm{Hom}_R^H(Y, H)$*,*

$$f = ((\varepsilon \circ f) \otimes \mathrm{id}) \circ \rho.$$

Demonstração. Defina

$$\begin{array}{rccc} \varphi\colon & \mathrm{Hom}_R^H(Y,H) & \longrightarrow & \mathrm{Hom}_R(Y,R) \\ & f & \longmapsto & \varepsilon \circ f \end{array}$$

$$\begin{array}{rccc} \psi\colon & \mathrm{Hom}_R(Y,R) & \longrightarrow & \mathrm{Hom}_R^H(Y,H) \\ & g & \longmapsto & (g \otimes \mathrm{id}) \circ \rho \end{array}$$

A função φ está claramente bem definida. Por outro lado, para ψ, devemos mostrar que $\psi(g)$ é um homomorfismo de H-comódulos, isto é, mostremos que para toda $g \in Hom_R(Y, R)$, a aplicação linear $\psi_g := \psi(g)$ torna comutativo o seguinte diagrama:

$$\begin{array}{ccc} Y & \xrightarrow{\psi_g} & H \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle\Delta} \\ Y \otimes H & \xrightarrow{\psi_g \otimes \mathrm{id}} & H \otimes H \end{array}$$

Como ρ é um homomorfismo de H-comódulos, isto é, $(\rho \otimes \mathrm{id}) \circ \rho = (\mathrm{id} \otimes \Delta) \circ \rho$, então

$$\begin{aligned} (\psi_g \otimes \mathrm{id}) \circ \rho &= (((g \otimes \mathrm{id}) \circ \rho) \otimes \mathrm{id}) \circ \rho \\ &= (g \otimes \mathrm{id} \otimes \mathrm{id}) \circ (\rho \otimes \mathrm{id}) \circ \rho \\ &= (g \otimes \mathrm{id} \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \Delta) \circ \rho \\ &= \Delta \circ (g \otimes \mathrm{id}) \circ \rho \\ &= \Delta \circ \psi_g. \end{aligned}$$

Portanto ψ está bem definida.

Como $((\varepsilon \otimes \mathrm{id}) \circ \Delta)(x) = x$ para todo $x \in H$ e usando que $f \in \mathrm{Hom}_R^H(Y, H)$, ou seja, $\Delta \circ f = (f \otimes \mathrm{id}) \circ \rho$ temos que

$$\begin{aligned}(\psi \circ \varphi)(f) &= \psi \circ \varepsilon \circ f) \\ &= ((\varepsilon \circ f) \otimes \mathrm{id}) \circ \rho \\ &= (\varepsilon \otimes \mathrm{id}) \circ ((f \otimes \mathrm{id}) \circ \rho) \\ &= (\varepsilon \otimes \mathrm{id}) \circ \Delta \circ f \\ &= f\end{aligned}$$

e

$$\begin{aligned}(\varphi \circ \psi)(g) &= \varphi \circ ((g \otimes \mathrm{id}) \circ \rho) \\ &= \varepsilon \circ (g \otimes \mathrm{id}) \circ \rho \\ &= (g \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \varepsilon) \circ \rho \\ &= g.\end{aligned}$$

Isto mostra a primeira afirmação do enunciado. A segunda afirmação é consequência imediata da bijeção:

$$f = (\psi \circ \varphi)(f) = \psi(\varepsilon \circ f) = ((\varepsilon \circ f) \otimes \mathrm{id}) \circ \rho.$$

■

Teorema 4.3.6. *Seja $R \subset B$ uma extensão H-cleft. Então existe uma correspondência biunívoca*

$$\mathrm{Alg}_R^H(T, B) \longleftrightarrow \mathrm{Alg}_R(S, R).$$

Em particular, para todo $\omega \in \mathrm{Alg}_R^H(T, B)$ existe único $\chi \in \mathrm{Alg}_R(S, R)$ tal que

$$\omega = (\chi \otimes \mathrm{id}) \circ \Omega. \tag{4.3}$$

Demonstração. A correspondência biunívoca segue diretamente dos lemas anteriores. Mostremos a equação (4.3). Sejam ρ coação e γ seção para B. Dado $\omega \in \mathrm{Alg}_R^H(T, B)$, pelo Lema 4.3.3, existe único $\alpha \in \mathrm{Hom}_R^H(Z_H, H)$ tal que $\omega(Z_i^x) = (\gamma \circ \alpha)(Z_i^x)$. Pelo Lema 4.3.5, temos que $\alpha = ((\varepsilon \circ \alpha) \otimes \mathrm{id}) \circ \rho$. Como $\varepsilon \circ \alpha \in \mathrm{Hom}_R(Z_H, R)$, então, pelo Lema 4.3.4, existe único $\chi \in \mathrm{Alg}_R(S, R)$ tal que $(\varepsilon \circ \alpha)(Z_i^x) = \chi(t_i^x)$. Com isso, para todo $x \in H$ e $i \geq 1$

$$\begin{aligned}
\omega(Z_i^x) &= (\gamma \circ \alpha)(Z_i^x) \\
&= \gamma \circ (((\varepsilon \circ \alpha) \otimes \mathrm{id}) \circ \rho)(Z_i^x) \\
&= \gamma \circ ((\varepsilon \circ \alpha) \otimes \mathrm{id}) \left(\sum Z_i^{x_1} \otimes x_2\right) \\
&= \gamma \left(\sum (\varepsilon \circ \alpha)(Z_i^{x_1}) \otimes x_2\right) \\
&= \sum (\varepsilon \circ \alpha)(Z_i^{x_1}) \otimes \gamma(x_2) \\
&= \sum \chi(t_i^{x_1}) \otimes \gamma(x_2) \\
&= (\chi \otimes \mathrm{id}) \circ \sum t_i^{x_1} \otimes \gamma(x_2) \\
&= ((\chi \otimes \mathrm{id}) \circ \Omega)(Z_i^x).
\end{aligned}$$

■

Corolário 4.3.7. *Seja $R \subset B$ uma extensão H-cleft e $P \in T$. Se $P \in \ker \Omega$ então P é uma H-identidade polinomial para B. Em outras palavras,* $\ker(\Omega) \subseteq \mathrm{Id}_H(B)$.

Demonstração. Pelo Teorema 4.3.6, para cada $\omega \in \mathrm{Alg}_R^H(T, B)$ existe $\chi \in \mathrm{Alg}_R(S, R)$ tal que

$$\omega = (\chi \otimes \mathrm{id}) \circ \Omega.$$

Se $P \in \ker \Omega$ então

$$\omega(P) = ((\chi \otimes \mathrm{id}) \circ \Omega)(P) = 0.$$

Portanto $P \in \mathrm{Id}_H(B)$. ■

Tomando $R = k$ um corpo infinito, Kassel mostrou que vale a recíproca desse corolário:

Teorema 4.3.8. *[31, 2.4] Sejam k um corpo infinito, $k \subset B$ uma extensão H-cleft e $P \in T$. Então $P \in \ker(\Omega)$ se e somente se P é uma H-identidade polinomial para B. Em outras palavras,* $\ker(\Omega) = \mathrm{Id}_H(B)$.

Mais adiante, na Seção 5.2, em que R é um anel finito, será mostrado que o polinômio (5.7) está em $\mathrm{Id}_H(B)$ mas não em $\ker(\Omega)$.

Capítulo 5

Problema do Isomorfismo para Extensões H-cleft

Neste capítulo, trataremos do problema do isomorfismo para $R \subset B$ uma extensão H-cleft. Ou seja, dadas $R \subset B$ e $R \subset B'$ duas extensões H-cleft, se $\mathrm{Id}_H(B) = \mathrm{Id}_H(B')$ então será que $B \cong B'$ como H-comódulo álgebras?

A primeira seção trata do problema do isomorfismo para as extensões H-cleft sobre álgebras monomiais não semissimples. Este problema foi resolvido afirmativamente quando $\mathbb{G}$ (como na Definição 2.5.1) é do tipo I por Kassel em 2013 [31] sob a hipótese de k um corpo algebricamente fechado. Sob esta mesma hipótese, respondemos a questão afirmativamente para todas as álgebras monomiais não semissimples [43].

Na segunda seção buscamos estender os resultados anteriores tanto quanto possível para um anel comutativo com unidade e mostramos que para $H = H_N^q$ as H_N^q-identidades polinomiais são capazes de distinguir as $R \subset B$ extensões H_N^q-cleft se R for finito e $N \in R^\times$. Uma versão preliminar de um artigo contendo este trabalho pode ser encontrado em [39].

5.1 Problema do Isomorfismo para Extensões $A(\mathbb{G})$-cleft sobre k

5.1.1 As Extensões $A(\mathbb{G})$-Cleft sobre k

Nesta seção estaremos considerando $R = k$ um corpo algebricamente fechado de característica zero e $H = A(\mathbb{G})$ uma álgebra de Hopf monomial não semissimples

(conforme Seção 2.5).

As extensões $k \subset B$ $A(\mathbb{G})$-cleft foram caracterizadas por Bichon, em 2006 [10]. Sendo extensões sobre um corpo k com $\dim_k(A(\mathbb{G})) < \infty$ então, pela Proposição 3.5.7, tal caracterização inclui também todos os objetos $A(\mathbb{G})$-Galois.

O resultado principal desta seção será o Teorema 5.1.8, mostrando que as $A(\mathbb{G})$-identidades polinomiais contêm informação suficiente para distinguir os objetos $A(\mathbb{G})$-Galois a menos de isomorfismo.

Considere a seguinte álgebra:

Definição 5.1.1. Para cada $A(\mathbb{G})$, sejam $\sigma \in Z^2(G, k^\times)$ e $a \in k$. Definimos $A_{\sigma,a}(\mathbb{G})$ como sendo a álgebra com geradores $\{u_x \mid x \in G\} \sqcup \{u_y\}$ sujeita às relações:

$$u_x u_{x'} = \sigma(x, x')u_{xx'},\ u_1 = 1,\ u_y u_x = \chi(x)u_x u_y \text{ e } u_y^d = a u_{g^d},$$

para todo $x, x' \in G$.

A proposição a seguir define um critério para que as álgebras $A_{\sigma,a}(\mathbb{G})$ sejam objetos $A(\mathbb{G})$-Galois:

Teorema 5.1.2. *[10, 2.3] A álgebra $A_{\sigma,a}(\mathbb{G})$ tem estrutura de $A(\mathbb{G})$-comódulo álgebra com coação $\rho\colon A_{\sigma,a}(\mathbb{G}) \longrightarrow A_{\sigma,a}(\mathbb{G}) \otimes A(\mathbb{G})$ dada por $\rho(u_y) = u_1 \otimes y + u_y \otimes g$ e $\rho(u_x) = u_x \otimes x$ para todo $x \in G$. Além disso, $A_{\sigma,a}(\mathbb{G})$ é um objeto $A(\mathbb{G})$-Galois se e somente se*

$$a\sigma(g^d, x) = a\chi(x)^d\sigma(x, g^d), \tag{5.1}$$

para todo $x \in G$. Neste caso, o conjunto $\{u_x u_y^i \mid x \in G \text{ e } 0 \leqslant i \leqslant d-1\}$ é uma base de $A_{\sigma,a}(\mathbb{G})$ e a aplicação $\gamma\colon A(\mathbb{G}) \longrightarrow A_{\sigma,a}(\mathbb{G})$, $xy^i \mapsto u_x u_y^i$ é um isomorfismo de $A(\mathbb{G})$-comódulos.

Como corolário desta proposição e do Teorema 3.4.3 temos:

Corolário 5.1.3. *Se $A_{\sigma,a}(\mathbb{G})$ é um objeto $A(\mathbb{G})$-Galois, então o isomorfismo γ da proposição anterior é uma seção para $A_{\sigma,a}(\mathbb{G})$.*

Ainda que $A_{\sigma,a}(\mathbb{G})$ não seja necessariamente um objeto $A(\mathbb{G})$-Galois, todo objeto $A(\mathbb{G})$-Galois é do tipo $A_{\sigma,a}(\mathbb{G})$:

Proposição 5.1.4. *[10, 2.9] Seja B um objeto $A(\mathbb{G})$-Galois. Então existem $\sigma \in Z^2(G, k^\times)$ e $a \in k$ tal que $B \cong A_{\sigma,a}(\mathbb{G})$ como $A(\mathbb{G})$-comódulo álgebras.*

A proposição a seguir estabelece um critério de isomorfismo para os objetos $A(\mathbb{G})$-Galois:

Teorema 5.1.5. *[10, 2.10] Sejam $\sigma, \tau \in Z^2(G, k^\times)$ e $a, b \in k$ tais que$A_{\sigma,a}(\mathbb{G})$ e $A_{\tau,b}(\mathbb{G})$ são objetos $A(\mathbb{G})$-Galois. Então os $A(\mathbb{G})$-comódulo álgebras $A_{\sigma,a}(\mathbb{G})$ e $A_{\tau,b}(\mathbb{G})$ são isomorfos se e somente se existe $\nu\colon G \longrightarrow k^\times$ com $\nu(1) = 1$ tal que*

$$\sigma = \partial(\nu)\tau \text{ e } b = a\nu(g^d). \tag{5.2}$$

Os resultados a seguir foram baseados ou parafraseados de Bichon [10].

Proposição 5.1.6. *Seja $\mathbb{G}$ um dado de grupo dos tipos II ou IV. Então todo objeto $A(\mathbb{G})$-Galois é isomorfo a $A_{\sigma,0}(\mathbb{G})$ para algum $\sigma \in Z^2(G, k^\times)$.*

Demonstração. Seja B um objeto $A(\mathbb{G})$-Galois. Pela Proposição 5.1.4, $B \cong A_{\sigma,a}(\mathbb{G})$ para certos $\sigma \in Z^2(G, k^\times)$ e $a \in k$. No tipo II, $d = n$ e $\chi^d \neq 1$, logo $g^d = 1$ e assim, $\sigma(x, g^d) = 1$. No tipo IV não existe $\sigma \in Z^2(G, k^\times)$ que satisfaça $\sigma(g^d, x) = \chi^d(x)\sigma(x, g^d)$, para todo $x \in G$. Nos dois casos, a condição (5.1) é satisfeita se e somente se, $a = 0$. Portanto $B \cong A_{\sigma,0}$ para algum $\sigma \in Z^2(G, k^\times)$. ∎

Proposição 5.1.7. *Seja $\mathbb{G}$ um dado de grupo dos tipos III, V ou VI. Então todo objeto $A(\mathbb{G})$-Galois é isomorfo a $A_{\sigma,0}(\mathbb{G})$ ou $A_{\sigma,1}(\mathbb{G})$ para algum $\sigma \in Z^2(G, k^\times)$.*

Demonstração. Seja B um objeto $A(\mathbb{G})$-Galois. Pela Proposição 5.1.4, $B \cong A_{\tau,a}(\mathbb{G})$ para certos $\tau \in Z^2(G, k^\times)$ e $a \in k$. Se $a = 0$ então segue do Teorema 5.1.2 que $A_{\tau,0}$ é um objeto $A(\mathbb{G})$-Galois. Para $a \neq 0$, seja $\nu\colon G \longrightarrow k^\times$ uma aplicação tal que $\nu(1) = 1$ e $\nu(g^d) = a$ (note que $g^d \neq 1$). Tomando $\sigma = \partial(\nu)\tau \in Z^2(G, k^\times)$, temos que

$$\sigma(g^d, x) = \partial(\nu)\tau(g^d, x) = \partial(\nu)\chi(x)^d\tau(x, g^d) = \chi(x)^d\sigma(x, g^d),$$

para todo $x \in G$. Logo, pelo Teorema 5.1.2, $A_{\sigma,1}(\mathbb{G})$ é um objeto $A(\mathbb{G})$-Galois. Segue do Teorema 5.1.5 que $A_{\tau,a}(\mathbb{G}) \cong A_{\sigma,1}(\mathbb{G})$. ∎

5.1.2 $A(\mathbb{G})$-identidades polinomiais para $A_{\sigma,a}(\mathbb{G})$

Nesta subseção vamos mostrar o primeiro dos dois principais resultado desta tese:

Teorema 5.1.8. *Seja k um corpo algebricamente fechado de característica zero e $A(\mathbb{G})$ uma álgebra monomial não semissimples. Sejam B e B' objetos $A(\mathbb{G})$-Galois. Se*

$$\mathrm{Id}_{A(\mathbb{G})}(B) = \mathrm{Id}_{A(\mathbb{G})}(B'),$$

então B e B' são isomorfos como $A(\mathbb{G})$-comódulo álgebras.

Em outras palavras, todas as extensões $k \subset B$ $A(\mathbb{G})$-Galois são determinadas a menos de isomorfismo por suas $A(\mathbb{G})$-identidades polinomiais.

Note que o problema está bem colocado, ou seja, os objetos $A(\mathbb{G})$-Galois são álgebras com $A(\mathbb{G})$-identidade polinomial. Isso se dá pelo **??** e pelo fato de toda identidade polinomial ser uma H-identidade polinomial.

Usaremos a aplicação Ω definida na Seção 4.3 com uma alteração no seu contra-domínio. Tal alteração utiliza a Proposição 5.1.4 que garante que todo objeto $A(\mathbb{G})$-Galois B é isomorfo a algum $A_{\sigma,a}(\mathbb{G})$. Logo, faz sentido redefinir a aplicação universal de H-comódulo álgebras como

$$\begin{array}{rccc} \Omega\colon & T & \longrightarrow & S \otimes A_{\sigma,a}(\mathbb{G}) \\ & Z_i^z & \longmapsto & t_i^{z_1} \otimes \gamma(z_2) \end{array}$$

com γ a seção $\gamma(xy^i) = u_x u_y^i$, para todo $x, \in G$ e $0 \leq i \leq d-1$, dada no Corolário 5.1.3.

Claramente, podemos considerar Z_{kG} um subespaço de $Z_{A(\mathbb{G})}$ e $k^\sigma G$ como subálgebra de $A_{\sigma,a}(\mathbb{G})$ gerada pelos símbolos u_x ($x \in G$) e relações $u_x u_{x'} = \sigma(x, x')u_{xx'}$ e $u_1 = 1$, para todo $x, x' \in G$. Note que como σ é um 2-cociclo, $k^\sigma G$ é de fato uma álgebra torcida.

Como $\Omega(Z_i^x) = t_i^{x_1} \otimes u_{x_2}$, para todo $x \in G$, temos que $\Omega(Z_{kG}) \subseteq S\left(t_{kG}\right) \otimes k^\sigma G$.

O resultado a seguir é essencialmente parte do resultado [31, 3.4] mostrado por Kassel no contexto das álgebras de Hopf monomiais não semissimples do tipo I. Entretanto, constata-se aqui que a mesma demonstração continua válida para os tipos II a VI.

Proposição 5.1.9. *Seja k um corpo algebricamente fechado de característica zero. Sejam $A_{\sigma,a}(\mathbb{G})$ e $A_{\tau,a}(\mathbb{G})$ objetos $A(\mathbb{G})$-Galois para certos $a \in k$ e $\sigma, \tau \in Z^2(G, k^\times)$. Se*

$$\mathrm{Id}_{A(\mathbb{G})}(A_{\sigma,a}(\mathbb{G})) = \mathrm{Id}_{A(\mathbb{G})}(A_{\tau,a}(\mathbb{G}))$$

então os 2-cociclos σ e τ são coomólogos, ou seja, existe $\nu\colon G \longrightarrow k^\times$ com $\nu(1) = 1$ tal que $\tau = \partial(\nu)\sigma$.

Demonstração. Considere o diagrama:

$$\begin{array}{ccccccc} 0 & \longrightarrow & I_{kG}(k^\sigma G) & \longrightarrow & T\left(Z_{kG}\right) & \xrightarrow{\Omega} & S\left(t_{kG}\right) \otimes k^\sigma G \\ & & \downarrow{\scriptstyle \imath} & & \downarrow{\scriptstyle \imath_T} & & \downarrow{\scriptstyle \imath_S} \\ 0 & \longrightarrow & I_{A(\mathbb{G})}\left(A_{\sigma,a}(\mathbb{G})\right) & \longrightarrow & T\left(Z_{A(\mathbb{G})}\right) & \xrightarrow{\Omega} & S\left(t_{A(\mathbb{G})}\right) \otimes A_{\sigma,a}(\mathbb{G})) \end{array}$$

A aplicação vertical $\imath_T$ é induzida pela inclusão $kG \hookrightarrow A(\mathbb{G})$ e $\imath_T$ é injetora. A aplicação $\imath_S$ é induzida pela combinação das inclusões $kG \hookrightarrow A(\mathbb{G})$ e $k^\sigma G \hookrightarrow A_{\sigma,a}(\mathbb{G})$. A aplicação $\imath_S$ leva os geradores $t_i^x \otimes u_{x'}$ de $S\left(t_{kG}\right) \otimes k^\sigma G$ neles

mesmos, vistos como elementos de $S\left(t_{A(\mathbb{G})}\right) \otimes A_{\sigma,a}(\mathbb{G})$. Note que as sequências horizontais são exatas pelo Teorema 4.3.8. É corriqueiro verificar que os diagramas são comutativos. Portanto a restrição de $\imath_T$ para $\mathrm{Id}_{kG}(k^\sigma G)$ dada por $\imath$ e é injetora. Disto, segue que, em $T(Z_{A(\mathbb{G})})$,

$$\mathrm{Id}_{kG}\left(k^\sigma G\right) = T\left(Z_{kG}\right) \cap \mathrm{Id}_{A(\mathbb{G})}\left(A_{\sigma,a}(\mathbb{G})\right).$$

Assim, pela Proposição 4.2.5,

$$\begin{aligned}
\mathrm{Id}_G\left(k^\sigma G\right) &= \mathrm{Id}_{kG}\left(k^\sigma G\right) \\
&= T\left(Z_{kG}\right) \cap \mathrm{Id}_{A(\mathbb{G})}\left(A_{\sigma,a}(\mathbb{G})\right) \\
&= T\left(Z_{kG}\right) \cap \mathrm{Id}_{A(\mathbb{G})}\left(A_{\tau,b}(\mathbb{G})\right) \\
&= \mathrm{Id}_{kG}\left(k^\tau G\right) \\
&= \mathrm{Id}_G\left(k^\tau G\right).
\end{aligned}$$

então, por [1, 2.11], os 2-cociclos σ e τ são coomólogos. ∎

Para os dados de grupo do tipo II e IV o resultado anterior é suficiente para resolver o problema do isomorfismo dado que devido à Proposição 5.1.6 a condição $b = a\nu(g^d)$ do Teorema 5.1.5 é trivial. Porém, para os tipos II, V e VI, necessitaremos de certas $A(\mathbb{G})$-identidades polinomiais específicas. Por simplicidade de notação, alguns Z-símbolos e t-símbolos serão abreviados do seguinte modo:

$$\begin{aligned}
E &:= Z_1^1, & t_1 &:= t_1^1, \\
X &:= Z_1^g, & t_x &:= t_1^g, \\
Y &:= Z_1^y, & t_y &:= t_1^y.
\end{aligned}$$

Sejam $\mathbb{G} = (G, g, \chi, \mu)$ um dado de grupo e $d = o(\chi(g))$, de modo que $\chi(g)$ seja uma raiz d-ésima primitiva da unidade em k. No restante desta seção, denote $q := \chi(g)$.

Proposição 5.1.10. *Sejam $A_{\sigma,a}(\mathbb{G})$ um objeto $A(\mathbb{G})$-Galois. Em T, considere o elemento*

$$\mathcal{P} = (YX - qXY)^d - (1-q)^d X^d Y^d. \tag{5.3}$$

Então $\mathcal{P}$ é uma $A(\mathbb{G})$-identidade polinomial para $A_{\sigma,a}(\mathbb{G})$ se e somente se $a = 0$.

Demonstração. Seja $\Omega\colon T \longrightarrow S \otimes A_{\tau,b}(\mathbb{G})$. Pelo Teorema 4.3.8, $\mathcal{P}$ é uma

$A(\mathbb{G})$-identidade polinomial para $A_{\tau,b}(\mathbb{G})$ se e somente se $\Omega(\mathcal{P}) = 0$. Temos que:

$$\begin{aligned}\Omega(E) &= t_1 \otimes u_1,\\ \Omega(X) &= t_g \otimes u_g,\\ \Omega(Y) &= t_1 \otimes u_y + t_y \otimes u_g.\end{aligned}$$

Dado que Ω é um homomorfismo de álgebras,

$$\begin{aligned}\Omega(E^d) &= t_1^d \otimes u_1,\\ \Omega(X^d) &= t_g^d \otimes u_g^d,\\ \Omega(YX - qXY) &= (1-q)t_g t_y \otimes u_g^2,\\ \Omega((YX - qXY)^d) &= (1-q)^d t_g^d t_y^d \otimes u_g^{2d}.\end{aligned}$$

Visto que $t_1 \otimes u_y$ e $t_y \otimes u_g$ q-comutam então, pelo Lema 2.5.4,

$$\Omega(Y^d) = t_1^d t_y^d \otimes u_y^d u_g^d$$

Com isso,

$$\Omega(\mathcal{P}) = (1-q)^d t_g^d \otimes t_y^d u_g^{2d} - (1-q)^d t_g^d \otimes u_g^d (t_1^d u_y^d + t_y^d u_g^d) = -a(1-q)^d t_1^d t_g^d \otimes u_g^d u_{g^d}.$$

Como $(1-q) \neq 0$, então $\Omega(\mathcal{P}) = 0$ se e somente se $a = 0$. ∎

Proposição 5.1.11. *Seja $\mathbb{G}$ um dado de grupo do tipo III, V ou VI. Sejam $A_{\sigma,a}(\mathbb{G})$ e $A_{\tau,b}(\mathbb{G})$ objetos $A(\mathbb{G})$-Galois. Se $A_{\sigma,a}(\mathbb{G}) \cong A_{\tau,b}(\mathbb{G})$ então $a = b$.*

Demonstração. Suponha que $a \neq b$. Pela Proposição 5.1.7, podemos supor que $a = 0$ e $b = 1$. Como $A_{\sigma,a}(\mathbb{G}) \cong A_{\tau,b}(\mathbb{G})$ então $\mathrm{Id}_{A(\mathbb{G})}(A_{\sigma,a}(\mathbb{G})) = \mathrm{Id}_{A(\mathbb{G})}(A_{\tau,b}(\mathbb{G}))$. Logo, segue da Proposição 5.1.10 que $\mathcal{P}$ é uma $A(\mathbb{G})$-identidade polinomial para $A_{\sigma,0}(\mathbb{G})$ mas não é uma $A(\mathbb{G})$-identidade polinomial para $A_{\tau,1}(\mathbb{G})$. Desta contradição, segue que $a = b$. ∎

Com isso, nos tipos III, V e VI a condição $b = a\nu(g^d)$ do Teorema 5.1.5 se resume ao caso trivial (quando $a = b = 0$) ou $\nu(g^d) = 1$ (quando $a = b = 1$). Precisamos mostrar então que, no segundo caso, se as ${}_\alpha H$-identidades polinomiais coincidem então $\nu(g^d) = 1$.

Para cada $\sigma, \tau \in Z^2(G, k^\times)$, denote

$$\begin{aligned}S &:= \sigma(g^d, g^d)\sigma(g^d, g^{2d}) \dots \sigma(g^d, g^{(m-1)d})\\ T &:= \tau(g^d, g^d)\tau(g^d, g^{2d}) \dots \tau(g^d, g^{(m-1)d})\end{aligned}$$

Proposição 5.1.12. *Sejam $A_{\sigma,1}(\mathbb{G})$ e $A_{\tau,1}(\mathbb{G})$ objetos $A(\mathbb{G})$-Galois. Defina*

$$\mathcal{P} = (-(YX - qXY)^d + (1-q)^d X^d Y^d)^m - (1-q)^n S E^n X^n.$$

Então $\mathcal{P}$ é uma $A(\mathbb{G})$-identidade polinomial para $A_{\tau,1}(\mathbb{G})$ se e somente se $S = T$. Em particular, $\mathcal{P}$ é uma $A(\mathbb{G})$-identidade polinomial para $A_{\sigma,1}(\mathbb{G})$.

Demonstração. Escreva

$$c_\sigma := \sigma(g,g)\sigma(g,g^2)\dots\sigma(g,g^{d-1})$$
$$c_\tau := \tau(g,g)\tau(g,g^2)\dots\tau(g,g^{d-1})$$

Sabemos que $\mathcal{P}$ é uma $A(\mathbb{G})$-identidade polinomial para $A_{\tau,1}(\mathbb{G})$ se e somente se $\Omega(\mathcal{P}) = 0$. Temos que:

$$\Omega(E) = t_1 \otimes v_1,$$
$$\Omega(X) = t_g \otimes v_g,$$
$$\Omega(Y) = t_1 \otimes v_y + t_y \otimes v_g.$$

Como Ω é um homomorfismo de álgebras,

$$\Omega(E^d) = t_1^d \otimes v_1,$$
$$\Omega(X^d) = t_g^d \otimes v_g^d,$$
$$\Omega(YX - qXY) = (1-q) t_g t_y \otimes v_g^2,$$
$$\Omega((YX - qXY)^d) = (1-q)^d t_g^d t_y^d \otimes v_g^{2d}.$$

Visto que $t_1 \otimes v_y$ e $t_y \otimes v_g$ q-comutam então,

$$\Omega(Y^d) = t_1^d \otimes v_y^d + t_y^d \otimes v_g^d$$

E portanto

$$\Omega(-(YX - qXY)^d + (1-q)^d X^d Y^d) = (1-q)^d t_1^d t_g^d \otimes v_g^d v_y^d.$$

Com isso,

$$\begin{aligned}\Omega((-(YX-qXY)^d+(1-q)^dX^dY^d)^m) &= (1-q)^n t_1^n t_g^n \otimes (v_g^d v_y^d)^m \\ &= (1-q)^n t_1^n t_g^n \otimes (v_g^d v_{g^d})^m \\ &= (1-q)^n t_1^n t_g^n \otimes (c_\tau v_{g^d}^2)^m \\ &= (1-q)^n t_1^n t_g^n \otimes c_\tau^m (v_{g^d}^m)^2 \\ &= (1-q)^n t_1^n t_g^n \otimes c_\tau^m (Tv_1)^2 \\ &= (1-q)^n t_1^n t_g^n \otimes c_\tau^m T^2 v_1\end{aligned}$$

Por outro lado,

$$\begin{aligned}\Omega((1-q)^n SE^n X^n) &= (1-q)^n S t_1^n t_g^n \otimes v_g^n \\ &= (1-q)^n S t_1^n t_g^n \otimes (v_g^d)^m \\ &= (1-q)^n S t_1^n t_g^n \otimes (c_\tau v_{g^d})^m \\ &= (1-q)^n S t_1^n t_g^n \otimes c_\tau^m (v_{g^d})^m \\ &= (1-q)^n S t_1^n t_g^n \otimes c_\tau^m T v_1 \\ &= (1-q)^n t_1^n t_g^n \otimes c_\tau^m ST v_1\end{aligned}$$

E assim,

$$\Omega(\mathcal{P}) = (1-q)^n t_1^n t_g^n \otimes c_\tau^m (T-S)Tv_1.$$

Logo $\Omega(\mathcal{P}) = 0$ se e somente se $T = S$.

Em particular, $\mathcal{P}$ é uma $A(\mathbb{G})$-identidade polinomial para $A_{\sigma,1}(\mathbb{G})$. ■

Lema 5.1.13. *Sejam $\mathbb{G} = (G, g, \chi, \mu)$ um dado de grupo e $\sigma, \tau \in Z^2(G, k^\times)$. Se σ e τ são coomólogos então $S = \nu(g^d)^m T$, para toda $\nu\colon G \longrightarrow k^\times$ tal que $\sigma = \partial(\nu)\tau$ e $\nu(1) = 1$.*

Demonstração. Basta escrever

$$\begin{aligned}\sigma(g^d, g^d) &= \nu(g^d)\nu(g^d)\nu(g^{2d})^{-1}\tau(g^d, g^d) \\ \sigma(g^d, g^{2d}) &= \nu(g^d)\nu(g^{2d})\nu(g^{3d})^{-1}\tau(g^d, g^{2d}) \\ &\vdots \\ \sigma(g^d, g^{(m-1)d}) &= \nu(g^d)\nu(g^{(m-1)d})\nu(g^n)^{-1}\tau(g^d, g^{(m-1)d}).\end{aligned}$$

Então $S = \nu(g^d)^m T$. ■

Proposição 5.1.14. *Sejam $A_{\sigma,1}(\mathbb{G})$ e $A_{\tau,1}(\mathbb{G})$ objetos $A(\mathbb{G})$-Galois para certos $\sigma, \tau \in Z^2(G, k^\times)$. Se*

$$\mathrm{Id}_{A(\mathbb{G})}(A_{\sigma,1}(\mathbb{G})) = \mathrm{Id}_{A(\mathbb{G})}(A_{\tau,1}(\mathbb{G}))$$

então $A_{\sigma,1}(\mathbb{G}) \cong A_{\tau,1}(\mathbb{G})$ como $A(\mathbb{G})$-comódulo álgebras.

Demonstração. Pela Proposição 5.1.9, existe $\nu(g^d)^m = 1$, para todo $\nu\colon G \longrightarrow k^\times$ tal que $\sigma = \partial(\nu)\tau$ e $\nu(1) = 1$. Como as $A(\mathbb{G})$-identidades polinomiais coincidem, o polinômio $\mathcal{P}$ da Proposição 5.1.12 é uma $A(\mathbb{G})$-identidade polinomial para $A_{\tau,1}(\mathbb{G})$ e portanto $S = T$. Pelo Lema 5.1.13, $\nu(g^d)^m = 1$.

Seja $N = \langle g \rangle$ o grupo cíclico gerado por g. Fixe ζ uma raiz em k do polinômio $p(x) = x^d - \nu(g^d)$. Defina $f\colon N \longrightarrow k^\times$ por $f(g^r) = 1/\zeta^r$. Não é difícil ver que a aplicação f está bem definida, é um homomorfismo de grupos, $f(1) = 1$ e $f(g^d) = 1/\nu(g^d)$.

Pelo teorema principal em Huang [24], o homomorfismo de grupos $f\colon N \longrightarrow k^\times$ dado por $f(g^r) = 1/\zeta^r$ se estende a um homomorfismo de grupos $F\colon G \longrightarrow k^\times$.

Com isso, dado o 2-cobordo $\nu\colon G \longrightarrow k^\times$, podemos definir para todo $x \in G$,

$$\eta(x) = F(x)\nu(x)$$

tal que $\eta(1) = 1$, $\sigma = \partial(\eta)\tau$ (pois $\sigma = \partial(\nu)\tau$) e $\eta(g^d) = 1$, o que, pelo Teorema 5.1.5 conclui a demonstração. ∎

Com esses resultados, passamos à demonstração do Teorema 5.1.8.

Demonstração. Em vista do trabalho de Kassel [31, 3.4] para as álgebras monomiais não semissimples do Tipo I, portanto podemos assumir que $A(\mathbb{G})$ é dos tipos II a VI.

Segue da Proposição 5.1.7 que dados dois objetos $A(\mathbb{G})$-Galois A e B, então $A \cong A_{\sigma,a}(\mathbb{G})$ e $B \cong A_{\tau,b}(\mathbb{G})$ para certos $\sigma, \tau \in Z^2(G, k^\times)$ e $a, b \in k$.

Para os tipos II e IV, $a = b = 0$ devido à Proposição 5.1.6. Então o resultado segue da Proposição 5.1.9.

Para os tipos III, V e VI, $a, b \in \{0, 1\}$ devido à Proposição 5.1.7. Como $\mathrm{Id}_{A(\mathbb{G})}(A_{\sigma,a}(\mathbb{G})) = \mathrm{Id}_{A(\mathbb{G})}(A_{\tau,b}(\mathbb{G}))$, pela Proposição 5.1.11, temos que $a = b$. Se $a = b = 0 então$, novamente, o resultado segue da Proposição 5.1.9. Se $a = b = 1$ então o resultado segue da Proposição 5.1.14. ∎

5.2 Problema do Isomorfismo para Extensões H_N^q-cleft sobre R

5.2.1 As Extensões H_N^q-cleft sobre R

O objetivo do trabalho de Masuoka em [37] é classificar as extensões $A \subset B$ H_N^q-cleft. As definições e resultados a seguir são adaptações de [37] para o caso $A = R$.

Fixe H_N^q uma álgebra de Taft sobre R.

Definição 5.2.1. Dada uma tripla $\underline{d} = (u, a, b)$, com $u \in R^\times$ e $a, b \in R$, definimos um par $(\mathcal{B}_{\underline{d}}, \varphi_{\underline{d}})$ da seguinte forma: $\mathcal{B}_{\underline{d}}$ é uma álgebra gerada pelos símbolos v_g, v_x com relações

(R1) $v_g^N = u$,

(R2) $v_x^N = a$,

(R3) $v_x v_g = q v_g v_x + b v_g^2$

e $\varphi_{\underline{d}}\colon H_N^q \longrightarrow \mathcal{B}_{\underline{d}}$ a aplicação linear dada por

$$\varphi_{\underline{d}}(g^m x^n) = v_g^m v_x^n,\ 0 \leqslant m, n < N.$$

A tripla $\underline{d} = (u, a, b)$ é chamada de dados *cleft*.

Os resultados a seguir pretendem garantir que $R \subset \mathcal{B}_{\underline{d}}$ é uma extensão H_N^q-cleft. Mais ainda, que toda extensão $R \subset B$ H_N^q-cleft é isomorfa a $\mathcal{B}_{\underline{d}}$ para algum $\underline{d}$.

Proposição 5.2.2. *[37, 2.15]*

1) $\mathcal{B}_{\underline{d}}$ *é um* R*-módulo livre com base* $\{v_g^m v_x^n,\ 0 \leqslant m, n < N\}$.

2) $\mathcal{B}_{\underline{d}}$ *tem estrutura de* H_N^q*-comódulo álgebra determinada por*

$$v_g \mapsto v_g \otimes g$$
$$v_x \mapsto 1 \otimes x + v_x \otimes g.$$

A subálgebra de coinvariantes de $\mathcal{B}_{\underline{d}}$ *é* R.

3) A aplicação $\varphi_{\underline{d}}\colon H_N^q \longrightarrow \mathcal{B}_{\underline{d}}$ *dada por*

$$\varphi_{\underline{d}}(g^m x^n) = v_g^m v_x^n,\ 0 \leqslant m, n < N$$

é uma seção para $\mathcal{B}_{\underline{d}}$.

Então $(\mathcal{B}_{\underline{d}}, \varphi_{\underline{d}})$ *é um sistema cleft para* H_N^q *sobre* R.

Teorema 5.2.3. *[37, 2.17] Toda extensão* H_N^q*-cleft sobre* R *é isomorfa como* H_N^q*-comódulo álgebra a* $\mathcal{B}_{\underline{d}}$ *para certos dados cleft* $\underline{d}$.

O próximo resultado define um critério de isomorfismo para as extensões H_N^q-cleft.

Proposição 5.2.4. *[37, 2.19] Sejam* $\mathcal{B}_{\underline{d}}$ *e* $\mathcal{B}_{\underline{d'}}$ *extensões* H_N^q*-cleft sobre* R.

1. *Se* $F\colon \mathcal{B}_{\underline{d'}} \longrightarrow \mathcal{B}_{\underline{d}}$ *é um isomorfismo de* H_N^q*-comódulo álgebras, então existe um par* $(s,t) \in R^\times \times R$ *tal que*

$$F(v'_g) = sv_g \quad e \quad F(v'_x) = v_x + tv_g. \tag{5.4}$$

2. *Se* $(s,t) \in R^\times \times R$, *então o homomorfismo de álgebras* $F\colon \mathcal{B}_{\underline{d}} \longrightarrow \mathcal{B}_{\underline{d'}}$ *dado por* (5.4) *está bem definido se e somente se*

$$\begin{aligned} u' &= s^N u, \\ a' &= a + t(t+b+qb)(t+b+q^2b)\dots(t+b+q^{N-1}b)u, \\ b' &= (b+t-qt)s^{-1}. \end{aligned} \tag{5.5}$$

Neste caso, F *é um isomorfismo de* H_N^q*-comódulo álgebras.*

Se $1-q \in R^\times$, podemos reduzir os dados cleft de 3 para 2 parâmetros e simplificar os critérios em Proposição 5.2.4.

Corolário 5.2.5. *Seja* $R \subset \mathcal{B}_{(u,a,b)}$ *uma extensão* H_N^q*-cleft. Se* $1-q \in R^\times$ *então existe* $a' \in R$ *tal que* $\mathcal{B}_{(u,a,b)} \cong \mathcal{B}_{(u,a',0)}$.

Demonstração. Pela Proposição 5.2.4 é suficiente encontrar um par $(s,t) \in R^\times \times R$ que satisfaça as equações (5.5). Tome $s=1$ e $t=-b/(1-q)$. A primeira e a terceira equações em (5.5) são claramente satisfeitas. Já a segunda equação determina o valor de a' a ser utilizado. ∎

A partir de agora denotaremos $\mathcal{B}_{(u,a,0)}$ simplesmente por $\mathcal{B}_{(u,a)}$.

A Proposição 5.2.4, tendo em vista o Corolário 5.2.5, nos dá um novo critério para distinguir as extensões H_N^q-cleft quando $1-q \in R^\times$:

Proposição 5.2.6. *Sejam* $R \subset \mathcal{B}_{(u,a)}$ *e* $R \subset \mathcal{B}_{(u',a')}$ *duas extensões* H*-cleft. Então* $\mathcal{B}_{(u,a)} \cong \mathcal{B}_{(u',a')}$ *se e somente se existe* $s \in R^\times$ *tal que*

$$\begin{aligned} u' &= s^N u, \\ a' &= a \end{aligned} \tag{5.6}$$

5.2.2 H_N^q-identidades polinomiais para $\mathcal{B}_{u,a}$

Nosso objetivo é mostrar o segundo dos dois principais resultados desta tese:

Teorema 5.2.7. *Sejam R um anel finito e H_N^q uma álgebra de Taft sobre R. Sejam $R \subset B$ e $R \subset B'$ extensões H_N^q-cleft. Se $N \in R^\times$ e*

$$\mathrm{Id}_{H_N^q}(B) = \mathrm{Id}_{H_N^q}(B')$$

então $B \cong B'$ como H_N^q-comódulo álgebras.

Seja H_N^q uma álgebra de Taft sobre R e fixe uma base $\{g^m x^n, 0 \leqslant m, n < N\}$. Denote por $E = Z_1^1$, $G = Z_1^g$ e $X = Z_1^x$. Então a coação $\delta\colon T \longrightarrow T \otimes H$ da Proposição 4.2.1 que torna T um H_N^q-comódulo álgebra é dada, nesses símbolos, por

$$\begin{aligned}\delta(E) &= E \otimes 1\\ \delta(G) &= G \otimes g\\ \delta(X) &= E \otimes x + X \otimes g.\end{aligned}$$

Proposição 5.2.8. *Seja $R \subset \mathcal{B}_{(u,a)}$ uma extensão H_N^q-cleft. Para cada homomorfismo de H_N^q-comódulo álgebras $f\colon T \longrightarrow \mathcal{B}_{(u,a)}$ existem únicos $\lambda, \mu, \xi \in R$ tais que*

1) $f(E) = \lambda$,

2) $f(G) = \mu v_g$,

3) $f(X) = \lambda v_x + \xi v_g$.

Demonstração. Fixe uma base $\{v_g^m v_x^n \,|\, 0 \leqslant m, n < N\}$ para $\mathcal{B}_{(u,a)}$ como na Proposição 5.2.2. Considere a coação $\rho\colon \mathcal{B}_{(u,a)} \longrightarrow \mathcal{B}_{(u,a)} \otimes H_N^q$ dada na mesma proposição por

$$\begin{aligned}\rho(v_g) &= v_g \otimes g\\ \rho(v_x) &= 1 \otimes x + v_x \otimes g.\end{aligned}$$

Para cada $P \in T$, existem únicos coeficientes $\alpha_{m,n}^P \in R$ $(0 \leqslant m, n < N)$ tais que

$$f(P) = \sum_{m,n=0}^{N-1} \alpha_{m,n}^P v_g^m v_x^n.$$

Como f é um homomorfismo de H_N^q-comódulos, ou seja $\rho \circ f = (f \otimes \mathrm{id}) \circ \delta$, podemos calcular os valores dos coeficientes $\alpha_{m,n}^P$ quando P é um dos símbolos E, G e X.

Primeiramente, do Lema 2.5.4, temos que

$$\begin{aligned}\rho \circ f(P) &= \sum_{m,n=0}^{N-1} \alpha_{m,n}^{P} \rho(v_g)^m \rho(v_x)^n \\ &= \sum_{m,n=0}^{N-1} \alpha_{m,n}^{P} (v_g \otimes g)^m (1 \otimes x + v_x \otimes g)^n \\ &= \sum_{m,n=0}^{N-1} \alpha_{m,n}^{P} \sum_{l=0}^{n} \binom{n}{l}_q v_g^m v_x^{n-l} \otimes g^{m+n-l} x^l,\end{aligned}$$

que é uma expressão em termos da base de $\mathcal{B}_{(u,a)} \otimes H_N^q$.

Como$(f \otimes \mathrm{id}) \circ \delta(P) = \rho \circ f(P)$, temos que:

i) Para $P = E$,

$$\begin{aligned}(f \otimes \mathrm{id}) \circ \delta(E) &= f(E) \otimes 1 \\ &= \left(\sum_{m,n=0}^{N-1} \alpha_{m,n}^{E} v_g^m v_x^n \right) \otimes 1 \\ &= \left(\alpha_{0,0}^{E} + \sum_{m=1}^{N-1} \alpha_{m,N-m}^{E} v_g^m v_x^{N-m} + \sum_{\substack{m,n=0 \\ 0 \neq m+n \neq N}}^{N-1} \alpha_{m,n}^{E} v_g^m v_x^n \right) \otimes 1\end{aligned}$$

e

$$\begin{aligned}\rho \circ f(E) = \Bigg(\alpha_{0,0}^{E} + \sum_{m=1}^{N-1} \alpha_{m,N-m}^{E} v_g^m v_x^{N-m} \Bigg) \otimes 1 + \sum_{m=1}^{N-1} \alpha_{m,N-m}^{E} v_g^m \otimes g^m + \\ + \sum_{m=1}^{N-1} \alpha_{m,N-m}^{E} \sum_{l=1}^{N-m-1} \binom{N-m}{l}_q v_g^m v_x^{N-m-l} \otimes g^{N-l} x^l + \\ + \sum_{\substack{m,n=0 \\ 0 \neq m+n \neq N}}^{N-1} \alpha_{m,n}^{E} \sum_{l=0}^{n} \binom{n}{l}_q v_g^m v_x^{n-l} \otimes g^{m+n-l} x^l.\end{aligned}$$

Comparando os coeficientes destas equações obtemos $\alpha_{m,n}^{E} = 0$ sempre que $(m,n) \neq (0,0)$ e $\alpha_{0,0}^{E}$ é o único fator restante, então tome $\lambda := \alpha_{0,0}^{E}$. Assim, $f(E) = \lambda$.

ii) Para $P = G$,

$$\begin{aligned}(f \otimes \mathrm{id}) \circ \delta(G) &= f(G) \otimes g \\ &= \left(\sum_{m,n=0}^{N-1} \alpha_{m,n}^{G} v_g^m v_x^n \right) \otimes g \\ &= \left(\alpha_{1,0}^{G} v_g + \alpha_{0,1}^{G} v_x + \sum_{m=2}^{N-1} \alpha_{m,N+1-m}^{G} v_g^m v_x^{N+1-m} \right) \otimes g + \\ &+ \sum_{\substack{m,n=0 \\ 1 \neq m+n \neq N+1}}^{N-1} \alpha_{m,n}^{G} v_g^m v_x^n \otimes g\end{aligned}$$

e

$$\begin{aligned}\rho \circ f(G) = &\left(\alpha_{1,0}^{G} v_g + \alpha_{0,1}^{G} v_x + \sum_{m=2}^{N-1} \alpha_{m,N+1-m}^{G} v_g^m v_x^{N+1-m} \right) \otimes g + \\ &+ \alpha_{0,1}^{G} \otimes x + \sum_{m=2}^{N-1} \alpha_{m,N+1-m}^{G} v_g^m \otimes g^m x^{N+1-m} + \\ &+ \sum_{m=2}^{N-1} \alpha_{m,N+1-m}^{G} \sum_{l=1}^{N+1-m} \binom{N+1-m}{l}_q v_g^m v_x^{N+1-m-l} \otimes g^{N+1-l} x^l + \\ &+ \sum_{\substack{m,n=0 \\ 1 \neq m+n \neq N+1}}^{N-1} \alpha_{m,n}^{G} \sum_{l=0}^{n} \binom{n}{l}_q v_g^m v_x^{n-l} \otimes g^{m+n-l} x^l.\end{aligned}$$

Comparando os coeficientes nestas equações, temos que $\alpha_{m,n}^{G} = 0$ sempre que $(m,n) \neq (1,0)$ e o único termo que permanece indeterminado é $\alpha_{1,0}^{G}$. Tomando $\mu := \alpha_{1,0}^{G}$, temos $f(G) = \mu v_g$.

iii) Para $P = X$, como $\alpha_{m,n}^{E} = 0$ sempre que $(m,n) \neq (0,0)$,

$$\begin{aligned}(f \otimes \mathrm{id}) \circ \delta(X) &= f(E) \otimes x + f(X) \otimes g \\ &= \alpha_{0,0}^{E} \otimes x + \sum_{m,n=0}^{N-1} \alpha_{m,n}^{X} v_g^m v_x^n \otimes g \\ &= \alpha_{0,0}^{E} \otimes x + \alpha_{1,0}^{X} v_g \otimes g + \alpha_{0,1}^{X} v_x \otimes g + \\ &+ \sum_{m=2}^{N-1} \alpha_{m,N+1-m}^{X} v_g^m v_x^{N+1-m} \otimes g + \sum_{\substack{m,n=0 \\ 1 \neq m+n \neq N+1}}^{N-1} \alpha_{m,n}^{X} v_g^m v_x^n \otimes g\end{aligned}$$

e

$$\begin{aligned}\rho\circ f(X) = &\left(\alpha^X_{1,0}v_g + \alpha^X_{0,1}v_x + \sum_{m=2}^{N-1}\alpha^X_{m,N+1-m}v_g^m v_x^{N+1-m} + \right)\otimes g + \\ &+\left(\alpha^X_{0,1} + \sum_{m=2}^{N-1}\alpha^X_{m,N+1-m}\binom{N+1-m}{1}_q v_g^m v_x^{N-m}\right)\otimes x + \\ &+\sum_{m=2}^{N-1}\alpha^X_{m,N+1-m}v_g^m\otimes g^m x^{N+1-m} + \\ &+\sum_{m=2}^{N-1}\alpha^X_{m,N+1-m}\sum_{l=2}^{N+1-m-l}\binom{N+1-m}{l}_q v_g^m v_x^{N+1-m-l}\otimes g^{N+1-l}x^l + \\ &+\sum_{\substack{m,n=0\\ 1\neq m+n\neq N+1}}^{N-1}\alpha^X_{m,n}\sum_{l=0}^{n}\binom{n}{l}_q v_g^m v_x^{n-l}\otimes g^{m+n-l}x^l.\end{aligned}$$

Desta vez, comparando os coeficientes, temos que $\alpha^X_{1,0}$ é livre, $\alpha^X_{0,1} = \alpha^E_{0,0} = \lambda$ e $\alpha^X_{m,n} = 0$ se $(m,n) \neq (1,0)$ ou $(m,n) \neq (0,1)$. Tomando $\xi := \alpha^X_{1,0}$, temos $f(X) = \lambda v_x + \xi v_g$.

■

Obviamente, a proposição anterior permanece verdadeira substituindo E, G e X respectivamente por Z^1_i, Z^g_i e Z^x_i, para qualquer $i \geq 2$.

De volta à nossa questão principal: Para a álgebra de Taft H^q_N, dados $R \subset B$ e $R \subset B'$ extensões H^q_N-cleft, em que condições $\mathrm{Id}_{H^q_N}(B) = \mathrm{Id}_{H^q_N}(B')$ implica $B \cong B'$ como H^q_N-comódulo álgebras?

Tendo em vista o Teorema 5.2.3, o Corolário 5.2.5 e a Proposição 5.2.6, podemos reescrever a questão anterior da seguinte forma: Quando é que $\mathrm{Id}_{H^q_N}(\mathcal{B}_{(u,a)}) = \mathrm{Id}_{H^q_N}(\mathcal{B}_{(u',a')})$ implica que $a' = a$ e que existe $s \in R^\times$ tal que $u' = s^N u$? Vamos analisar esta questão dividindo-a naturalmente em duas partes. Comecemos pela questão de decidir se $a' = a$:

Para que $\mathrm{Id}_{H^q_N}(\mathcal{B}_{(u,a)}) = \mathrm{Id}_{H^q_N}(\mathcal{B}_{(u',a')})$ implique $a' = a$, mostraremos que é suficiente pedir $1 - q \in R^\times$. Note que esta condição é a mesma do Corolário 5.2.5. Logo não estamos impondo restrição adicional com essa hipótese.

Faremos isso através de uma H^q_N-identidade polinomial conveniente:

Proposição 5.2.9. *Seja $R \subset \mathcal{B}_{(u,a)}$ uma extensão H^q_N-cleft. Então*

$$\mathcal{P}_a = (XG - qGX)^N - (1-q)^N G^N X^N + (1-q)^N a E^N G^N$$

é uma H^q_N-identidade polinomial para $\mathcal{B}_{(u,a)}$.

Demonstração. Seja $f\colon T \longrightarrow \mathcal{B}_{(u,a)}$ um homomorfismo de H_N^q-comódulo álgebras. Pela Proposição 5.2.8 em vista do Lema 2.5.4 temos que

$$\begin{aligned} f((XG - qGX)^N) &= (1-q)^N \mu^N \xi^N u^2 \\ f((1-q)^N G^N X^N) &= (1-q)^N \mu^N (\xi^N u^2 + \lambda^N ua) \\ f((1-q)^N a E^N G^N) &= (1-q)^N a \lambda^N \mu^N u \end{aligned}$$

Então $f(\mathcal{P}_a) = 0$. ∎

O tipo de polinômio $\mathcal{P}_a$ foi usado na Proposição 5.1.10 para o problema do isomorfismo para extensões cleft sobre as álgebras de Hopf monomiais não semissimples. Para demonstrar aquele resultado usamos o homomorfismo Ω, definido em (4.1). Porém, como já alertamos, Ω não funciona tão bem se R não for um corpo infinito. No caso do polinômio $\mathcal{P}_a$ acima, coincidentemente, $\Omega(\mathcal{P}_a) = 0$, ou seja, poderíamos ter usado Ω para mostrar a Proposição 5.2.9 ao invés de ter usado Proposição 5.2.8 com basicamente a mesma demonstração da Proposição 5.1.10. Entretanto, precisaremos de um outro polinômio mais adiante (5.7) que é uma H_N^q-identidade polinomial que não está em $\ker(\Omega)$. Por isso, optamos por usar a Proposição 5.2.8 também para o polinômio $\mathcal{P}_a$.

Proposição 5.2.10. *Sejam $R \subset \mathcal{B}_{(u,a)}$ e $R \subset \mathcal{B}_{(u',a')}$ extensões H_N^q-cleft. Se $1-q \in R^\times$ e*

$$\mathrm{Id}_{H_N^q}(\mathcal{B}_{(u,a)}) = \mathrm{Id}_{H_N^q}(\mathcal{B}_{(u',a')}),$$

então $a' = a$.

Demonstração. Pela Proposição 5.2.9, $\mathcal{P}_a$ é uma H_N^q-identidade polinomial para $\mathcal{B}_{(u,a)}$ e $\mathcal{P}_{a'}$ é uma H_N^q-identidade polinomial para $\mathcal{B}_{(u',a')}$. Como os T-ideais das H_N^q-identidades coincidem, então $\mathcal{P}_a - \mathcal{P}_{a'} = (1-q)^N(a-a')E^N G^N$ é uma H_N^q-identidade polinomial para $\mathcal{B}_{(u,a)}$.

Então para todo homomorfismo de H_N^q-comódulo álgebras $f\colon T \longrightarrow \mathcal{B}_{(u,a)}$, temos que $f(\mathcal{P} - \mathcal{P}') = 0$. Em particular, a seção de $\mathcal{B}_{(u,a)}$, $\gamma\colon H \longrightarrow \mathcal{B}_{(u,a)}$ dada por $\gamma(g^m x^n) = v_g^m v_x^n$ (que é um homomorfismo de H_N^q-comódulos) define um homomorfismo de H_N^q-comódulo álgebras $\Gamma\colon T \longrightarrow \mathcal{B}_{(u,a)}$ tal que $\Gamma(E) = \gamma(1) = 1$ e $\Gamma(G) = \gamma(g) = v_g$.

Portanto $0 = \Gamma(\mathcal{P} - \mathcal{P}') = (1-q)^N(a-a')u$. Como $(1-q)^N$ e u estão em $R^\times$, então $a' = a$. ∎

Tendo garantido que $\mathrm{Id}_{H_N^q}(\mathcal{B}_{(u,a)}) = \mathrm{Id}_{H_N^q}(\mathcal{B}_{(u',a')})$ é suficiente para obter $a' = a$ desde que $1 - q \in R^\times$, agora daremos condições suficientes para obter $s \in R^\times$ tal que $u' = s^N u$.

Precisaremos de duas hipóteses extras: R finito e $N \in R^\times$.

Lembremos de algumas propriedades gerais dos anéis finitos que nos serão úteis:

Observação 5.2.11. Seja R um anel (comutativo com unidade) finito. Então:

1) Anéis locais, anéis indecomponíveis e anéis sem idempotentes próprios são conceitos equivalentes.

2) Se R tem qualquer das propriedades equivalentes em 1) então todo elemento de R é uma unidade ou nilpotente. Isto é, para todo $x \in R$, ou $x^{\alpha} = 1$ ou $x^{\beta} = 0$, com α o expoente de $R^{\times}$ e β o índice de nilpotência do radical de R.

3) R é Artiniano. Portanto, por [35, 2.21 e 2.22], a identidade 1_R se decompõe unicamente em uma soma de idempotentes primitivos dois a dois ortogonais $1_R = e_1 + \ldots + e_n$. Em particular, para cada $r \in R$, a decomposição $r = re_1 + \ldots + re_n$ é única. Isso induz uma decomposição (em blocos) $R = R_1 \times \ldots \times R_n$ de anéis locais, com $R_i := Re_i$ e e_i o elemento identidade de R_i para todo $i = 1, \ldots, n$.

A partir de agora, sempre que R for um anel finito, fixe α como o expoente de $R^{\times}$ e β como o índice de nilpotência de R.

Proposição 5.2.12. *Seja R um anel e N um inteiro positivo. Se* $\operatorname{char} R > 0$ *então são equivalentes:*

1. $(N, \operatorname{char} R) = 1$,

2. $N \in R^{\times}$.

Demonstração. Se $(N, \operatorname{char} R) = 1$ então existem $x, y \in \mathbb{Z}$ tais que $aN + b \operatorname{char} R = 1$. Logo, $aN = 1$ em R e portanto $N \in R^{\times}$.

Para mostrar que (*2.*) implica (*1.*), seja $(N, \operatorname{char} R) = d > 0$. Então existem $x, y \in \mathbb{Z}$ tais que $N = dx$ e $\operatorname{char} R = dy$. $N \in R^{\times}$ implica que $d \in R^{\times}$. Por sua vez, $dy = 0$ em R implica $d \in R^{\times}$, então $y = 0$ em R. Logo $y = 0$ ou $\operatorname{char} R \mid y$. Mas $y \neq 0$ pois $\operatorname{char} R = dy$ e $\operatorname{char} R > 0$. Então $\operatorname{char} R \mid y$. Logo $y = \operatorname{char} R$ e portanto $d = 1$. ∎

Ao definir as álgebras de Taft [45] sobre um corpo k, Earl Taft pede indiretamente que $\operatorname{char} k = 0$ ou $(N, \operatorname{char} k) = 1$. No caso de R um anel finito, manteremos $(N, \operatorname{char} R) = 1$ como hipótese, ou equivalentemente, $N \in R^{\times}$.

O próximo lema é uma combinação de dois resultados de Janusz:

Lema 5.2.13. *[26, 2.1 e 2.4] Sejam R um anel indecomponível e $f(x) = x^n - c$ com $n > 1$ e $c \in R$. Se $n, c \in R^{\times}$ então $f(x)$ não possui mais que n raízes em R. Além disso, se x_1 e x_2 são raízes distintas de $f(x)$ em R, então $x_1 - x_2 \in R^{\times}$.*

Lema 5.2.14. *[36, IV, §1, 1.11] Sejam k um corpo e $f(x) = a_n x^n + \dots a_1 x + a_0$, com $a_0, \dots, a_n \in k$. Seja $a \in k$ uma raiz de $f(x)$. Então a é uma raiz simples se e somente se $f'(a) \neq 0$.*

Proposição 5.2.15. *Seja $N \geqslant 2$ e suponha que existe q uma raiz do N-ésimo polinômio ciclotômico em R. Se R é finito e $N \in R^\times$, então:*

1. *$N = o(q)$. Em particular, $N \mid \alpha$,*
2. *$1 - q \in R^\times$.*

Demonstração.

1. Seja $m := o(q)$. Dado $\mathfrak{m}$ um ideal maximal de R, seja $\mathbb{F} = R/\mathfrak{m}$ (o corpo com elementos $\overline{r} := r + \mathfrak{m}, r \in R$). Tome o polinômio $f(x) = x^N - 1$ em $\mathbb{F}[x]$. Como $q^N = 1$, temos que $\overline{q}^N = 1$ e portanto $f(\overline{q}) = 0$. Pelo Lema 5.2.14, $\overline{q}$ é uma raiz simples de f se e somente se $f'(q) = N\overline{q}^{N-1} \neq 0$. Este é o caso, dado que $N \in R^\times$.

   Por outro lado, usando polinômios ciclotômicos e pelo fato de $m \mid N$,

$$\begin{aligned} f(\overline{q}) = \overline{q}^N - 1 &= \prod_{d \mid N} \Phi_d(\overline{q}) \\ &= \left(\prod_{d \mid m} \Phi_d(\overline{q}) \right) \left(\prod_{\substack{d \mid N \\ d \nmid m \\ d \neq N}} \Phi_d(\overline{q}) \right) \Phi_N(\overline{q}) \\ &= (\overline{q}^m - 1) \left(\prod_{\substack{d \mid N \\ d \nmid m \\ d \neq N}} \Phi_d(\overline{q}) \right) \Phi_N(\overline{q}) \end{aligned}$$

   Observe que $\overline{q}^m - 1 = 0$ e $\Phi_N(\overline{q}) = 0$. Como q é uma raiz simples de f, necessariamente $o(q) = m = N$. Em particular, como R é finito, o teorema de Lagrange garante que $N \mid \alpha$.

2. Usando a decomposição em blocos de R por uma família de idempotentes primitivos dois a dois ortogonais $\{e_i\}$, seja $1 - q = \sum_i (1 - q)e_i$. Para obter $1 - q \in R^\times$ é suficiente mostrar que $(1 - q)e_i \in R_i^\times$ para cada i. R_i é indecomponível, $N, e_i \in R_i^\times$ e 1 e q são raízes distintas de $f(x)$ ($q \neq 1$ pois $o(q) = N \geqslant 2$), temos pelo Lema 5.2.13 que $1 - q \in R^\times$.

■

Seja $G = Z_1^g$ o Z-símbolo definido na Seção 5.2.2 e fixado $N \mid \alpha$, fixe também d o inteiro tal que $\alpha = dN$.

Proposição 5.2.16. *Seja $R \subset \mathcal{B}_{(u,a)}$ uma extensão H_N^q-cleft. Se R é finito e $N \in R^\times$ então*

$$\mathcal{Q}_u = (u^d - G^\alpha)G^\beta \tag{5.7}$$

é uma H_N^q-identidade polinomial para $\mathcal{B}_{(u,a)}$.

Demonstração. Seja $f\colon T \longrightarrow \mathcal{B}_{(u,a)}$ um homomorfismo de H_N^q-comódulo álgebras. Pela Proposição 5.2.8 temos que

$$f((u^d - G^\alpha)G^\beta) = u^d(1-\mu^\alpha)\mu^\beta v_g^\beta.$$

Observe que $f(\mathcal{Q}_u) = 0$ se e somente se $(1-\mu^\alpha)\mu^\beta = 0$. Como R é finito, então existe uma família de idempotentes primitivos dois a dois ortogonais $\{e_i\}_{i=1}^n$ que induz uma decomposição em blocos $R = R_1 \times \ldots \times R_n$. Portanto

$$\begin{aligned}(1-\mu^\alpha)\mu^\beta &= \sum_{i=1}^n (1-\mu^\alpha)\mu^\beta e_i \\ &= \sum_{i=1}^n \left(1e_i - (\mu e_i)^\alpha\right)(\mu e_i)^\beta \\ &= 0\end{aligned}$$

O último passo é válido pois para todo $\mu \in R$ e $i = 1, \ldots, n$, temos que μe_i é uma unidade ou um elemento nilpotente em R_i. Se μe_i é uma unidade, então $(\mu e_i)^\alpha = 1e_i$. Se (μe_i) é nilpotente então $(\mu e_i)^\beta = 0$.

Portanto $f(\mathcal{Q}_u) = 0$. ∎

Nota. A H-identidade polinomial $\mathcal{Q}_u$ em (5.7) não está necessariamente em $\ker(\Omega)$, como definido em (4.1). De fato, como

$$\Omega(\mathcal{Q}_u) = (u^d \otimes 1 - t_g^\alpha \otimes v_g^\alpha)(t_g^\beta \otimes v_g^\beta) = t_g^\beta \otimes v_g^\beta u^d - t_g^\alpha t_g^\beta \otimes u^d v_g^\beta = (t_g^\beta \otimes v_g^\beta)(1 \otimes 1 - t_g^\alpha \otimes 1)u^d,$$

então $\Omega(\mathcal{Q}_u) = 0$ se somente se $t_g^\alpha = 1$, o que não ocorre (lembre-se que as únicas relações em $S(t_H)$ são as de comutação). ∎

Enquanto $\mathcal{P}_a$ era capaz de garantir $a' = a$, o polinômio $\mathcal{Q}_u$ não resolve a questão $u' = s^N u$ diretamente. O polinômio $\mathcal{Q}_u$ consegue garantir que $(u')^d = u^d$. Para encontrar $s \in R^\times$ tal que $u' = s^N u$, daremos mais alguns passos posteriormente.

Proposição 5.2.17. *Sejam $R \subset \mathcal{B}_{(u,a)}$ e $R \subset \mathcal{B}_{(u',a')}$ duas extensões H_N^q-cleft. Se $\mathrm{Id}_{H_N^q}(\mathcal{B}_{(u,a)}) = \mathrm{Id}_{H_N^q}(\mathcal{B}_{(u',a')})$ então $(u')^d = u^d$, com d dado por $\alpha = dN$.*

Demonstração. Considere a H_N^q-identidade polinomial $\mathcal{Q}_u$ de $\mathcal{B}_{(u,a)}$ (em (5.7)). Como as H_N^q-identidades polinomiais coincidem, então $\mathcal{Q}_u \in \mathrm{Id}_{H_N^q}(\mathcal{B}_{(u',a')})$. Logo, para todo homomorfismo de H_N^q-comódulo álgebras $f\colon T \longrightarrow \mathcal{B}_{(u,a)}$,

$$0 = f(\mathcal{Q}_u) = (u^d - (u')^d \mu^\alpha)\mu^\beta v_g^\beta.$$

Em particular, para $\mu = 1$, temos que $u^d = (u')^d$. ∎

Em vista do teorema fundamental dos grupos abelianos finitamente gerados, o próximo resultado mostra que $u^d = (u')^d$ é suficiente para obter $s \in R^\times$ tal que $u' = s^N u$.

Lema 5.2.18. *Seja $G \neq 0$ um grupo abeliano finito e α o expoente de G. Então G é gerado por um subconjunto de $\{g \in G \mid o(g) = \alpha\}$.*

Demonstração. Pelo teorema fundamental dos grupos abelianos finitamente gerados, [22, 5.3], $G \cong (\mathbb{Z}/n_1\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/n_r\mathbb{Z})$ com $n_1 \mid n_2 \mid \ldots \mid n_r$. Como $(\mathbb{Z}/n_i\mathbb{Z})$ é cíclico para todo i, então o expoente e a ordem de cada fator coincidem. Portanto $n_r = \alpha$. Tome $V = \{(1,\ldots,1),(0,1,\ldots,1),(0,0,1,\ldots,1)),\ldots,(0,\ldots,0,1)\}$. Não é difícil ver que V gera G e $o(v) = \alpha$ para todo $v \in V$. ∎

Proposição 5.2.19. *Seja $N \geqslant 2$ e suponha que existe uma raiz q do N-ésimo polinômio ciclotômico em R. Se R é finito e $N \in R^\times$ então, para cada $c \in R^\times$, o polinômio $f(x) = x^N - c$ possui uma raiz em R se e somente se $c^d = 1$.*

Demonstração. Se existe $t \in R^\times$ tal que $t^N = c$ então $c^d = t^{Nd} = t^\alpha = 1$. Por outro lado, como pelo Lema 5.2.18, um subconjunto de $\{y \in R^\times \mid o(y) = \alpha\}$ gera $R^\times$, então existe $y \in R^\times$ e $b > 0$ tais que $c = y^b$, com $o(y) = \alpha$. Então $y^{bd} = 1$. Portanto existe $m > 0$ tal que $bd = \alpha m = Ndm$. Logo $b = Nm$. Então, podemos escrever $c = y^b = (y^m)^N$. Tomando $t = y^m$ temos que $f(t) = 0$. ∎

Isso é suficiente para resolver a questão de $u' = s^N u$:

Proposição 5.2.20. *Seja $R \subset \mathcal{B}_{(u,a)}$ e $R \subset \mathcal{B}_{(u',a')}$ extensões H_N^q-cleft. Se R é finito, $N \in R^\times$ e $\mathrm{Id}_{H_N^q}(\mathcal{B}_{(u,a)}) = \mathrm{Id}_{H_N^q}(\mathcal{B}_{(u',a')})$, então existe $s \in R^\times$ tal que $u' = s^N u$.*

Demonstração. Pela Proposição 5.2.17, temos que $(u')^d = u^d$. Tomando $c = u'u^{-1}$ na Proposição 5.2.19 obtemos $u' = s^N u$. ∎

Finalmente, o teorema principal desta seção (Teorema 5.2.7) segue diretamente da Proposição 5.2.10 e da Proposição 5.2.20 tendo em vista a Proposição 5.2.15 e a Proposição 5.2.4.

Referências Bibliográficas

[1] Aljadeff, E., and Haile, D. Simple G-graded algebras and their polynomial identities. *Trans. Amer. Math. Soc. 366*, 4 (2014), 1749–1771.

[2] Aljadeff, E., and Kassel, C. Polynomial identities and noncommutative versal torsors. *Adv. Math. 218*, 5 (2008), 1453–1495.

[3] Aluffi, P. *Algebra: chapter 0*, vol. 104 of *Graduate Studies in Mathematics*. Amer. Math. Soc., 2009.

[4] Amitsur, S. A. Polynomial identities. *Israel J. Math. 19* (1974), 183–199.

[5] Andruskiewitsch, N., and Ferrer Santos, W. The beginnings of the theory of Hopf algebras. *Acta Appl. Math. 108*, 1 (2009), 3–17.

[6] Bahturin, Y., and Diniz, D. Graded identities of simple real graded division algebras. *J. Algebra 500* (2018), 316–334.

[7] Bahturin, Y., and Yasumura, F. Graded polynomial identities as identities of universal algebras. *Linear Algebra App. 562* (2019), 1 – 14.

[8] Bergman, G. M. The diamond lemma for ring theory. *Adv. in Math. 29*, 2 (1978), 178–218.

[9] Bianchi, A., and Diniz, D. Identities and isomorphisms of finite-dimensional graded simple algebras. *Journal of Algebra 526* (2019), 333–344.

[10] Bichon, J. Galois and bigalois objects over monomial non-semisimple Hopf algebras. *J. Algebra Appl. 5*, 5 (2006), 653–680.

[11] Blattner, R. J., Cohen, M., and Montgomery, S. Crossed products and inner actions of Hopf algebras. *Trans. Amer. Math. Soc. 298*, 2 (1986), 671–711.

[12] Borel, A. Homology and cohomology of compact connected Lie groups. *Proc. Nat. Acad. Sci. U.S.A. 39* (1953), 1142–1146.

[13] Brzezinski, T., and Wisbauer, R. *Corings and comodules*, vol. 309 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2003.

[14] Chase, S. U., and Sweedler, M. E. *Hopf algebras and Galois theory*. Lecture Notes in Mathematics, Vol. 97. Springer-Verlag, Berlin-New York, 1969.

[15] Chen, X.-W., Huang, H.-L., Ye, Y., and Zhang, P. Monomial Hopf algebras. *J. Algebra 275*, 1 (2004), 212–232.

[16] Dascalescu, S., Natasescu, C., and Raianu, S. *Hopf Algebra: An Introduction*, vol. 235 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., 2001.

[17] Di Vincenzo, O. M., and Spinelli, E. Graded polynomial identities on upper block triangular matrix algebras. *J. Algebra 415* (2014), 50–64.

[18] Doi, Y. Equivalent crossed products for a Hopf algebra. *Comm. Algebra 17*, 12 (1989), 3053–3085.

[19] Doi, Y., and Takeuchi, M. Cleft comodule algebras for a bialgebra. *Comm. Algebra 14*, 5 (1986), 801–817.

[20] Drensky, V. S., and Racine, M. L. Distinguishing simple Jordan algebras by means of polynomial identities. *Comm. Algebra 20*, 2 (1992), 309–327.

[21] Drinfeld, V. G. Quantum groups. *Proceedings of the International Congress of Mathematicians, Vol. 1, 2* (1987), 798–820.

[22] Dummit, D. S., and Foote, R. M. *Abstract Algebra*, 3th ed. John Wiley and Sons Inc., 2004.

[23] Hopf, H. Über die Topologie der Gruppen-Mannigfaltigkeiten und ihre Verallgemeinerungen. *Ann. of Math. (2) 42* (1941), 22–52.

[24] Huang, Q. Extension of irreducible characters from normal subgroups. *Linear and Multilinear Algebra 27*, 2 (1990), 117–119.

[25] Hungerford, T. W. *Algebra*. No. 73 in Graduate Texts in Mathematics. Springer-Verlag, 1980.

[26] Janusz, G. J. Separable algebras over commutative rings. *Trans. Amer. Math. Soc. 122* (1966), 461–479.

[27] Ji, C.-G., and Li, W.-P. Values of coefficients of cyclotomic polynomials. *Discr. Math. 308*, 23 (2008), 5860–5863.

[28] Karasik, Y. *G*-graded central polynomials and *G*-graded Posner's theorem. *Trans. Amer. Math. Soc. 372*, 8 (2019), 5531–5546.

[29] Karpilovsky, G. *Projective representations of finite groups*, vol. 94 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 1985.

[30] Kassel, C. *Quantum Groups*. No. 155 in Graduate Texts in Mathematics. Springer-Verlag, 1995.

[31] Kassel, C. Examples of polynomial identities distinguishing the Galois objects over finite-dimensional Hopf algebras. *Ann. Math. Blaise Pascal 20*, 2 (2013), 175–191.

[32] Koshlukov, P., and Zaicev, M. Identities and isomorphisms of graded simple algebras. *Linear Algebra Appl. 432*, 12 (2010), 3141–3148.

[33] Kreimer, H. F., and Cook, II, P. M. Galois theories and normal bases. *J. Algebra 43*, 1 (1976), 115–121.

[34] Kushkuleĭ, A. K., and Razmyslov, Y. P. Varieties generated by irreducible representations of Lie algebras. *Vestnik Moskov. Univ. Ser. I Mat. Mekh.*, 5 (1983), 4–7.

[35] Lam, T. Y. *A first course in noncommutative rings*, vol. 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.

[36] Lang, S. *Algebra*, third ed., vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[37] Masuoka, A. Cleft extensions for a Hopf algebra generated by a nearly primitive element. *Comm. Algebra 22*, 11 (1994), 4537–4559.

[38] Montgomery, S. *Hopf Algebras and their Actions on Rings*. No. 82 in Regional Conference Series in Mathematics. American Mathematical Soc., 1993.

[39] Oliveira, A. G., and Schützer, W. On some H-cleft extensions which are distinguished by their polynomial H-identities, 2022.

[40] Radford, D. E. *Hopf Algebras*, vol. 49 of *Series on Knots and Everything*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.

[41] Ramos Borges, A., Fidelis, C., and Diniz, D. Graded isomorphisms on upper block triangular matrix algebras. *Linear Algebra Appl. 543* (2018), 92–105.

[42] Razmyslov, Y. P. *Identities of algebras and their representations*, vol. 138 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1994. Translated from the 1989 Russian original by A. M. Shtern.

[43] Schützer, W., and Oliveira, A. G. On some H-Galois objects and their polynomial H-identities. *Arch. Math. (Basel) 116*, 1 (2021), 7–18.

[44] Shestakov, I., and Zaicev, M. Polynomial identities of finite dimensional simple algebras. *Comm. Algebra 39*, 3 (2011), 929–932.

[45] Taft, E. J. The order of the antipode of finite-dimensional Hopf algebra. *Proc. Nat. Acad. Sci. U.S.A. 68* (1971), 2631–2633.

[46] Ulbrich, K.-H. Vollgraduierte Algebren. *Abh. Math. Sem. Univ. Hamburg 51* (1981), 136–148.